3/2025 anteprima

Rivista di diritto dei media

ISSN 2532-9146

Rule of Law in the Age of AI*

Federica Paolucci, Oreste Pollicino, Charlotte Waldron

Table of Contents

1. Introduction

«Any society in which no provision is made for guaranteeing rights or for the separation of powers has no Constitution», states art. 16 of the Declaration of Human and Civic Rights of 26 August 1789.[1]
The force of this provision lies in its insistence that the law's purpose is not abstract moral vindication, but the concrete disciplining of power.[2] The rule of law, in this European understanding,[3] does not describe a final state of affairs but a structural condition: it ensures that authority is channelled through general and foreseeable norms, and that it remains subject to institutional checks capable of providing redress.[4] Its function is instru-

* This article reflects the views of all the authors. Authorship for Sections 2, 2.1, 3 and 4 lies primarily with Oreste Pollicino, while Sections 5, 6, 6.1, 6.2, 6.3, 6.4 and 6.5 were written primarily by Federica Paolucci. The introduction and conclusion are the result of collective drafting.

1 Declaration of Human and Civic Rights, 26 August 1789.

2 *Ex multis,* C. de Montesquieu, *The Spirit of Laws*, Book XI, in *Wikisource*.

3 This paper adopts a primarily European perspective on the rule of law. Comparative dimensions are acknowledged, and reference is made to A. Sajó, *The Rule of Law*, in R. Schütze-R. Masterman (eds.), *The Cambridge Companion to Comparative Constitutional Law*, Oxford, 2019, 258 ff. Sajo underlines the plurality of national traditions but also the specifically European understanding of the rule of law as a structural condition rather than a final state of affairs. Methodologically, this paper adopts an analysis that is both doctrinal and institutional. It reconstructs the Union's rule-of-law standard from primary law and the Court of Justice's jurisprudence and treats conditionality mechanisms, particularly the budgetary conditionality regulation and the Recovery and Resilience Facility, as examples of how constitutional standards are rendered administrable through verifiable safeguards.

4 On this point, see Marta Cartabia who highlights that, in the European constitutional tradition, the rule of law is not conceived as a static outcome but as a structural

mental. It is not an end in itself,[5] but the indispensable means by which fundamental rights and other relevant values are secured and granted.

Alongside the more formalistic historical visions of the rule of law, focused on legality in its narrow sense, namely that public action be authorised by law, scholarship and institutional organisations have progressively emphasised its substantive dimension.[6] The rule of law is not only about constraining authority through predictable and general norms but also about securing rights and access to redress.[7] This double orientation, law as a restraint on power, and the rule of law as a means to protect rights, is precisely what explains why the debate about Artificial Intelligence (hereinafter, AI) cannot be cast in purely technological or efficiency terms.

The rule of law has already faced severe challenges in past constitutional crises in Europe, where pressures to bypass checks and guarantees in the name of emergencies or expediency weakened its foundations.[8] Those experiences show that crises of legality and rights protection are not new phenomena; the advent of AI risks reproducing them in new forms, or even exacerbating them, by introducing technological opacity and a potential displacement of responsibility.[9]

When decisions are increasingly mediated, or even taken, by automated systems, the question that arises is whether the guarantees associated with legality, separation of powers, and effective judicial protection remain intact.[10] The issue is not only that AI may produce errors or biases, but that

---

requirement that channels public authority through general and foreseeable norms, while ensuring its submission to institutional checks capable of redress. See M. Cartabia, *The Rule of Law and the Role of Courts*, in *Italian Journal of Public Law*, 10, 2018, 1.

[5] «The chief merit of the teleological approach to the rule of law is that it puts this overarching purpose into perspective. The rule of law is not a goal in and of itself that should be fetishised, but a means that can help achieve other related values, such as the protection of human rights and public accountability, and thus democracy», N. A. Smuha (ed.), *The Rule of Law*, in *Algorithmic Rule By Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law*, Cambridge, 2024, 95 ff.

