International journal of applied management and economics
Vol : 02 , N° 14, June 2025
ISSN : 2509-0720

Digital Constitutionalism 2.0: A Disruptive Governance Framework for European Artificial-Intelligence Regulation Beyond the European Union Artificial Intelligence Act.

– **Author 1 :** BENSEGHIR Jadoua,

(1) : PhD in Law (in progress), LL.M. in International Trade and Investment Law, Dual Master's in Business Law.
College, University : Hassan II University of Casablanca, Morocco (Doctoral Researcher), University of Szeged, Hungary (LL.M.), University of Nice Sophia-Antipolis, France & Mundiapolis University, Morocco (Dual Master's).

Conflict of interest: The author reports no conflict of interest.

To quote this article: BENSEGHIR Jadoua (2025) « Digital Constitutionalism 2.0: A Disruptive Governance Framework for European Artificial-Intelligence Regulation Beyond the European Union Artificial Intelligence Act »,

IJAME : Volume 02, N° 14 | Pp: 301 – 334.

Submission Date : May 2025
Publication Date : June 2025

DOI : 10.5281/zenodo.15807966

Abstract

This paper takes a look at the EU's project of digital constitutionalism amid the governance puzzles posed by AI. The Union's present formula (anchored in proportionality, state-centric rules, and static risk boxes) struggles to keep pace with AI's fast-moving, opaque, and deeply political harms. Threats such as electoral manipulation, vanishing explainability, the hollowing out of the GDPR's Right to be Forgotten, and ever-widening surveillance risks are already testing the system's seams. Through a systematic review, the analysis exposes structural weak spots. It then sizes up the main reform options, the EU AI Act and others, marking both their promise and their blind corners. Synthesizing those findings, the paper sketches a *"Universal AI Regulation Model (UARM)",* an example of a polycentric framework that couples dynamic socio-political impact tests with prophylactic bans on high-risk uses, algorithmic restitution, and innovation-friendly safe harbors. By foregrounding democratic resilience, transparency, and adaptability, the *UARM* aims to square AI's disruptive power with the EU's core commitments to human fundamental rights, the rule of law, and digital sovereignty. The conclusion is blunt: only agile, context-aware regulation will safeguard Europe's constitutional ethos in the algorithmic age.

Keywords: *Artificial Intelligence Regulation; Digital Constitutionalism; Fundamental Rights; EU Governance; Algorithmic Accountability; GDPR; AI Ethics; Surveillance Technologies; Regulatory Frameworks; Democratic Resilience; Risk Assessment.*

1. Introduction

It is today more obvious than ever that the rapid integration of artificial intelligence into governance poses unprecedented challenges to the European Union's constitutional order. We must admit that the EU has pioneered digital constitutionalism, a project to extend constitutional safeguards into the digital realm. However, its frameworks increasingly struggle to address AI's opacity, scale, potential for systemic impact,[1] and is thus in serious risk of obsolescence.[2]

Therefore, this paper contends that the EU's digital constitutionalism model requires a paradigm shift. We begin by diagnosing structural flaws in the current framework. Notably including its reliance on proportionality balancing, state-centric enforcement, and static risk classifications. Through case studies (ranging from "deepfake election interference" to "biases in predictive policing") we illustrate how AI exacerbates these weaknesses, thus eroding privacy, accountability and, democratic integrity. Our analysis then critiques emerging regulatory responses, such as the AI Act's risk-tiered approach and ethical soft-law initiatives, revealing gaps in enforcement, adaptability, and redress. Building on this foundation, the paper proposes the Universal AI Regulation Model (UARM), a dynamic framework designed to preempt harm while fostering innovation. By synthesizing insights from notable emergent AI regulatory models proposed by scholars, the UARM model that we propose reimagines AI regulation as a "continuous and rights-preserving process" that can help fill in the cracks left by the EU AI Act as we highlighted. We argue in this paper that only through such adaptive, multi-stakeholder approaches can the EU safeguard its constitutional values in an AI-driven future.

II. Methodology

This paper employs a mixed-methods approach to analyze the EU's regulatory response to AI and propose a novel governance framework. The methodology is structured into three phases. Each employs distinct analytical techniques. The first phase combines doctrinal legal analysis and qualitative case studies. The second phase adopts a different method. It utilizes comparative policy evaluation and interdisciplinary synthesis. The third phase employs normative design and iterative modeling to construct what we call the "Universal AI Regulation Model

[1] Sascha Bredt, 'Artificial Intelligence (AI) in the Financial Sector - Potential and Public Strategies' (2019) 2 *Frontiers in Artificial Intelligence 16* <https://doi.org/10.3389/frai.2019.00016> accessed 10 January 2025

[2] Matej Avbelj, 'Reconceptualizing constitutionalism in the AI-run algorithmic society' (2023) 11(1) International Journal of Constitutional Law 112–137. <https://www.researchgate.net/publication/385325570_Reconceptualizing_Constitutionalism_in_the_AI_Run_Algorithmic_Society> accessed 10 January 2025

(UARM)", grounded on gaps identified in earlier phases. Limitations facing this paper's methodology that we can cite include a reliance on secondary data, which may exclude emergent AI risks, and the theoretical nature of the "UARM," which requires empirical validation. Political and technical implementation challenges are acknowledged but not exhaustively resolved.

III. Literature Review

1. Framing Digital Constitutionalism

Let us first start by defining what is meant by this concept. Digital constitutionalism has rapidly gained attention as a legal and theoretical framework that aims to apply or adapt traditional constitutional values to the digital realm.[3]

We can say that Digital constitutionalism, at its core, interrogates how fundamental rights, institutional checks and balances, and democratic principles function in an environment increasingly shaped by technological intermediaries and transnational corporate actors. In contrast to earlier libertarian ideals of a *"borderless internet,"* digital constitutionalism acknowledges that large technology companies and powerful governmental bodies can exert quasi-constitutional authority online.[4] This development triggers questions around legitimacy, fundamental rights protection, and the proper balance between AI innovation and AI regulation.[5]

Reflecting the dynamism and complexity of the digital environment, scholarship on digital constitutionalism traverses broad concerns: from the normative goals it seeks to achieve, to the historical underpinnings that situate it within global capitalism, and to specific regulatory instruments, such as the European Union's General Data Protection Regulation (GDPR)[6], the proposed AI Act[7], or the European Declaration on Digital Rights[8]. The literature also questions

[3] Angelo Jr Golia, 'Critique of Digital Constitutionalism: Deconstruction and Reconstruction from a Societal Perspective' (2024) 13 *Global Constitutionalism* 488–518 <https://doi.org/10.1017/S2045381723000126> accessed 10 January 2025

[4] Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4(3) *Social Media + Society* 2056305118787812 <https://journals.sagepub.com/doi/10.1177/2056305118787812> accessed 10 January 2025

[5] Rowena Rodrigues, 'Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities' (2020) 4 *Journal of Responsible Technology* 100005 <https://doi.org/10.1016/j.jrt.2020.100005> accessed 10 January 2025

[6] Regulation (EU) 2016/679 General Data Protection Regulation [2016] OJ L 119/1.

[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence [2024] OJ L1689/1.

[8] Regulation (EU) 2023/C 23/01 'European Declaration on Digital Rights and Principles for the Digital Decade' [2023] OJ C 23/1

whether digital constitutionalism constitutes a revolutionary paradigm or merely an evolution of established constitutional traditions for the digital age.

Multiple authors contend that digital constitutionalism must be understood both as an extension of contemporary constitutional values and as a reaction to the novel constraints of platform power. Celeste (in *Digital constitutionalism: a socio-legal approach* and *Constitutionalism in the Digital Age*[9]) argues that digital constitutionalism *"embodies the idea of projecting the values of contemporary constitutionalism in the context of the digital society."* This projection involves, on one hand, adopting rights-based frameworks (privacy, data protection, freedom of expression[10]) and, on the other hand, considering how new forms of private and public power arise in the digital sphere. Celeste[11] further develops a "socio-legal" lens, proposing that traditional categories of constitutional law are insufficient and must expand to include non-state norms (e.g., platform policies, codes of conduct).[12]

Meanwhile, Celeste in another paper (*Digital constitutionalism: Mapping the constitutional response to digital technology's challenges*[13]) conceptualizes these new normative responses, such as platform charters and global statements of digital human rights,[14] [15] as part of an ongoing "process of constitutionalisation" in which multiple actors (private companies, EU institutions, states, and civil society) reshape constitutional principles to fit the digital realm. From this vantage, emergent legal gaps are best addressed through flexible, iterative mechanisms that recognize the transnational nature of online regulation.

While many authors view digital constitutionalism as promising, Terzis (*Against Digital*

[9] Edoardo Celeste, 'Digital Constitutionalism: A Socio-Legal Approach' (2024) 10(2) *European Data Protection Law Review* 146–149 <https://doi.org/10.21552/edpl/2024/2/5> accessed 10 January 2025

[10] See Article 10 CFR - freedom of expression. <https://doi.org/10.21552/edpl/2024/2/5> accessed 10 January 2025

[11] Ibid.

[12] *"Digital constitutionalism would denote processes of instilling constitutional values and principles into the rules of private tech corporations, with particular attention to digital platforms." Ibid.*

[13] Edoardo Celeste, 'Digital constitutionalism: mapping the constitutional response to digital technology's challenges' (2021) 9(3) International Journal of Law and Information Technology 253–281. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3219905> accessed 10 January 2025

[14] See for example : Meta Platforms Inc, 'Corporate Human Rights Policy' (31 March 2021) <https://about.fb.com/wp-content/uploads/2021/03/Facebooks-Corporate-Human-Rights-Policy.pdf> accessed 10 January 2025

[15] Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4(3) *Social Media + Society* 2056305118787812 <https://journals.sagepub.com/doi/10.1177/2056305118787812> accessed 10 January 2025

Constitutionalism[16]) issues a strong critique, challenging the premise that there is a "constitutional vacuum" in the digital sphere. Terzis points out that law (whether through corporate statutes, intellectual property rights, or everyday commercial rules) has long underpinned the rise of formidable corporate players. The narrative of digital constitutionalism can flatten complex realities and, in doing so, exaggerates the promise of a purely legal "revolution." Instead, the author urges a richer historical and economic excavation of how corporate authority gained legitimacy, challenging legal scholars to probe the structural forces concentrating digital power.

2. Digital Constitutionalism in the European Context

Pereira (*Mapping the values of digital constitutionalism: guiding posts for digital Europe?*[17]) asks a vital question: which core values (transparency, accountability, fundamental rights) truly anchor digital constitutionalism? By charting how those ideals surface in the GDPR, the Digital Services Act, and beyond, he shows that platformization[18] and market concentration make it urgent to nail down clear normative signposts for EU policy.