[6] On formalistic accounts see A. Sajó, *The Rule of Law*, cit., 1, noting the risks of reducing the rule of law to mere legality. On the crises that have already tested the resilience of the rule of law in the EU see F. Casolari, *Il rispetto della rule of law nell'ordinamento giuridico dell'Unione europea: un dramma in due atti: The respect of the rule of law within the legal order of the European Union: A drama in two acts*, in *DPCE Online*, 28, 2016, 135 ff. On how technological opacity and algorithmic governance risk reproducing or aggravating these crises see N.A. Smuha (ed.), *From Rule of Law to Algorithmic Rule by Law*, in *Algorithmic Rule By Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law*, Cambridge, 2024, 151 ff.

[7] This aspect is particularly relevant when considering the role of the judiciary, as emphasised by leading scholarship: M. Cartabia, *The Rule of Law and the Role of Courts*, cit.; K. Lenaerts, *The Rule of Law and the Coherence of the Judicial System of the European Union*, in *Common Market Law Review*, 44(6), 2007, 1625 ff.; D. Lustig-J. H. H. Weiler, *Judicial review in the contemporary world-Retrospective and prospective*, in *International Journal of Constitutional Law*, 16(2), 2018, 315 ff.

[8] J. H. H. Weiler, *Europe In Crisis—On «Political Messianism», «Legitimacy» and the «Rule Of Law»*, in *Singapore Journal of Legal Studies*, 2012, 248 ff.

[9] On AI autonomy, allow the referral to O. Pollicino-F. Paolucci, *Regulating AI Autonomy: A Constitutional Framework for the Digital Era*, in M. Durante - U. Pagallo (eds.), *The De Gruyter Handbook on Law and Digital Technologies*, Berlin, 2025, 353 ff.

[10] These guarantees correspond to the essential components of the rule of law as

it reconfigures where power is exercised and how it is justified.[11] Decisions that once bore the marks of human judgement, subject to established administrative or judicial procedures, now emerge from systems whose rationality is statistical, whose operations are opaque, and whose governance depends on technical as well as legal choices.[12] In this sense, AI is not external to the constitutional order but internal to it: it both tests and redefines the conditions under which the rule of law is realised.[13]

To analyse this tension, it is necessary first to clarify what is meant by the rule of law in the European context. Although scholarly debate distinguishes "thin" or formal accounts, legality, prospectivity, clarity, and stability, from "thick" or substantive accounts that fold rights and equality into the concept itself, both converge on the idea that the rule of law is a discipline of power. Raz's conception of the rule of law as a "virtue" of legal systems, ensuring that law can guide conduct, highlights its formal dimension.[14] Waldron's emphasis on procedure and contestation underlines its practical and participatory nature.[15] On a different level, the Venice Commission's Rule-of-Law Report synthesises these traditions into five operational pillars: legality, legal certainty, the prohibition of arbitrariness, equality before the law, and access to justice.[16] In the EU's legal order, these have been rendered justiciable through art. 19(1) TEU and art. 47 CFR, which the Court of Justice has read together with art. 2 TEU to produce enforceable institutional minima.[17]

---

identified by the Venice Commission: European Commission for Democracy through Law (Venice Commission), *Rule of Law Checklist*, CDL-AD(2016)007, adopted 11–12 March 2016, paras 12-15.

[11] K. Crawford, *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*, Yale, 2021; G. De Gregorio, *The Normative Power of Artificial Intelligence*, in *Indiana Law Journal*, 30(2), 2023, 55 ff.; O. Caramaschi, *Il costituzionalismo al cospetto dell'intelligenza artificiale: nuove sfide, quali soluzioni*, in *Rivista italiana di informatica e diritto*, 7(1), 2025, 23 ff.