Celeste, in his work on the *European Declaration on Digital Rights*[19] (*Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights*[20]), he frames the forthcoming Declaration as both an instructional charter and a diplomatic tool for the Union's wider digital-sovereignty push. While the Declaration mostly reasserts long-standing freedoms, its programmatic tone signals Brussels's intent to export its governance model, internally and to the world.

That ambition echoes in Czarnocki's work (*Saving EU digital constitutionalism through the proportionality principle and a transatlantic digital accord*[21]), where the real trick, he argues,

[16] Petros Terzis, 'Against digital constitutionalism' (2024) 3(2) European Law Open 336–352. <https://doi.org/10.1017/elo.2024.15> accessed 10 January 2025

[17] Miguel Pereira, 'Mapping the values of digital constitutionalism: guiding posts for digital Europe?' (2024) 10(2) UNIO – EU Law Journal 1–25. <https://doi.org/10.21814/unio.10.2.6045> accessed 10 January 2025

[18] Nieborg, D. B., & Helmond, A. (2019). 'The political economy of Facebook's platformization in the mobile ecosystem: Facebook Messenger as a platform instance.' *Media, Culture & Society*, *41*(2), 196-218. <https://doi.org/10.1177/0163443718818384> accessed 10 January 2025

[19] European Commission, 'European Declaration on Digital Rights and Principles for the Digital Decade' (2022) <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles-digital-decade> accessed 10 January 2025

[20] Edoardo Celeste, 'Digital constitutionalism, EU digital sovereignty ambitions and the role of the European Declaration on Digital Rights' (2023) 14(1) International Journal of Law and Information Technology 45–67. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4698091> accessed 10 January 2025

[21] Jan Czarnocki, 'Saving EU digital constitutionalism through the proportionality principle and a transatlantic digital accord' (2023) 28(4) European Public Law 789–812. <https://www.martenscentre.eu/wp-content/uploads/2021/10/5.pdf> accessed 10 January 2025

is balancing rights protection with economic dynamism. He proposes using the proportionality principle as the compass for a transatlantic accord, extending the *"Brussels effect"* without diluting the EU's rights-first DNA.[22]

3. Digital Constitutionalism & AI

AI's march into public decision-making has turned digital constitutionalism into a stress test. Palladino's (See *A digital constitutionalism framework for Ai*[23]*)* hybrid framework blends societal-constitutional theory with science-and-tech studies with the goal of embedding fundamental rights into AI by design. He goes onto mapping rights into four rule types (coding, security, inclusionary, exclusionary) and insisting that multi-stakeholder coalitions embed them directly into technical standards under the EU AI Act. Yet he worries, and so do I, that private capture of standard-setting and tech solutionism could blunt accountability.[24]

Avbelj in his work *'Reconceptualizing Constitutionalism in the AI Run Algorithmic Society'*[25] pushes further, arguing state-centric constitutions look clumsy against AI's transnational infrastructure. His antidote is *"algorithmic accountability,"* a reflexive legal posture that morphs with technological change. Pollicino and Paolucci[26] pick up the thread, critiquing the AI Act's reactive fixation on high-risk systems and its skimpy procedural guard-rails; due-process tools, they say, to ensure horizontal rights enforcement against private actors.[27]

Campos' *A Necessary Cognitive Turn in Digital Constitutionalism* offers a pragmatic twist: *"regulated self-regulation."*[28] Comparing the GDPR with Brazil's AI bills, he champions a mix of state oversight and sector expertise (certifications, codes of conduct) while warning that anything less than harmonised standards risks fragmentation and stifling innovation.[29]

[22] Charlotte Siegmann and Markus Anderljung, 'The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market' (GovAI
Report, 2022) <https://cdn.governance.ai/Brussels_Effect_GovAI.pdf> accessed 10 January 2025

[23] Palladino N, 'A Digital Constitutionalism Framework for Ai' (2023) 3 Rivista di Digital Politics 521. <https://www.internetpolicyresearch.eu/a-digital-constitutionalism-framework-for-ai-security-and-fundamental-rights-in-the-ai-act/4931> accessed 10 January 2025

[24] *Ibid.*

[25] Matej Avbelj, 'Reconceptualizing Constitutionalism in the AI-Run Algorithmic Society' (2023) 11(1) *International Journal of Constitutional Law* 112–137 <https://www.researchgate.net/publication/385325570_Reconceptualizing_Constitutionalism_in_the_AI_Run_Algorithmic_Society> accessed 10 January 2025

[26] Pollicino O and Paolucci F, 'Digital Constitutionalism' in L Floridi, M Ziosi and M Taddeo (eds), Companion to Digital Ethics (OUP 2024). <http://dx.doi.org/10.2139/ssrn.5098492> accessed 10 January 2025

[27] *Ibid.*

[28] Campos R, 'A Necessary Cognitive Turn in Digital Constitutionalism: Regulated Self-Regulation as a Regulatory Mechanism for Artificial Intelligence (AI) in Comparative Law' in Digital Constitutionalism (Nomos 2025). <https://www.nomos-elibrary.de/de/10.5771/9783748938644-113.pdf> accessed 10 January 2025

[29] *Ibid.*

Taken together, these scholars cast digital constitutionalism as a dual mission: re-assert fundamental rights and adapt law to AI's borderless, technical realities. Yet tensions linger between rigid rulebooks and AI's fluid social impact, leaving the reconciliation of constitutional norms and algorithmic power an unfinished business.

IV. Development

1. Why the EU Needs More Than Digital Constitutionalism whilst facing AI?

Artificial intelligence is reshaping Europe's legal landscape, and not always for the better. This can be a legitimate cause of concern because the socio-political heft of AI can tilt public discourse and skew economic opportunity, eroding democratic debate and personal autonomy in the process. Add in explainability gaps (given the sheer scale, speed, and opacity of advanced models) and the rule of law starts to wobble. Training pipelines threaten the GDPR's "Right to Be Forgotten", while unanswered questions about liability for AI-driven crimes expose cracks in accountability and legal liability. Finally, AI fuelled surveillance amplifies state monitoring, risking privacy collapse and, in the worst case, authoritarian creep. Together, these pressures reveal just how limited Europe's current digital constitutionalism playbook really is, and underscores the necessity for more disruptive regulatory models.

A. The Socio-Political Impact of AI

AI has already left fingerprints on EU elections, when Cambridge Analytica's[30] micro-targeted ads deepened polarisation. In France's 2017 presidential race, bot-driven amplification of leaked emails warped voter perceptions.[31] Fast-forward to Slovakia, 2023: a deep-fake audio clip rocked parliamentary polls at the eleventh hour.[32] [33]

Each episode shows how algorithms can hijack narratives and punch holes in democratic safeguards. If AI can forecast behaviour, steer voters, and shape policy, what chance does a static rulebook have? Robust regulation is now non-negotiable.

B. AI Explainability: Scale, Velocity, and 'Black Box' Problems

[30] Keith Jakee and Demi Fink, 'Micro-targeting Voters in the 2016 US Election: Was Cambridge Analytica Really Different?' (SSRN Working
Paper, 1 May 2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4843786> accessed 10 January 2025

[31] Reuters, 'US Far-Right Activists, WikiLeaks and Bots Help Amplify Macron Leaks: Researchers' *Reuters* (Paris, 5 May 2017) <https://www.reuters.com/world/us-far-right-activists-wikileaks-and-bots-help-amplify-macron-leaks-research-idUSKBN18302L/> accessed 10 January 2025

[32] Matyáš Boháček, 'Slovakia as the Precursor to Deepfake-Enabled Election Interference: Lessons Learned and Pathways Forward' in *Proceedings of the 18th ICWSM* (AAAI Press 2024) 3–6 June 2024 <https://workshop-proceedings.icwsm.org/pdf/2024_67.pdf> accessed 10 January 2025

[33] Laura De Nadal and Patrik Jančárik, 'Beyond the Deepfake Hype: AI, Democracy, and "the Slovak Case"' (2024) 5(4) *HKS Misinformation Review* <https://misinforeview.hks.harvard.edu/article/beyond-the-deepfake-hype-ai-democracy-and-the-slovak-case/> accessed 10 January 2025

Across the EU, AI tools are spreading at a dizzying speed, and, as noticed, every fresh deployment sharpens worries about who is watching the watchers. The EU's digital-constitutional project suddenly finds itself wrestling with opaque "black boxes" that block meaningful oversight and chip away at core constitutional principles.

When technical opacity meets legal uncertainty, clarity and predictability (the twin pillars of fair rights enforcement) start to wobble.[34] Courts and regulators are left to patch the gaps piecemeal, producing a patchwork of guidance that varies from one jurisdiction to the next.[35] Small wonder, then, that people on the receiving end of an AI-led decision cannot always grasp, let alone challenge, the outcome.

The problem runs deeper than procedure. By clouding intent and causation,[36] AI's opacity scrambles traditional legal tests that rely on traceable reasoning. Autonomous, self-learning models sift through patterns well beyond human perception, making responsibility harder to pin down. Frameworks like Bathaee's *"supervision-transparency model"*[37] therefore tie liability to human oversight and explainability, an approach that tries to realign algorithmic complexity with long-standing norms of accountability and fairness.[38]

Opacity breeds bias as well. When the underlying data are skewed or hidden, AI systems recycle historic prejudices (think of racially biased recidivism scores[39]) and those affected need a genuine chance to probe or contest the logic.[40] No one should accept a life-changing decision they cannot inspect or scrutinize. That principle fuels the rise of Explainable AI (XAI)[41] tools designed to open the black box.

[34] Marco Almada, 'Governing the Black Box of AI' (SSRN Pre-print, 7 November 2023) <https://ssrn.com/abstract=4587609> accessed 10 January 2025

[35] *Ibid.*

[36] Lehmann, J., Breuker, J., & Brouwer, B. (2004). 'Causation in AI and law.' Artificial Intelligence and Law, 12, 279-315. <https://www.researchgate.net/publication/220539291_Causation_in_AI_and_Law> accessed 10 January 2025

[37] Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31(2) *Harvard Journal of Law & Technology* 889 <https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf> accessed 10 January 2025

[38] *Ibid.*

[39] Van Dijck, G. 'Predicting recidivism risk meets AI act.' European Journal on Criminal Policy and Research, 28(3), 407-423. (2022). <https://link.springer.com/article/10.1007/s10610-022-09516-8> accessed 10 January 2025

[40] Sharon D Nelson and John W Simek, 'The Ethical and Legal Implications of Black-Box Artificial Intelligence' (Sensei Enterprises White Paper, 2020) <https://senseient.com/wp-content/uploads/Black-Box-AI.pdf> accessed 10 January 2025

[41] Andreas Holzinger *et al*, 'Explainable AI Methods - A Brief Overview' in Benjamin Biecek, Piotr Molnar and Wojciech Samek (eds), *Extending Explainable AI Beyond Deep Models and Classifiers* (Springer 2020) 13–38 <https://link.springer.com/chapter/10.1007/978-3-031-04083-2_2> accessed 10 January 2025

Taken together, these dynamics make one thing plain: tackling AI opacity is no optional add-on to the EU's digital constitutionalism, it is a necessity. Unless we embed transparency, accountability, and fairness into the heart of the system, the constitutional values we prize risk slipping through our fingers.

C. AI's training & The threat to the GDPR's Right to be Forgotten

Finally, vast training datasets collide head-on with privacy protections. Let's take here the example of the GDPR's Right to Be Forgotten,[42] [43] which aims to let individuals erase digital traces of personal data, but data hungry AI models embed those traces so deeply that effective deletion becomes a logistical nightmare, or more truthfully, an impossibility.[44] Without stronger tools (we can cite here : synthetic substitution, retraining mandates, or granular data-lineage tracking, etc...) the RTBF risks becoming more aspiration than reality.

The current patchwork of voluntary *"ethical AI"* pledges, though well-intentioned, simply lacks teeth. These codes circle around privacy in a narrow sense while ignoring wider rights such as the RTBF. Without hard-law safeguards grounded in international human-rights norms and EU data-protection principles, AI platforms can collect and retain data (and we are most importantly referring to personal data, although non-personal data remains important as well) in ways that deepen inequality and erode autonomy. Only rights-based, enforceable rules, coupled with tangible sanctions will keep developers answerable for how their systems handle personal data, and for the ripple effects on the individuals behind those data points.[45]

Yet even perfect legislation must reckon with AI's built-in quirks: permanent memory and the knack for piecing together profiles from scraps of information.[46] The RTBF, as framed in the GDPR, leans on human metaphors of forgetting, metaphors that collide head-on with how AI actually works. Full deletion or anonymization sounds tidy on paper, but wait, AI's regenerative memory makes it nearly unachievable ! This stark mismatch exposes a widening gulf between

[42] See Recital 65 GDPR.

[43] See the CJEU's *Google Spain* and *GC v CNIL* cases as jurisprudential pillars of this principle.

[44] See: *"The underlying technology of ChatGPT, a large language model (LLM), is trained on vast amounts of data, potentially including sensitive personal information."* Xukang Wang and Ying Cheng Wu, 'Balancing Innovation and Regulation in the Age of Generative Artificial Intelligence' (2024) 14 *Journal of Information Policy* <https://doi.org/10.5325/jinfopoli.14.2024.0012> accessed 10 January 2025

[45] Sakiko Fukuda-Parr *et al*, 'Emerging Consensus on Ethical AI: A Human-Rights Critique of Stakeholder Guidelines' (2021) 12 *Global Policy* 32 <https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.12965> accessed 10 January 2025

[46] Francesco Paolo Levantino, 'Generative and AI-Powered Oracles: "What Will They Say about You?"' (2023) 51 *Computer Law & Security Review* 105898 <https://doi.org/10.1016/j.clsr.2023.105898> accessed 10 January 2025

the EU's data-protection ideals and the technological realities on the ground. [47]

The RTBF needs reimagining as a broader right rooted in personal informational self-determination.[48] The sheer technical and economic hurdles of scrubbing data from sprawling AI models threaten the very privacy-centric pillars of digital constitutionalism. It's time for a more flexible oversight regime, one capable of policing *"personhood-less"*[49] AI without sacrificing core rights.

D. Autonomous AI and Liability: Unresolved Questions in Tort and Criminal Law

The march of autonomous AI forces (and shall do so even more heavily in the upcoming years) lawyers and ethicists to revisit familiar legal doctrines. Our present tort law and criminal law rules were built for human agents, not code that learns on its own ! Some voices suggest granting AI legal personhood so it can carry liability, yet, that leap feels premature: these AI systems (although can be quite clever) lack moral agency, contextual judgment, and the critical reasoning we -Jurists- usually tie to legal personhood.[50]

Crucially, AI's pattern-spotting prowess is not a genuine human thought, surprisingly, a point even the once-swaggering tech sector now concedes. Equating the two would muddy accountability and cloud serious debate over AI legal personhood.[51] Moreover, sewing a cloak of personhood onto algorithms raises ethical and doctrinal puzzles that stray far from traditional culpability.[52] The possibility of prosecuting a robot, along with the applicable mens rea[53] doctrine and the sanctions that might follow[54]merits careful analysis.

We today witness how Autonomous-vehicle mishaps bring the problem into sharp relief. Today's rules cannot cleanly allocate blame among developers, operators, and end-users,

[47] Eduard Fosch Villaronga, Peter Kieseberg and Tiffany Li, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2018) 34 *Computer Law & Security Review* 304–318 <https://scholarship.law.bu.edu/faculty_scholarship/817/> accessed 10 January 2025

[48] Cheng-Chi Chang, 'When AI Remembers Too Much: Reinventing the Right to Be Forgotten for the Generative Age' (2024) 19 *Washington Journal of Law, Technology & Arts* 23 <https://digitalcommons.law.uw.edu/wjlta/vol19/iss3/2/> accessed 10 January 2025

[49] *Reference here is made to AI still lacking legal personhood.*

[50] Brandeis Marshall, 'No Legal Personhood for AI' (2023) 4 *Patterns* 100861 <https://doi.org/10.1016/j.patter.2023.100861> accessed 10 January 2025

[51] *Ibid.*

[52] Mireille Hildebrandt, 'Legal Personhood for AI?' in *Law for Computer Scientists and Other Folk* (OUP 2019) <https://www.researchgate.net/publication/343161002_Legal_Personhood_for_AI> accessed 10 January 2025

[53] Paul H Robinson, 'Mens Rea' (2002) 151 *University of Pennsylvania Law Review* 29 <https://scholarship.law.upenn.edu/faculty_scholarship/34> accessed 10 January 2025

[54] Monika Simmler and Nora Markwalder, 'Guilty Robots? Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence' (2018) 29 *Criminal Law Forum* 1 <https://doi.org/10.1007/s10609-018-9360-0> accessed 10 January 2025

leaving courts to improvise.[55] We urgently need to decide whether an autonomous system acts as an independent wrongdoer or merely extends its human handlers.[56] Until that question is settled, liability in the age of self-directing AI will remain a moving target.

Notably, the European Parliament's resolution of 16 February 2017[57] marked the first regulatory foothold in this arena, setting out non-binding recommendations on civil-law rules for robotics and broader AI governance. It's an excellent start. Likewise, on 28 September 2022, the European Commission unveiled its proposal for an Artificial Intelligence Liability Directive, adapting existing non-contractual civil-liability rules to cover harm caused by artificial-intelligence systems and their use.[58]

Persistent uncertainty surrounds how best to classify robot autonomy: whether it can be accommodated within existing legal categories or whether it demands an entirely new AI-specific liability framework.[59] Current developments increasingly indicate that novel legal rules will be required to resolve these unprecedented dilemmas.

E. AI and the Surveillance State

The fusion of AI technologies with governmental surveillance has sparked deep worries about privacy erosion, the contested legality of biometric policing under Directive (EU) 2016/680,[60] and the ever-present risk of authoritarian overreach that we can't deny. Even within the EU, these smart tools are now undeniably stress-testing the core of the European digital constitutionalism project, which originally aims to shield fundamental rights and keep state power in check in the digital age.

[55] Shreyansh Upadhyay, 'Navigating Liability in Autonomous Robots: Legal and Ethical Challenges in Manufacturing and Military Applications' *The Yale Review of International Studies* (17 March 2021) <https://yris.yira.org/column/navigating-liability-in-autonomous-robots-legal-and-ethical-challenges-in-manufacturing-and-military-applications/> accessed 10 January 2025

[56] Priyanka Majumdar, Bindu Ronald and Rupal Rautdesai, 'Artificial Intelligence, Legal Personhood and Determination of Criminal Liability' (2019) 6(6) *Journal of Critical Reviews* 323–330 <https://www.researchgate.net/publication/383994634_Artificial_Intelligence_Legal_Personhood_and_Determination_of_Criminal_Liability> accessed 10 January 2025

[57] European Parliament, 'Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))' [2017] OJ C 252/239 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2017:252:TOC> accessed 10 January 2025

[58] European Commission, *Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)* COM (2022) 496 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496> accessed 10 January 2025

[59] Pin Lean Lau, 'The Extension of Legal Personhood in Artificial Intelligence' (2019) 46 *Revista de Bioética y Derecho* 47–66 <https://revistes.ub.edu/index.php/RBD/article/view/27064> accessed 10 January 2025

[60] See Article 4(1)(b) of the Directive (EU) 2016/680 on the processing of personal data by competent authorities for the purposes of law enforcement. *(applies to competent authorities only)* <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng> accessed 10 January 2025

Empirical studies on predictive policing in South Africa for example shows that AI driven systems, while they can be efficient, they most importantly really magnify algorithmic bias[61] against already marginalised groups.[62] Another striking example, that comes from the United States of America, where we notice a growing dependence on algorithmic tools in urban policing, and that is being criticised for reshaping notions of *"reasonable suspicion"* and undermining long-standing legal standards.[63]

Even inside the EU, the *"world human rights legislator-in-chief"*, Clearview AI (a facial-recognition platform that scrapes images from the web) was fined 20 million euros by France's CNIL for unlawful personal-data processing and for ignoring data-subject rights.[64]

Globally, authoritarian exporters (China foremost) normalise AI-powered surveillance, demonstrating how such tech can cement repression.[65]

Democratic backsliding can also unfold in liberal democracies like the USA or France when AI surveillance spreads unchecked.[66] Examples of Suites such as PredPol and Palantir[67] [68] have already jeopardised privacy and fundamental rights, both pillars of the EU's digital-constitutionalism vision and the Charter of Fundamental Rights of the European Union

[61] See definition: *" "Algorithmic discrimination" occurs when automated systems contribute to unjustified different treatment or impacts disfavoring people based on their race, color, ethnicity, sex …, religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law. Depending on the specific circumstances, such algorithmic discrimination may violate legal protections."*
The White House, *Blueprint for an AI Bill of Rights* (Office of Science and Technology Policy, 2022) <https://www.whitehouse.gov/ostp/ai-bill-of-rights/> accessed 10 January 2025

[62] Singh, 'Policing by Design: Artificial Intelligence, Predictive Policing, and Human Rights in South Africa' (2022). <https://journals.co.za/doi/full/10.10520/ejc-ajcj_v7_n1_a7> accessed 10 January 2025

[63] Gandy, 'The Algorithm Made Me Do It!' IAMCR (2019). <https://www.asc.upenn.edu/sites/default/files/2021-03/%22The%20Algorithm%20Made%20Me%20Do%20It!%20Predictive%20Policing,%20Cameras,%20Social%20Media%20and%20Affective%20Assessment.%22%20IAMCR%202019..pdf> accessed 10 January 2025