[12] This dynamic has been vividly illustrated in the European debate by the *SCHUFA* case, concerning algorithmic credit scoring, and by controversies surrounding the deployment of biometric recognition technologies, both of which highlight how opaque, statistical rationalities challenge the guarantees of transparency, accountability and effective judicial redress. See ECJ, Case C-634/21, *OQ v. Land Hesse,* 7 December 2023; ECJ, Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministres,* 21 June 2022. From a doctrinal point of view, see P. De Hert-G. Bouchagiar, *European Biometric Surveillance, Concrete Rules and Uniform Enforcement: Beyond Regulatory Abstraction and Local Enforcement*, in *Cambridge Handbook on Facial Recognition in the Modern State*, Oxford, 2024, 139 ff.; E. Falletti-C. Gallese, *Credit scoring judicial review between the Court of Justice of the European Union and comparative case law*, in *Rivista di diritto dei media,* 3, 2024, 92 ff.

[13] P. Burgess, *AI and the Rule of Law : The Necessary Evolution of a Concept*, in P. Burgess (eds.), *AI and the Rule of Law : The Necessary Evolution of a Concept*, Oxford, 2024.

[14] J. Raz, *The Rule of Law and its Virtue*, cit.

[15] J. Waldron, *The Rule of Law*, in E. N. Zalta - U. Nodelman (eds.), *The Stanford Encyclopedia of Philosophy*, Stanford, 2023.

[16] See the "Report on the Rule of law", adopted in Venice, March 25-26, 2011 - CDL-AD (2011)003rev., and the "Rule of Law Checklist", adopted in Venice, March 11-12, 2016 - CDL-AD(2016)007.

[17] ECJ, Case C-64/16, *Associação Sindical dos Juízes Portugueses (ASJP) v Tribunal de Contas*, 27 February 2018, §31-52, where the Court held that art. 19(1) TEU, read in conjunction with art. 47 CFR and art. 2 TEU, requires Member States to ensure effective judicial

What matters for present purposes is that the rule of law operates as a bridge between legality and rights.[18] Its formal dimension disciplines how power is exercised: laws must be clear, general, and foreseeable; decisions must be taken by authorised bodies on the basis of lawful procedures; records must be kept and reasons given. Its substantive dimension ensures that legality does not become an empty shell: decisions must respect equality and non-discrimination, remain proportionate, and allow for effective remedies before an independent tribunal. This combination of form and substance makes the rule of law the principal means by which fundamental rights are guaranteed in practice.

Artificial intelligence activates both dimensions simultaneously. Exogenously, when automated systems are used in domains such as welfare, education, migration or credit, the legality of their deployment depends on whether the decision-making process respects the principles just outlined: whether it is supported by a lawful basis and purpose, whether transparency obligations are discharged, whether human oversight is real, and whether remedies are available in time to matter.[19] Endogenously, AI also raises questions about the legality of design and governance within the systems themselves: how data are sourced and managed, how objectives and thresholds are defined, how retraining and change control occur, and how responsibility is distributed along the provider–deployer chain.[20] These are not technical details but normative choices. They define who is accountable, what counts as an error, and which values are privileged in trade-offs between efficiency and fairness. To ignore them would be to allow a displacement of legal judgment into opaque technical parameters.[21]

The European Union has progressively operationalised this functional understanding of the rule of law through its own reporting practice. The 2025 Rule of Law Report and its updated methodology confirm that legality, legal certainty, prevention of abuse of power, equality and access

protection and judicial independence as part of the rule of law.

18 «In some ways, it is once again the principles of the rule of law that are trying to rise from the ruins of the nation state and regain strength on a global scale. It is still the age-old dream of imposing rules on power. But dreaming is not enough: as has always been the case in the difficult history of the struggle for rights, dreams must be accompanied by political struggle», R. Bin, *Lo Stato di diritto*, Bologna, 2017, 120 (aut. trans.).