[64] European Data Protection Board, 'French SA fines Clearview AI EUR 20 million' (EDPB, 2022) <https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en> accessed 10 January 2025

[65] Feldstein, 'The Global Expansion of AI Surveillance' Carnegie Endowment for International Peace (2019). <https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en> accessed 10 January 2025

[66] Peterson and Hoffman, 'Geopolitical Implications of AI and Digital Surveillance Adoption' (2022). <https://www.brookings.edu/wp-content/uploads/2022/06/FP_20220621_surveillance_exports_peterson_hoffman_v2.pdf> accessed 10 January 2025

[67] Castets-Renard, 'Human Rights and Algorithmic Impact Assessment for Predictive Policing' (2019). <https://www.cambridge.org/core/books/constitutional-challenges-in-the-algorithmic-society/human-rights-and-algorithmic-impact-assessment-for-predictive-policing/A68760BA3304664CC15C1BE7FC5CCD73> accessed 10 January 2025

[68] Rashida Richardson, Jason Schultz and Kate Crawford, 'Dirty Data, Bad Predictions: How Civil-Rights Violations Impact Police Data, Predictive-Policing Systems and Justice' (2019) *NYU Law Review Online* <https://papers.ssrn.com/abstract=3333423> accessed 10 January 2025

(CFR).[69]

Taken together, these non-EU instances foreshadow challenges the Union must anticipate. Transplanting opaque, AI-driven policing models (plagued by the *black-box* problem) would jar with the EU's commitment to transparency and accountability on human-rights[70] and data-protection[71] grounds. One promising safeguard, often highlighted in the literature, is the algorithmic impact assessment (AIA):[72] mandatory ex-ante AIAs (as proposed in the draft AI Act) or voluntary transparency reports could secure human-rights protections. This approach dovetails with the EU's *"Ethics Guidelines for Trustworthy AI,"*[73] which call for accountability and strong risk-mitigation in AI applications.

The EU's digital constitutionalism framework must seek to counter such risks by promoting AI regulation models that uphold democratic values, distinguishing itself from authoritarian approaches through strict regulation and oversight of AI when used in surveillance and policing.[74] The EU's legislative initiatives, such as the proposed AI Act, exemplify its leadership in creating a normative framework that balances innovation with human rights protection.[75] The AI Act's near-total ban[76] on real-time facial recognition in public spaces exemplifies how the EU is upholding its digital-constitutionalism principles[77].

F. Fault Lines in the EU Digital Constitutionalism: Why the Present EU digital constitutionalism Framework Cannot Regulate AI?

Artificial intelligence has exposed deep fissures in the European Union's project of "digital constitutionalism", as shown by the effort to extend constitutional safeguards into the digital realm. Although laudable in scope, the existing framework of European digital constitutionalism cannot keep pace with AI's speed, opacity, and global reach. This section

[69] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

[70] See Articles 7–8 of the Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

[71] See Recital 71 of the Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1.

[72] *AIAs are systematic evaluations of an AI system's effects on fundamental rights.* For more see: Daniel Reisman *et al*, 'Algorithmic Impact Assessments: A Practical Framework for Public Agency' (*AI Now Institute Report*, 2018) <https://ainowinstitute.org/wp-content/uploads/2023/04/aiareport2018.pdf> accessed 10 January 2025

[73] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (2019). <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 10 January 2025

[74] *Ibid.*

[75] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [2024] OJ L 168/1

[76] *Given that the AI Act's real-time FR ban has carve-outs (terrorism, child abduction).*

[77] European Parliament, 'Artificial Intelligence Act: MEPs adopt landmark law' (8 March 2024) <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law> accessed 10 January 2025

explains why. It identifies structural weaknesses: the limits of proportionality review, a state-centric view of power, the rights-versus-innovation dilemma, regulatory fragmentation, slow law-making and the clash between EU digital sovereignty and multinational tech giants. Pinpointing these flaws sets the stage for re-thinking constitutional theory and crafting more agile regulatory tools that can protect fundamental rights in an AI-driven world.

Firstly, Proportionality, long the EU's touchstone for balancing legitimate regulatory aims against rights intrusions, now complicates AI governance. The draft AI Act's risk-based model requires *"risk levels [to] be assessed at various levels and by various actors … [and] are essentially context-dependent,"* generating divergent classifications and eroding legal certainty.[78] Conceptually, proportionality *"relativizes rights,"* forces incommensurable values onto a utilitarian scale, and may justify sacrificing core liberties for aggregate welfare gains.[79] In practice, the doctrine pushes regulators onto a tension: strict ex-ante controls risk chilling innovation, while lenient standards leave high-impact systems unchecked. Until proportionality is anchored by hard safeguards, such as mandatory AIAs, the EU's digital constitutionalism project will remain vulnerable to AI's scale, opacity and velocity.

Secondly, the EU's digital constitutionalism model privileges public-law controls, yet AI governance is increasingly shaped by private platforms whose quasi-sovereign power escapes traditional state-centric tools.[80] This mismatch leaves enforcement gaps precisely where high-impact systems are deployed. Compounding the problem, divergent national transpositions of EU directives produce a patchwork of standards: identical AI applications may be lawful in Bruxelles, contested in Paris, and unreviewed in Rome, undermining legal certainty

[78] Mahler, T. 'Between risk management and proportionality: The risk-based approach in the EU's Artificial Intelligence Act Proposal.' (2021). Nordic Yearbook of Law and Informatics. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4001444> accessed 10 January 2025

[79] Czarnocki, J. 'Between Rights, Interests, and Risk-The Role of the Proportionality Balancing in the EU Digital Law. Interests, and Risk-The Role of the Proportionality Balancing in the EU Digital Law (February 20, 2024). https://law.stanford.edu/publications/no-83-between-rights-interests-and-risk-the-role-of-the-proportionality-balancing-in-the-eu-digital-law/> accessed 10 January 2025

[80] Ochigame, R. 'The invention of 'ethical AI': How big tech manipulates academia to avoid regulation.' Economies of virtue, 49 (2019). https://mediarep.org/bitstream/handle/doc/20441/TOD_46_Phan_2022_Economies-of-Virtue_.pdf> accessed 10 January 2025

and equal protection.[81] Although the 2018 Coordinated Plan on AI[82] aims to align Member-State approaches, political discretion and uneven administrative capacity still foster fragmentation[83]. Finally, the Union's quest for "digital sovereignty" collides with the extraterritorial reach of multinational tech firms, whose data flows, cloud infrastructures and algorithmic models remain anchored outside EU jurisdiction.[84] Together, these state-private, intra-EU and transnational frictions obstruct a coherent response to AI's risks and dilute the protective ambitions of EU digital constitutionalism.

Thirdly, legislative inertia compounds these structural deficits. The ordinary legislative procedure (requiring trilogue negotiation, multilingual drafting, and national transposition) moves far more slowly than AI innovation cycles. By the time an instrument such as the AI Act nears adoption, underlying models have evolved, new risks have surfaced, and industry norms have shifted. This temporal lag produces regulatory obsolescence, widens enforcement gaps, and weakens the EU's capacity to uphold digital-constitutionalism guarantees in real time.[85]

In sum, the Union's digital constitutionalism project stands at an inflection point. Unless it transcends proportionality's indeterminacy, recalibrates its state-centric lens to confront private algorithmic power, streamlines legislative timetables, and welds fragmented national regimes into a genuinely pan-European architecture, the gap between AI's disruptive capacities and the EU's law protective reach will continue to widen. A next-generation framework, anchored in

[81] *An example of a national policy is that of France. In January 2020, French National Assembly deputy Pierre-Alain Raphan proposed a Charter for Artificial Intelligence and Algorithms (Charte de l'intelligence artificielle et des algorithmes), which was subsequently referred to the Parliamentary Committee on Constitutional Legislation. The authors of the project suggested that the Charter be referenced in the French Constitution's preamble and that fundamental issues be enshrined within it.* Alqodsi, Enas Mohammed, and Dmitry Gura. 'High tech and legal challenges: Artificial intelligence-caused damage regulation.' Cogent Social Sciences 9.2 (2023): 2270751. <https://www.tandfonline.com/doi/abs/10.1080/23311886.2023.2270751> accessed 10 January 2025

[82] European Commission (2018b) Coordinated plan on artificial intelligence. Communication COM (2018) 795 final. Brussels 7.12.2018.

[83] Ulnicane, Inga. 'Artificial Intelligence in the European Union: Policy, ethics and regulation.' The Routledge handbook of European integrations. Taylor & Francis, 2022. <https://www.researchgate.net/publication/359721509_Artificial_intelligence_in_the_European_Union_Policy_ethics_and_regulation> accessed 10 January 2025

[84] Cyman, Damian, Elizaveta Gromova, and Edvardas Juchnevicius. 'Regulation of artificial intelligence in BRICS and the European Union.' Brics law journal 8.1 (2021): 86-115. <https://www.bricslawjournal.com/jour/article/view/452?locale=en_US> accessed 10 January 2025

[85] See: *"At present, the few existing laws are being resorted to in order to judicially settle damages caused by AI-supported products and services. While cases are multiplying, the legislative branch seems to be moving at a negligible speed compared to technological advancements."*
Patricia Almeida, Carlos Santos and Josivania Silva Farias, 'Artificial Intelligence Regulation: A Meta-Framework for Formulation and Governance' (2020). <https://scholarspace.manoa.hawaii.edu/bitstreams/261a0c41-b149-4f55-9297-33c3e57d14e1/download> accessed 10 January 2025

hard ex-ante safeguards[86], mandatory algorithmic-impact assessments, and robust transnational enforcement, offers the most credible path toward restoring coherence and ensuring that technological progress remains tethered to the Union's foundational commitment to digital fundamental rights.

2. Emerging AI regulation: the future of the EU's Digital Constitutionalism Model

Public policies on artificial intelligence often focus on three main objectives: fostering the growth of local AI industries, addressing and mitigating economic challenges and unemployment caused by AI.[87] This section takes a different approach by shifting the focus to regulatory frameworks and emerging models of AI governance. Building on the limitations discussed in the previous chapter, it sets aside the economic and technological dimensions explored elsewhere to delve into how regulation can actually evolve. The discussion begins with an analysis of the EU's groundbreaking AI Act, followed by an exploration of radical and forward-thinking theories of AI regulation. The section sets the base for recommendations of an AI regulation framework that the EU should adopt to ensure continually upholding its digital constitutionalism principles while fostering AI innovation.