19 See District Court of The Hague, 5 February 2020, *NJCM c.s./Netherlands (SyRI)*, declaring unlawful the use of an automated risk-scoring system in welfare on grounds of lack of transparency and disproportionate interference with the right to privacy under art. 8 ECHR. Scholars argue on the human rights implication of this system of digital welfare, as in A. Rachovitsa-N. Johann, *The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case*, in *Human Rights Law Review*, 22(2), 2022, 10 ff.; S. Ranchordás, *The invisible citizen in the digital state: Administrative law meets digital constitutionalism*, in J. De Poorter *et al.* (eds.), *European yearbook of constitutional law*, ebook, 2024; M. van Bekkum-F. Z. Borgesius, *Digital welfare fraud detection and the Dutch SyRI judgment*, in *European Journal of Social Security*, 23(4), 2021, 323 ff.

20 On the legality of AI system design and governance, see Regulation (EU) 2024/1689 (hereinafter, AI Act), arts. 9-15, 26 (risk management, data governance, human oversight and accountability across the provider–deployer chain).

21 On the necessity to redefine and clarify the boundaries of the AI legal responsibility, see G. Finocchiaro, *The regulation of artificial intelligence*, in *AI & Society*, 39, 2024, 1961 ff.

to justice are not rhetorical values but working benchmarks[22] which are applied by the EU in specific areas: justice, anti-corruption framework, media freedom and media pluralism.[23] By translating art. 2 TEU into annual monitoring indicators, the Commission has effectively aligned itself with the Venice Commission, treating the rule of law as a set of verifiable conditions for rights protection.[24] This reinforces the claim that in the Union's constitutional grammar, the rule of law is a *means*, not an end.

Thus, the purpose of this paper is to assess whether the European Union's emerging framework for AI meets its own rule-of-law standard when both dimensions are taken into account. The central claim is twofold. Doctrinally, this article argues that the Union's conception of the rule of law is best understood as a functional principle: it is the means by which fundamental rights are made effective and public power is disciplined. Read in that key, the challenge of artificial intelligence is not merely whether new rules exist, but whether those rules deliver *remedy-capable* guarantees when decision-making becomes automated and partly opaque. Methodologically, the analysis anchors this assessment in the Venice Commission's Rule of Law Checklist, treating its benchmarks, legality, legal certainty, prevention of abuse of power, equality and non-discrimination, and access to justice, not as abstract values but as operational conditions that must be satisfied both in the use of AI and in its design and governance.

The paper proceeds by building this framework and then testing it against the Union's regulatory response. While Section II reconstructs the theoretical basis of the rule of law, Section III maps how autonomy in AI, understood as learning, adaptiveness and partial independence from human reasoning, reconfigures the *loci* of power and therefore the terms on which the rule of law must operate. Then, Section IV offers a concise technical account of autonomy to ground the legal analysis, distinguishing where opacity, statistical inference and model governance create friction with legality and reviewability. Section V asks whether the AI Act amounts to a constitutional response in this sense, examining in particular the reliance on an internal-market legal basis, delegated norm-making, standardisation and codes of practice. Section VI then applies the Venice Commission's Checklist, element by element, legality, legal certainty, prevention of abuse of power, equality and non-discrimination, and access to justice, to evaluate the Act and related instruments; here access to justice functions as the decisive hinge, because without intelligible explanations, evidence preservation and disclosure, and contestation pathways, the rule of law cannot serve its instrumental role. Finally, Section VII sets out *de iure condendo* proposals to re-align the framework with that role, including statutory

[22] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "2025 Rule of Law Report. The rule of law situation in the European Union", Strasbourg, 8.7.2025 COM(2025) 900 final.

[23] European Commission, "Methodology for the preparation of the Annual Rule of Law Report", 2025.

[24] The Venice Commission is a recurrent benchmark in the evaluation conducted in the Report. See, for instance, in the methodology where it is stated that the «Check List can help to identify specific risks and weaknesses», cit., 4.

bases for sensitive deployments, limits on soft-law reliance, clarified and enforceable oversight duties, independently verified equality safeguards, and remedies that guarantee reasons and evidence to courts and affected individuals. Throughout, the claim is: constitutionalisation is credible only if the rule of law works as a means. The contribution of the article is to provide a structured way to test that proposition in the AI domain and to indicate how the Union's framework can be re-oriented, doctrinally and practically, towards guarantees that are enforceable in fact, not merely in form.

2. Rule of Law: Theoretical Basis

In contemporary European constitutionalism, the rule of law is not a terminal value but a functional architecture. Its formal requirements have worth because they enable the substantive ones, equality, proportionality, and rights protection, to be exercised. On this view, the question to ask of any governance arrangement is not whether it can be described as "rule-of-law compliant" in the abstract, but whether it furnishes those who are governed with the concrete capacities to test power: a legal basis they can invoke, norms they can foresee, discretion they can challenge, and remedies they can obtain.

The rule of law has long occupied a central place in the European Union's constitutional imagination, but its precise content remains contested.[25] In Pitruzzella's formulation, its core elements are «the principle of legality, freedom and equality of citizens, separation of powers, independence of judges».[26] If the rule of law ensures that «it is the laws, not men, that govern us»,[27] and that the division of powers together with the principle of legality are the institutional devices that make this aspiration real.

As a matter of fact, the common law jurist Albert Venn Dicey famously defined the rule of law in three elements: the absolute supremacy of regular law as opposed to arbitrary power; equality before the law of all persons, regardless of status; and the constitution as the result of ordinary law, not a higher abstract text.[28] Dicey's view is often criticised as narrow and formalistic,[29] yet his insistence on equality before the ordinary courts still resonates in contemporary European jurisprudence. It anticipates one of the central doctrinal moves of the Court of Justice: that the availability of judicial review is an indispensable component of the Union's identity, and that independence and impartiality are not political aspirations but

[25] For a brief overview, A. Z. Huq, *The Rule of Law: A Very Short Introduction*, Oxford, 2024.

[26] G. Pitruzzella, *Stato di diritto, indipendenza delle corti e sovranità popolare: armonia o conflitto*, in *Rivista di Diritti comparati*, 3, 2018, 12 ff.

[27] R. Bin, *Lo Stato di diritto,* cit., 3.

[28] A. V. Dicey, *Introduction to the Study of the Law of the Constitution*, London, 1959.

[29] M. D. Walters, *The Spirit of Legality: A. V. Dicey and the Rule of Law*, in J. Meierhenrich - M. Loughlin (eds.), *The Cambridge Companion to the Rule of Law*, Cambridge UK, 2021, 153 ff.

legal requirements.

Modern legal philosophy has offered contrasting accounts of what the rule of law requires. Joseph Raz, in his seminal essay "The Rule of Law and Its Virtue," insisted that the rule of law is a *formal* virtue of legal systems.[30] For Raz, law must be capable of guiding behaviour: it should be general, prospective, clear, relatively stable, and applied by an independent judiciary. This "thin" conception has been influential in both scholarship and jurisprudence and continues to underpin arguments that the rule of law is primarily about foreseeability and legal certainty.[31]

By contrast, Lon Fuller proposed that law possesses an «inner morality»[32] consisting of requirements such as generality, publicity, clarity, non-contradiction, non-retroactivity, stability, and congruence between official action and declared rule. Although Fuller's account is sometimes classified as formal, his insistence that these requirements express a moral dimension of legality suggests a bridge between the thin and thick conceptions:[33] even the formal demands of law presuppose a normative commitment to treating individuals as subjects capable of understanding and following rules. Fuller's account resonates with the EU's concern for legitimate expectations, non-retroactivity, and coherence, all of which are now entrenched as general principles of Union law.[34]

Another relevant contribution comes from Jeremy Waldron's emphasis on procedure, as anticipated, which illustrates why the rule of law cannot be reduced to abstract legality.[35] For him, the essence of legality lies in the possibility for individuals to contest decisions and to receive reasons: a view that resonates strongly with the Union's insistence on effective judicial protection,[36] also addressed strongly by the Venice Commission's understanding of the rule of law.[37] On the other hand, Paul Craig's well-known distinction between formal and substantive conceptions confirms this point: rules may be general and clear, but without substantive guar-

[30] J. Raz, *The Rule of Law and its Virtue*, cit.