A. From Blueprint to Bottleneck: Strengths and Limits of the EU Artificial Intelligence Act

The European Union Artificial Intelligence Act (hereafter EU AI Act[88]), adopted in 2024, marks a groundbreaking step as the first horizontal[89], binding regulation on AI worldwide. Designed with a risk-based approach, the Act categorizes AI systems by risk levels, aiming to balance innovation with the protection of fundamental rights. The EU AI Act introduces the world's first comprehensive, risk-tiered framework for AI. Systems are classified along a four-level continuum: *unacceptable-risk* applications, such as social scoring, manipulative subliminal tools, and most real-time biometric identification, are banned outright. *High-risk* systems such as credit-scoring, critical-infrastructure control, law-enforcement analytics face stringent ex-ante duties on developers, including risk-management, data governance, human oversight, and conformity assessment obligations. *Limited-risk* tools, such as chatbots and deep-fake

[86] See Articles 16–23 of the draft AI Act.

[87] Barrio Andrés, Moisés. 'Towards legal regulation of artificial intelligence.' Revista IUS 15.48 (2021): 35-53. <https://revistaius.com/index.php/ius/article/view/661/856> accessed 10 January 2025

[88] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [2024] OJ L1689/1.

[89] *Horizontal regulation encompasses all AI applications across every sector, whereas vertical regulation is confined to a specific AI application or sector. See :* Holistic AI, 'Regulating AI: The Horizontal vs Vertical Approach' (Holistic AI, n.d.) <https://www.holisticai.com/blog/regulating-ai-the-horizontal-vs-vertical-approach> accessed 10 January 2025

generators, must merely disclose their AI nature; and finally, the *minimal-risk* uses that remain unregulated, although they still trigger general product-safety rules.[90]

The Act also crafts bespoke rules for *General-purpose* AI[91] models: all providers must publish training-data summaries and respect copyright, while *"systemic-risk"* models[92], as defined by compute thresholds, must undergo adversarial testing, incident reporting, and AI-Office supervision. Most compliance burdens fall on providers, though professional deployers of *high-risk* systems also assume defined responsibilities.[93] Furthermore, to support innovation, the Act introduces regulatory sandboxes,[94] offering controlled environments for developing and testing AI systems while ensuring compliance with the established framework.[95]

The EU AI Act has faced a chorus of critiques, and the themes are hard to miss: rigid taxonomy, hefty economic drag, nagging procedural gaps, and glaring socio-political blind spots.

Taxonomy matters because a static risk map (despite Article 7's "dynamic update") struggles to keep pace with AI's rapid evolution. New models emerge, legacy categories quickly become inadequate, and novel hazards slip through the gaps, leaving the very citizens the Act intends to protect most exposed.[96] Scholars add that the Act's technocratic, risk-first scaffolding overlooks broader social fallout: while the text lists "high-risk" use cases, it gives scant attention to systemic threats to democratic debate, media pluralism, and distributive justice.[97] Governing what many call *"an incredibly powerful and complex phenomenon"* with little more

[90] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [2024] OJ L1689/1.

[91] *Ibid. See Article 3 (63)* of the AI Act

[92] *Ibid. See Article 3 (65)* of the AI Act

[93] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [2024] OJ L1689/1.

[94] *"Regulatory sandboxes generally refer to regulatory tools allowing businesses to test and experiment with new and innovative products, services or businesses under supervision of a regulator for a limited period of time."* Madiega, T., & Van De Pol, A. L. (2022). Artificial intelligence act and regulatory sandboxes. *European Parliamentary Research Service*, 6. <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf> accessed 10 January 2025

[95] European Parliamentary Research Service, 'Artificial Intelligence Act' (Briefing) PE 733.544, March 2022. 'Artificial intelligence act and regulatory sandboxes' <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf> accessed 10 January 2025

[96] Finocchiaro, Giusella. 'The regulation of artificial intelligence.' *AI & SOCIETY* 39.4 (2024): 1961-1968. <https://cris.unibo.it/retrieve/5eb315d2-5f34-47fe-9394-5fda4980ee5e/The%20regulation%20of%20artificial%20intelligence.pdf> accessed 10 January 2025

[97] Nicoletta Rangone and Luca Megale, 'Risks without rights: The EU AI Act's approach to AI in law and rulemaking' (n.d.) European Journal of Risk Regulation <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risks-without-rights-the-eu-ai-acts-approach-to-ai-in-law-and-rulemaking/3AD4822C291C6591BAFD26524CD44C12> accessed 10 January 2025

than technical conformity check-lists, feels woefully inadequate when confronted with AI-propelled disinformation or election meddling.[98]

The Act loads firms with thick layers of paperwork, documentation, certification, and constant monitoring.[99] As supported by literature, small and medium enterprises (SMEs)[100] strain under these obligations, even when they opt for the "*lighter documentation track"* or the "*Innovation Package*."[101] Unlike deep-pocketed multinationals, these lean teams confront steep financial and operational hurdles that can blunt the very innovation the sector needs.[102]

Another significant issue lies in the Act's heavy emphasis on procedural safeguards and risk management. While these measures are undoubtedly necessary, the framework offers individuals virtually no avenue to contest opaque, black-box decisions or obtain meaningful redress. It lacks the robust liability provisions and enforcement mechanisms needed to remedy real-world harms.[103]

Scholars warn that such costs may erode Europe's competitive edge. Compliance alone could shave AI investment in the EU by up to 20 percent over five years.[104] This matters because capital is likely to gravitate toward jurisdictions with lighter regulatory burdens, thereby weakening Europe's competitive position in the global AI race.[105]

Transparency rules tell the same story. High-risk systems must file documentation and user-facing explanations, yet the Act offers no scalable way to make those explanations intelligible or context-specific. Opaque algorithmic choices will persist, leaving regulators frustrated and affected people in the dark.[106] Equally salient is the Act's silence on training-data

[98] Mauro Fragale and Valentina Grilli, 'Deepfake, deep trouble: The European AI Act and the fight against AI-generated misinformation' (Columbia Journal of European Law, Preliminary Reference 2024). <https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/> accessed 10 January 2025

[99] *Ibid.*

[100] European DIGITAL SME Alliance, 'DIGITAL SME Position Paper on the Artificial Intelligence Act' (Position Paper, 2021) <https://www.digitalsme.eu/policy/> accessed 10 January 2025

[101] *See Article 72*, EU AI Act.

[102] Finocchiaro, Giusella. 'The regulation of artificial intelligence.' AI & SOCIETY 39.4 (2024): 1961-1968. <https://cris.unibo.it/retrieve/5eb315d2-5f34-47fe-9394-5fda4980ee5e/The%20regulation%20of%20artificial%20intelligence.pdf> accessed 10 January 2025

[103] *Ibid.*

[104] Mueller B, 'How Much Will the Artificial Intelligence Act Cost Europe?' (Center for Data Innovation, July 2021) <https://itif.org/publications/2021/07/26/how-much-will-artificial-intelligence-act-cost-europe/> accessed 10 January 2025

[105] Finocchiaro, Giusella. 'The regulation of artificial intelligence.' AI & SOCIETY 39.4 (2024): 1961-1968. <https://cris.unibo.it/retrieve/5eb315d2-5f34-47fe-9394-5fda4980ee5e/The%20regulation%20of%20artificial%20intelligence.pdf> accessed 10 January 2025

[106] Nicoletta Rangone and Luca Megale, 'Risks without rights: The EU AI Act's approach to AI in law and rulemaking' (n.d.) European Journal of Risk Regulation.

erasure. By not reconciling model development with privacy guarantees (most notably the GDPR's RTBF, which is often technically infeasible in machine-learning contexts[107]) the legislation leaves a doctrinal gap.

Liability is another unresolved frontier. The Act emphasizes ex-ante risk controls yet says little about ex-post accountability when self-learning systems behave unpredictably. In the absence of the shelved AI Liability Directive,[108] victims may struggle to identify a responsible defendant under existing tort or criminal norms.[109]

Finally, although Chapter II[110] prohibits certain biometric and manipulative practices, some of its carve-outs and narrow definitions fall short of a comprehensive safeguard against an AI-enabled surveillance state.[111]

Together, these critiques suggest that this AI regulatory attempt cannot, by itself, secure the Union's broader digital constitutionalism objectives.Bridging its gaps will demand additional tools and more radical regulatory models that are lighter for smaller actors, agile enough for rapid innovation, and equipped with robust redress and accountability mechanisms. The next sections examine these "second-generation" regulatory proposals, which aim to refine and extend the Act's pioneering blueprint.

B. "Prudential Algorithmic Regulation": Embedding Ex-Ante Testing and Ongoing Audits

Recent scholarship recasts algorithmic regulation as a dual enterprise: algorithms are both regulatory tools and regulated objects. Fortes, Baquero & Restrepo[112] trace this to *Lessig's*

<https://www.researchgate.net/publication/389830238_Risks_Without_Rights_The_EU_AI_Act's_Approach_to_AI_in_Law_and_Rule-Making> accessed 10 January 2025

[107] Villaronga, E. F., Kieseberg, P., & Li, T. 'Humans forget, machines remember: Artificial intelligence and the right to be forgotten.' *Computer Law & Security Review*, *34*(2), 304-313. (2018). <https://scholarship.law.bu.edu/faculty_scholarship/817/> accessed 10 January 2025

[108] European Parliament, 'AI Liability Directive' (Legislative Train, A Europe fit for the Digital Age) <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-ai-liability-directive> accessed 10 January 2025

[109] *Note the forthcoming revision of the 'Product Liability Directive', (COM (2023) 495) that expands the scope of liability to digital products (including AI systems).*
Latham & Watkins LLP, 'New EU Product Liability Directive Comes Into Force' (Latham & Watkins LLP, n.d.) <https://www.lw.com/en/offices/admin/upload/SiteAttachments/New-EU-Product-Liability-Directive-Comes-Into-Force.pdf> accessed 10 January 2025

[110] See *Chapter II: Prohibited AI Practices*, EU AI Act. <https://artificialintelligenceact.eu/chapter/2/> accessed 10 January 2025

[111] Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States and Beyond' (2023) 26 *Yale Journal of Law & Technology* 671 <https://yjolt.org/sites/default/files/wachter_26yalejltech671.pdf> accessed 10 January 2025

[112] Pedro Rubim Borges Fortes, Pablo Marcello Baquero, and David Restrepo Amariles 2, 'Artificial Intelligence Risks and Algorithmic Regulation' European Journal of Risk Regulation (2022), 13, 357–372 <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/artificial-intelligence-risks-and-algorithmic-regulation/433B0044369D4389044E58232C7613C4> accessed 10 January 2025

“code is law”[113] insight, arguing that mathematical instructions already embed normative commands. Their model centers on a *prudential test*: before an automated decision-system is deployed in sensitive domains (credit, immigration, sentencing) it must demonstrate, through empirical trials, that its predictions are evidence-based, explainable and contestable. Continuous third-party audits then monitor drift and bias.[114] The approach’s strength lies in harnessing algorithms for self-monitoring while imposing transparency duties that expose discriminatory features. Yet two vulnerabilities persist. First, *“algorithmic neutrality”* is illusory,[115] bias can re-enter through training data or feature selection. Second, the framework still lacks hard enforcement levers: without statutory audit mandates or sanctioning powers, compliance may remain aspirational.[116]

C. UN-Centric Ethical Frameworks as an AI regulation

Eleonore Fournier-Tombs[117] proposes that the United Nations adopt a binding internal regulation for artificial intelligence, filling the normative gaps left by the EU AI Act, whose obligations do not extend to international organizations.

The proposed regulation would first align UN practice with the EU’s risk taxonomy by explicitly listing prohibited and high-risk applications, then require any high-risk system to secure FDA-style pre-authorization based on documented risk-management plans, data-governance audits, human-oversight guarantees, and post-deployment monitoring.

It would translate existing soft-law instruments, such as the UNESCO’s draft *Recommendation on the Ethics of AI,*[118] into binding organizational rules, thereby transforming ethical guidance into enforceable obligations, and in doing so create a transparent approval pathway that both

[113] Lawrence Lessig, *Code and Other Laws of Cyberspace* (2nd edn, Basic Books 2009)

[114] *Ibid.*

[115] *“Neutrality is the unconditional absence of bias... . Algorithmic neutrality cannot exist when the training data is human data, as bias is intrinsically human, and human bias cannot be eliminated, only reduced.”*
Morris DL and Taylor R, 'A Critical Data Ethics Analysis of Algorithmic Bias and the Mining/Scraping of Heirs’ Property Records' (IGI Global, 2023) <https://www.igi-global.com/dictionary/a-critical-data-ethics-analysis-of-algorithmic-bias-and-the-miningscraping-of-heirs-property-records/123126> accessed 10 January 2025

[116] Mireille Hildebrandt, ‘Algorithmic Regulation and the Rule of Law’ (2018) 376 *Philosophical Transactions of the Royal*
Society A 2128 <https://royalsocietypublishing.org/doi/10.1098/rsta.2017.0355> accessed 10 January 2025

[117] Eva Fournier-Tombs, ‘Towards a United Nations Internal Regulation for Artificial Intelligence’ (2021) *Big Data &*
Society <https://www.researchgate.net/publication/354233951_Towards_a_United_Nations_Internal_Regulation_for_Artificial_Intelligence> accessed 10 January 2025

[118] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*
(adopted 23 November 2021) <https://www.unesco.org/en/ethics/artificial-intelligence><https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence> accessed 10 January 2025

reduces developers' uncertainty and signals to member states and affected populations that UN-deployed AI satisfies robust safety and fundamental-rights standards.

Strengths of this regulation model include coherence with the Sustainable Development Goals and the potential to trigger a *"Geneva Effect,"* exporting UN standards much as the EU exports its own. However, some limitations will remain, such as adoption that would be voluntary for specialized agencies, the overlap with regional regimes that could cause redundancy, and the enforcement that would rely on internal compliance offices rather than external courts.

Still, by coupling treaty-level ethics with *FDA-style* pre-clearance, a UN Internal AI Regulation could harmonies disparate initiatives (such as the *OECD's Recommendations on AI*[119], the Council of Europe's *AI Convention*[120], the G7's *AI Code of Conduct*[121]) and provide a global floor for high-risk humanitarian AI, that can only further help the EU's digital constitutionalism objectives.

D. "AI Governance Meta-Framework": A Layered Roadmap from Principles to Enforcement

Drawing on a systematic review of 51 scholarly proposals, Almeida et al.[122] construct a meta-framework for Artificial Intelligence Regulation (AIR) that stitches together the entire policy cycle (agenda-setting, rule-making, certification, supervision and iterative reform) into a single, modular architecture. The model is organized along three interlocking layers: *technology* (data quality, model architecture, transparency tools such as XAI), *social impact* (stakeholder and labor-market assessments) and *governance* (legislative mandates, agile regulatory agencies and judicial oversight). By mapping 15 existing frameworks (from *"society-in-the-loop"* ethics[123] to agile soft-law sandboxes) onto this scaffold, the authors offer

[119] See Organisation for Economic Co-operation and Development, *OECD AI Principles* (2019) https://oecd.ai/en/ai-principles accessed 10 January 2025 and Yeung, K. 'Recommendation of the council on artificial intelligence (OECD).' International legal materials, 59(1), 27-34. (2020). <https://www.researchgate.net/publication/339879755_Recommendation_of_the_Council_on_Artificial_Intelligence_OECD> accessed 10 January 2025

[120] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (opened for signature 2024) <https://rm.coe.int/ai-convention-brochure/1680afaeba> accessed 10 January 2025

[121] White & Case, 'AI Watch: Global Regulatory Tracker - G7' (White & Case Insight, 2024) <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-g7> accessed 10 January 2025

[122] Almeida, P. G. R., et al., 'Meta-Framework for AI Regulation' Proceedings of the 53rd Hawaii International Conference on System Sciences (2020). <https://www.researchgate.net/publication/339025965_Artificial_Intelligence_Regulation_A_Meta-Framework_for_Formulation_and_Governance> accessed 10 January 2025

[123] Iyad Rahwan, 'Society-in-the-Loop: Programming the Algorithmic Social Contract' (2018) 20 *Ethics and Information Technology* 5–14 <https://doi.org/10.1007/s10676-017-9430-8> accessed 10 January 2025

a common vocabulary and a step-wise process that jurisdictions can tailor to their own risk tolerances and institutional capacities.[124] Its chief virtue is inclusivity and multistakeholder approach: legislators, regulators, industry and civil society are assigned explicit roles, enabling cross-disciplinary collaboration and gradual, feedback-driven rule-tightening. Yet the framework's breadth is also its weakness: without specified sanctioning mechanisms or binding timelines, implementation may stall, and consensus across divergent legal cultures remains uncertain. Still, as a synthesis of dispersed scholarship, the AIR meta-framework provides a credible blueprint for converging global AI governance debates.

E. Continuum of AI Governance: From Corporate Self-Structuring to Public Command in AI Regulation.

Hoffmann-Riem[125] maps a continuum of governance modes that together form the current regulatory mosaic for artificial intelligence. At one end lies *self-structuring*, where firms unilaterally shape their own AI design and compliance processes through internal policies or engineering choices. More *formalized company self-regulation* follows, exemplified by industry codes or de-facto technical standards that gain market authority. When such private rules operate under public auspices (through statutory incentives, accreditation, or liability offsets) they become *regulated self-regulation*, as illustrated by GDPR-style codes of conduct, certification schemes, and data-protection seals. A further step is *hybrid regulation*, in which public bodies co-draft or formally recognize private standards, an example would be the sector-specific AI audits that typify this collaborative model. Finally, *classical state regulation* supplies mandatory, enforceable norms (e.g., GDPR, cybersecurity statutes) and direct supervisory powers that close gaps left by softer instruments. Across all layers, techno-regulatory tools, embedded design requirements, default settings, and algorithmic audits, are gaining prominence, signaling a shift from purely textual rules to *"code-based enforcement"*, and thus further confirming that in the future, *Code is indeed Law*. Together, these overlapping mechanisms that create a Continuum of AI Governance, underscore the need for adaptable, multi-tiered strategies capable of matching AI's transnational scale and rapid evolution.

F. AIA's risk-based regulation with an IPCC's risk assessment integration.

[124] *Ibid.*

[125] Hoffmann-Riem, Wolfgang. 'Artificial intelligence as a challenge for law and regulation.' Regulating artificial intelligence (2020): 1-29. <https://link.springer.com/chapter/10.1007/978-3-030-32361-5_1> accessed 10 January 2025

The AIA's[126] risk-based regulation adopts a dynamic, scenario-driven approach that significantly improves upon the current EU AI Act's static risk categorization. Rather than assigning risk solely on broad application fields, the proposed model evaluates each AI system based on detailed risk scenarios. This approach integrates multiple determinants (hazard, exposure, vulnerability, and response) drawing inspiration from frameworks used in climate change risk assessment by the IPCC (Intergovernmental Panel on Climate Change)[127]. By mapping how risks overlap (aggregating, compounding, even cascading), this model mirrors AI's messy reality far better than a rigid checklist ever could. This is important because Robert Alexy's *proportionality test*[128] then steps in, quantifying the trade-off between an AI system's deployment and any blow to fundamental rights. Regulators can ask: is the cost of mitigation wildly out of line with the risk reduction? If so, safeguards are trimmed; if not, they're reinforced, matching legal armour to actual harm. Compare that with the current EU AI Act, which teeters between over-regulating and under-regulating fast-moving technologies. An enhanced, genuinely risk-tuned approach would foster legal certainty, keep compliance affordable, and still spur innovation. Most crucially, it ties regulatory weight to real-world impact, ensuring SMEs aren't smothered by red tape while Europe's core values[129] stay fully protected.

G. An "Algorithmic Safety Agency" Model: Pre-Market Approval for High-Risk AI

Andrew Tutt's 2017 proposal for an "FDA for Algorithms"[130] reframes AI governance around a public-health paradigm. Drawing an explicit analogy to drug and medical-device regulation, Tutt argues that certain "complex and dangerous" algorithms should not reach the market until an expert, politically independent agency certifies their safety and efficacy. The envisioned Algorithmic Safety Agency would (i) classify algorithms by complexity and risk, (ii) issue technical and design standards, and (iii) require evidence-based pre-market trials for high-risk systems, thereby preventing unacceptable harms without stifling innovation. Tutt contends that

[126] Novelli, Claudio, et al. 'AI Risk Assessment: A Scenario-Based, proportional methodology for the AI act.' Digital Society 3.1 (2024) <https://link.springer.com/article/10.1007/s44206-024-00095-1> accessed 10 January 2025

[127] Special Report on Climate Change and Land - IPCC site 2019 <https://www.ipcc.ch/srccl/> accessed 10 January 2025

[128] Alexy, R. (2010). 'A theory of constitutional rights.' Oxford university press.

[129] Novelli, Claudio, et al. 'AI Risk Assessment: A Scenario-Based, proportional methodology for the AI act.' Digital Society 3.1 (2024): 13. <https://link.springer.com/article/10.1007/s44206-024-00095-1> accessed 10 January 2025

[130] Tutt, A. 'An FDA for algorithms.' Admin. L. Rev., 69, 83. (2017). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747994#:~:text=Andrew%20Tutt%20,difficult%20regulatory%20puzzles%20algorithms%20pose> accessed 10 January 2025

tort law, criminal sanctions, and fragmented sectoral oversight lack the uniformity and ex-ante control necessary for learning systems whose failures may be opaque, catastrophic, and difficult to reverse. [131] Although no jurisdiction has yet adopted full pre-approval, elements of the model surface in contemporary proposals: the EU AI Act's third-party conformity assessments for high-risk AI, and civil-society petitions urging the U.S. Federal Trade Commission to halt unsafe AI releases, both echo the call for a central gatekeeper.[132] The "Algorithmic Safety Agency" thus offers a stringent, but conceptually coherent, template for jurisdictions seeking to move beyond post-hoc liability toward preventative licensing of high-risk AI.

H. Externalities with a Moral Twist: A Moral-Centric Paradigm for AI Regulation

Petit, N., & De Cooman, J[133]'s *"Externalities with a Moral Twist"* model strikes me as a refreshing take on AI regulation, one that puts society's ethical bill front and centre. The importance of this distinction lies in its focus on who ultimately bears the costs: in the absence of such a perspective, those moral costs and hidden burdens are off-loaded onto the public. Unlike the EU AI Act's neat risk taxonomy, which categorizes systems by technical criteria and likelihood of harm, this Fifth Model spotlights the very real ethical and social expenses that AI imposes on society. We clearly see that Artificial-intelligence governance and regulation is no longer a blank canvas but a crowded studio of overlapping experiments. A mature EU digital constitutionalism order will likely require a composite architecture that layers prudential trials and dynamic risk scoring onto the AI Act, backed by an EU-level safety agency and harmonized moral-externality assessments, while preserving AI innovation channels for SMEs. The next chapter offers a concrete blueprint for that upgrade. Drawing on the shortcomings diagnosed here, it sets out a new proposition for an AI Regulation model. Its ambition is simple: to ensure that AI's velocity accelerates, rather than undermines, the Union's constitutional commitment to human dignity, democracy and the rule of law.

3. The Universal AI Regulation Model: A Framework Proposition For The Future Of The EU's Digital Constitutionalism.

The European Union's digital constitutionalism, rooted in principles of democracy, transparency, and fundamental rights, faces unprecedented challenges from AI's rapid

[131] *Ibid.*

[132] *Think tanks like the Center for AI and Digital Policy (CAIDP) have endorsed something akin to this when they petitioned the U.S. FTC in 2021 to block releases of certain advanced AI until proven safe, effectively asking FTC to act like an FDA for AI.*

[133] Petit, N., & De Cooman, J. (2021). 'Models of Law and Regulation for AI.' The routledge social science handbook of AI, 199-221. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3706771> accessed 10 January 2025

evolution. While the EU AI Act marks progress, its static risk tiers, neglect of socio-political harms, and fragmented redress mechanisms render it insufficient. Building on critiques of existing frameworks and synthesizing insights from alternative regulatory paradigms, we propose through this chapter what we will be calling the "*Universal AI Regulation Model" (Hereunder "UARM")*, a dynamic, rights-preserving framework designed to govern all AI applications across the EU. This model integrates novel democratic safeguards, adaptive enforcement tools, and innovation-forward mechanisms to address gaps in the AI Act while advancing the EU's constitutional ethos.

A. Core Pillars of the Universal AI Regulation Model

- *Constitutional Resilience Through Polycentric Governance*

The UARM prioritizes democratic resilience by embedding safeguards against AI-mediated power asymmetries. Its architecture integrates three interconnected institutions. The proposed *EU Democracy Board for AI (EDB-AI)* functions as an independent agency with pre-market approval powers, tasked with scenario-driven risk assessments and issuing binding technical standards. Complementing this central body are National Civic Observatories, citizen panels empowered to audit AI systems via open model cards and real-time telemetry. Finally, Sectoral Micro-Regulators (specialized bodies in domains such as healthcare and finance) oversee AI within their existing mandates, ensuring context-specific scrutiny. This polycentric structure balances centralized oversight with localized accountability, mitigating regulatory capture while preserving subsidiarity.

- *Dynamic Socio-Political Impact Assessment (SPIA)*

Replacing the AI Act's static risk tiers, the UARM adopts a scenario-driven risk calculus inspired by IPCC climate models. AI systems are evaluated across four dimensions: hazard (which is the potential harm to rights or democracy), reach (which refers here to : the scale of deployment), epistemic opacity (which we can define as technical explainability challenges, as confirmed by specialists.), and democratic salience (notably, the most important prong, and which refers here to the impact on electoral integrity or public discourse). The vision is to have the scores dynamically updated using real-world data such as disinformation virality metrics (which platforms must be required to provide once they reach a certain number of users) or bias complaints, triggering adaptive safeguards such as license adjustments or mandatory code modifications. These rules can only be effective if they are coupled with significant sanctions, otherwise, they will remain useless.

- *Perpetual Licensing and Algorithmic Restitution*

High-salience AI systems, including large language models and biometric surveillance tools must require renewable licenses contingent on post-deployment SPIA performance. In this scenario, it would be efficient if violations activate two key mechanisms: first, providers must post *"democracy-impact bonds"*, which are financial reserves that shall be forfeited if audits reveal AI induced harms like voter suppression or disinformation amplification. Second, courts may issue algorithmic restitution orders that can mandate code changes, dataset purges, or transparency measures to remediate harm.

B. Democratic Safeguards and Enforcement Mechanisms

- Prophylactic Bans: Preserving Public Trust & democratic principles

First, real-time biometric surveillance in public spaces (facial recognition, gait analysis, and the like) is flatly banned, save for tightly scoped counter-terror operations under judicial review. Second, automated voter profiling that deduces political leanings or susceptibility to disinformation is off-limits. Third, synthetic media impersonating politicians, journalists, or public figures must embed cryptographically signed provenance watermarks; anything non-compliant is illegal. These prohibitions tackle structural risks the AI Act barely skims, such as algorithmic voter manipulation.

- Transparency Mandates for Electoral Integrity involving AI

The UARM turns transparency from slogan to software through two concrete levers. Platforms must host ad libraries with open APIs, showing real-time data on targeting parameters, spend, and virality for every AI-generated political post, letting civil-society watchdogs spot covert influence before it metastasizes. Meanwhile, all AI election content (text, audio, or video) must carry an indelible, machine-verifiable watermark that logs origin, model weights, and edit history. Non-compliant items are auto-delisted from EU servers, countering the AI Act's lukewarm "limited-risk" tag for synthetic media.

- Criminal Liability and Redress Mechanisms for AI caused harm

Serious breaches deploying banned systems or poisoning data, trigger EU-wide criminal penalties modeled on environmental-crime statutes. (See IPCC Model stated above). Victims get two justice lanes. The AI Ombuds Court, a specialist arm of the European Ombudsman, hears collective petitions, revokes licences, or orders counter-speech drives. In parallel, GDPR's Right to be Forgotten gains teeth: erased personal data inside training sets is swapped for verifiable synthetic stand-ins, preserving model integrity while restoring privacy.

C. Innovation and Competitiveness Imperatives

- IP Safe Harbors for Ethical Research

To keep alignment research alive, the UARM shields scholars reverse-engineering closed models. Peer-reviewed, non-commercial audits of black-box systems enjoy immunity from copyright suits. The EDB-AI backs SMEs by hosting open model repositories with anonymized weights and compliance toolkits, trimming reliance on proprietary benchmarks.

- Dual-Use Export Controls for AGI Governance

Recognizing AGI's existential stakes, the UARM files it under an "Infra-High-Risk Technology Directive", which will be nuclear tech's regulatory cousin. Developers must secure an international licence via outfits like an IAEA and/or OECD, while training runs topping 10^25 FLOPs[134] summon automatic EDB-AI oversight. Sovereign data stewardship keeps AGI datasets on EU soil, enabling audits and GDPR-compliant synthetic data swaps to preserve the RTBF.

- Regulatory Sandboxes 2.0: Co-Design for Compliance

Our proposed UARM model also supports Public-private co-design hubs that let universities, startups, and regulators test frontier tech (quantum AI, for instance) under provisional licences. Built-in kill switches and tamper-proof audit trails keep experiments safe, and validated systems win fast-track approval, slashing time-to-market significantly.

D. Why adopt the UARM?

The model broadens digital constitutionalism by weighing societal externalities (mental-health fallout, polarization) alongside individual harms via SPIA metrics. Binding EDB-AI standards knit enforcement across the single market, mending the AI Act's patchwork risk tiers. Globally, interoperability with UNESCO and OECD frameworks positions the EU to set the tone on ethical AI. The UARM's agile, context-aware blueprint does more than paper over cracks; it welds dynamic risk reviews, polycentric oversight, and algorithmic restitution into one coherent regime. Prophylactic bans, cryptographic transparency, and AGI-specific guard-rails fortify Europe's constitutional spine, while IP safe harbors and Sandboxes 2.0 keep innovation humming. AI now permeates every corner of life; the UARM shows that rigorous regulation and technological advance can walk hand in hand, shaping a digital future rooted in democratic principles.

[134] *"Floating-point operations per second (FLOPS) is a measure of a computer's performance based on the number of floating-point arithmetic calculations that the processor can perform within a second."* 'Floating-point operations per second (FLOPS)', Robert Sheldon. (August 2023) https://www.techtarget.com/whatis/definition/FLOPS-floating-point-operations-per-second accessed 10 January 2025

IV. Conclusion

The EU's digital constitutionalism project now finds itself at a crossroads. AI is redrawing the map of governance, yet the Union still leans on static, state-centric templates that invite regulatory obsolescence and even democratic back-sliding. As this paper shows, today's instruments, including the much-heralded AI Act, leave socio-political externalities, opaque algorithmic decision-making, and cross-border enforcement gaps largely untouched. Structural flaws, legislative inertia and piecemeal oversight among them, further expose fundamental rights to algorithmic harm. The Universal AI Regulation Model (UARM) proposed in this paper weaves together dynamic risk assessments, multi-stakeholder oversight, and algorithmic restitution to harmonize innovation with accountability. It enacts forward-looking bans on biometric surveillance, imposes guard-rails for synthetic media, and introduces AGI-specific controls to stave off existential dangers, while also offering pro-innovation mechanisms, such as regulatory sandboxes and IP safe harbours, to keep Europe at the ethical AI frontier. In doing so, UARM demonstrates that regulatory agility and constitutional resilience need not be mutually exclusive: embedding democratic safeguards at every stage of the AI lifecycle upholds human dignity, transparency, and the rule of law.

References

Legislation / Legal Instruments

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

Regulation (EU) 2016/679 General Data Protection Regulation [2016] OJ L 119/1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence [2024] OJ L1689/1.

European Parliament, 'Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))' [2017] OJ C 252/239 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2017:252:TOC accessed 10 January 2025.

Official Reports / Institutional Publications

- European Commission (2018b), *Coordinated Plan on Artificial Intelligence*, COM (2018) 795 final.
- European Commission, *Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)* COM (2022) 496 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496 accessed 10 January 2025.
- European Commission, *European Declaration on Digital Rights and Principles for the Digital Decade* (2022).
- European Data Protection Board, 'French SA Fines Clearview AI EUR 20 Million' (EDPB, 2022) https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en accessed 10 January 2025.
- European DIGITAL SME Alliance, *DIGITAL SME Position Paper on the Artificial Intelligence Act* (2021) https://www.digitalsme.eu/policy/ accessed 10 January 2025.
- European Parliament, *Artificial Intelligence Act: MEPs Adopt Landmark Law* (8 March 2024) https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law accessed 10 January 2025.
- European Parliament, *Legislative Train – AI Liability Directive* https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-ai-liability-directive accessed 10 January 2025.
- European Parliamentary Research Service, *Artificial Intelligence Act and Regulatory*

Sandboxes, PE 733.544, March 2022 https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf accessed 10 January 2025.

- Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (2024) https://rm.coe.int/ai-convention-brochure/1680afaeba accessed 10 January 2025.
- UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (adopted 23 November 2021) https://www.unesco.org/en/ethics/artificial-intelligence accessed 10 January 2025.
- OECD, *OECD AI Principles* (2019) https://oecd.ai/en/ai-principles accessed 10 January 2025.
- The White House, *Blueprint for an AI Bill of Rights* (Office of Science and Technology Policy, 2022) https://www.whitehouse.gov/ostp/ai-bill-of-rights/ accessed 10 January 2025.
- IPCC, *Special Report on Climate Change and Land* (2019) https://www.ipcc.ch/srccl/ accessed 10 January 2025.
- High-Level Expert Group on AI, *Ethics Guidelines for Trustworthy AI* (2019) https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai accessed 10 January 2025.
- Eva Fournier-Tombs, 'Towards a United Nations Internal Regulation for Artificial Intelligence' (2021) *Big Data & Society* https://www.researchgate.net/publication/354233951_Towards_a_United_Nations_Internal_Regulation_for_Artificial_Intelligence accessed 10 January 2025.

Books

Alexy, R. (2010). *A Theory of Constitutional Rights*. Oxford University Press.

Lessig, Lawrence, *Code and Other Laws of Cyberspace* (2nd edn, Basic Books 2009).

Book Chapters

- Andreas Holzinger et al, 'Explainable AI Methods - A Brief Overview' in Benjamin Biecek, Piotr Molnar and Wojciech Samek (eds), *Extending Explainable AI Beyond Deep Models and Classifiers* (Springer 2020) 13–38 https://link.springer.com/chapter/10.1007/978-3-031-04083-2_2 accessed 10 January

2025.

- Campos R, 'A Necessary Cognitive Turn in Digital Constitutionalism: Regulated Self-Regulation as a Regulatory Mechanism for Artificial Intelligence (AI) in Comparative Law' in *Digital Constitutionalism* (Nomos 2025) https://www.nomos-elibrary.de/de/10.5771/9783748938644-113.pdf accessed 10 January 2025.
- Pollicino O and Paolucci F, 'Digital Constitutionalism' in L Floridi, M Ziosi and M Taddeo (eds), *Companion to Digital Ethics* (OUP 2024) http://dx.doi.org/10.2139/ssrn.5098492 accessed 10 January 2025.
- Hoffmann-Riem, Wolfgang. 'Artificial intelligence as a challenge for law and regulation.' *Regulating Artificial Intelligence* (2020): 1–29 https://link.springer.com/chapter/10.1007/978-3-030-32361-5_1 accessed 10 January 2025.
- Petit, N., & De Cooman, J. (2021). 'Models of Law and Regulation for AI.' *The Routledge Social Science Handbook of AI*, 199–221 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3706771 accessed 10 January 2025.

Conference Papers

Almeida, P. G. R., et al., 'Meta-Framework for AI Regulation' Proceedings of the 53rd Hawaii International Conference on System Sciences (2020) https://www.researchgate.net/publication/339025965_Artificial_Intelligence_Regulation_A_Meta-Framework_for_Formulation_and_Governance accessed 10 January 2025.

Matyáš Boháček, 'Slovakia as the Precursor to Deepfake-Enabled Election Interference: Lessons Learned and Pathways Forward' in *Proceedings of the 18th ICWSM* (AAAI Press 2024) 3–6 June 2024 https://workshop-proceedings.icwsm.org/pdf/2024_67.pdf accessed 10 January 2025.

Journal Articles

Alqodsi, Enas Mohammed, and Dmitry Gura. 'High Tech and Legal Challenges: Artificial Intelligence-Caused Damage Regulation.' *Cogent Social Sciences* 9.2 (2023): 2270751. https://www.tandfonline.com/doi/abs/10.1080/23311886.2023.2270751 accessed 10 January 2025.

Angelo Jr Golia, 'Critique of Digital Constitutionalism: Deconstruction and Reconstruction from a Societal Perspective' (2024) 13 *Global Constitutionalism* 488–518 https://doi.org/10.1017/S2045381723000126 accessed 10 January 2025.

Barrio Andrés, Moisés. 'Towards Legal Regulation of Artificial Intelligence.' *Revista IUS* 15.48 (2021): 35–53. https://revistaius.com/index.php/ius/article/view/661/856 accessed 10 January 2025.

Brandeis Marshall, 'No Legal Personhood for AI' (2023) 4 *Patterns* 100861 https://doi.org/10.1016/j.patter.2023.100861 accessed 10 January 2025.

Celeste, Edoardo. 'Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges.' (2021) 9(3) *International Journal of Law and Information Technology* 253–281. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3219905 accessed 10 January 2025.

Celeste, Edoardo. 'Digital Constitutionalism: A Socio-Legal Approach.' (2024) 10(2) *European Data Protection Law Review* 146–149 https://doi.org/10.21552/edpl/2024/2/5 accessed 10 January 2025.

Celeste, Edoardo. 'Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights.' (2023) 14(1) *International Journal of Law and Information Technology* 45–67. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4698091 accessed 10 January 2025.

Francesco Paolo Levantino, 'Generative and AI-Powered Oracles: "What Will They Say about You?"' (2023) 51 *Computer Law & Security Review* 105898 https://doi.org/10.1016/j.clsr.2023.105898 accessed 10 January 2025.

Finocchiaro, Giusella. 'The Regulation of Artificial Intelligence.' *AI & SOCIETY* 39.4 (2024) https://cris.unibo.it/retrieve/5eb315d2-5f34-47fe-9394-5fda4980ee5e/The%20regulation%20of%20artificial%20intelligence.pdf accessed 10 January 2025.

Jan Czarnocki, 'Saving EU Digital Constitutionalism Through the Proportionality Principle and a Transatlantic Digital Accord' (2023) 28(4) *European Public Law* 789–812. https://www.martenscentre.eu/wp-content/uploads/2021/10/5.pdf accessed 10 January 2025.

Miguel Pereira, 'Mapping the Values of Digital Constitutionalism: Guiding Posts for Digital Europe?' (2024) 10(2) *UNIO – EU Law Journal* 1–25. https://doi.org/10.21814/unio.10.2.6045 accessed 10 January 2025.

Mireille Hildebrandt, 'Algorithmic Regulation and the Rule of Law' (2018) 376 *Philosophical*

Transactions of the Royal Society A 2128 https://royalsocietypublishing.org/doi/10.1098/rsta.2017.0355 accessed 10 January 2025.

Monika Simmler and Nora Markwalder, 'Guilty Robots? Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence' (2018) 29 *Criminal Law Forum* 1 https://doi.org/10.1007/s10609-018-9360-0 accessed 10 January 2025.

Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4(3) *Social Media + Society* 2056305118787812 https://journals.sagepub.com/doi/10.1177/2056305118787812 accessed 10 January 2025.

Petros Terzis, 'Against Digital Constitutionalism' (2024) 3(2) *European Law Open* 336–352. https://doi.org/10.1017/elo.2024.15 accessed 10 January 2025.

Pin Lean Lau, 'The Extension of Legal Personhood in Artificial Intelligence' (2019) 46 *Revista de Bioética y Derecho* 47–66 https://revistes.ub.edu/index.php/RBD/article/view/27064 accessed 10 January 2025.

Priyanka Majumdar, Bindu Ronald and Rupal Rautdesai, 'Artificial Intelligence, Legal Personhood and Determination of Criminal Liability' (2019) 6(6) *Journal of Critical Reviews* 323–330 https://www.researchgate.net/publication/383994634_Artificial_Intelligence_Legal_Personhood_and_Determination_of_Criminal_Liability accessed 10 January 2025.

Rowena Rodrigues, 'Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities' (2020) 4 *Journal of Responsible Technology* 100005 https://doi.org/10.1016/j.jrt.2020.100005 accessed 10 January 2025.

Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States and Beyond' (2023) 26 *Yale Journal of Law & Technology* 671 https://yjolt.org/sites/default/files/wachter_26yalejltech671.pdf accessed 10 January 2025.

Keith Jakee and Demi Fink, 'Micro-targeting Voters in the 2016 US Election: Was Cambridge Analytica Really Different?' (SSRN Working Paper, 1 May 2024) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4843786 accessed 10 January 2025.

Marco Almada, 'Governing the Black Box of AI' (SSRN Pre-print, 7 November 2023) https://ssrn.com/abstract=4587609 accessed 10 January 2025.

Web Articles / Blog Posts / News Media / Corporate

- Reuters, 'US Far-Right Activists, WikiLeaks and Bots Help Amplify Macron Leaks: Researchers' *Reuters* (Paris, 5 May 2017) https://www.reuters.com/world/us-far-right-activists-wikileaks-and-bots-help-amplify-macron-leaks-research-idUSKBN18302L/ accessed 10 January 2025.
- Ochigame, R. 'The Invention of 'Ethical AI': How Big Tech Manipulates Academia to Avoid Regulation.' *Economies of Virtue*, 49 (2019) https://mediarep.org/bitstream/handle/doc/20441/TOD_46_Phan_2022_Economies-of-Virtue_.pdf accessed 10 January 2025.
- Gandy, 'The Algorithm Made Me Do It!' IAMCR (2019) https://www.asc.upenn.edu/sites/default/files/2021-03/%22The%20Algorithm%20Made%20Me%20Do%20It!%20Predictive%20Policing,%20Cameras,%20Social%20Media%20and%20Affective%20Assessment.%22%20IAMCR%202019..pdf accessed 10 January 2025.
- Meta Platforms Inc, 'Corporate Human Rights Policy' (31 March 2021) https://about.fb.com/wp-content/uploads/2021/03/Facebooks-Corporate-Human-Rights-Policy.pdf accessed 10 January 2025.
- White & Case, 'AI Watch: Global Regulatory Tracker - G7' (White & Case Insight, 2024) https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-g7 accessed 10 January 2025.
- Holistic AI, 'Regulating AI: The Horizontal vs Vertical Approach' (Holistic AI, n.d.) https://www.holisticai.com/blog/regulating-ai-the-horizontal-vs-vertical-approach accessed 10 January 2025.