[31] See P. Craig, *Formal and substantive conceptions of the rule of law: an analytical framework*, London, 2017.

[32] L. L. Fuller, *The Morality of Law*, Yale, 1969.

[33] For a critical analysis of Fuller's conceptualisation of «inner morality», see, *ex multis,* P. P. Nicholson, *The Internal Morality of Law: Fuller and His Critics*, in *Ethics*, 84(4), 1974, 307 ff.; K. Rundle, *The Morality of the Rule of Law: Lon L. Fuller*, in J. Meierhenrich - M. Loughlin (eds.), *The Cambridge Companion to the Rule of Law*, Cambridge UK, 2021, 186 ff.

[34] For a broader reflection on the topic, see T. Tridimas, *The General Principles of Law in the European Union Legal Order*, in T. Tridimas (eds.), *The General Principles of EU Law*, Oxford, 2006.

[35] J. Waldron, *The Rule of Law*, cit., 3.

[36] As argued by Pitruzzella, «the independence of judges falls within the scope of EU law and is considered essential to guarantee the fundamental right to a fair trial, which, in turn, is necessary to ensure all the rights that individuals derive from EU law, safeguarding the value of the rule of law», in G. Pitruzzella, *Stato di diritto, indipendenza delle corti e sovranità popolare: armonia o conflitto*, in *Rivista di Diritti comparati*, 3, 2018, 9 ff. (aut. tr.).

[37] S. Granata-Menghini-S. Ninatti, *Chapter 10: The evolving paradigm of human rights protection as interpreted and influenced by the Venice Commission*, in L. Violini-A. Baraggia (eds.), *The Fragmented Landscape of Fundamental Rights Protection in Europe,* Cheltenham, 2018, 201 ff.

antees of equality and rights, legality becomes hollow.[38] Conversely, rights guarantees without procedural channels degenerate into vague aspirations. András Sajó has warned that this fragility is intrinsic: the rule of law is frequently invoked rhetorically while eroded in practice.[39] This insight is particularly relevant to the Union, where rule-of-law discourse has become central in confronting constitutional backsliding,[40] but is equally applicable to the technological sphere. Artificial intelligence illustrates the same risk: legality may be formally present through compliance checklists, while, in practice, access to reasons and remedies is curtailed.[41]

The multiplicity of these accounts should therefore be read not as a weakness but as evidence of the layered nature of the rule of law in modern constitutionalism. Nonetheless, the fragility noted by Sajó, and proved in factual terms by the so-called "rule of law crisis" or the "rule of law backsliding"[42] reminds us that these guarantees are never secured once and for all but require constant vigilance, especially when new modalities of exercising power, such as AI systems, enter the legal order.

In the European Union, this plural heritage has been crystallised into legal form. Art. 2 TEU elevates the rule of law to a foundational value;[43] art.

[38] P. Craig, *Formal and substantive conceptions of the rule of law: an analytical framework*, cit., 6.

[39] As the scholar acknowledges, «the rule of law is "an unqualified human good." But the rule of law can be easily highjacked and turned into rule by law; it is also a technique of those who grabbed state power lawfully to impose their will in a seemingly legitimate manner. Moreover, it is often self-defeating or unable to provide guidance especially where political and politicized actors would like to abuse the legal loopholes»; in A. Sajó, *Militant Rule of Law*, in *Verfassungsblog*, 20 December 2023.

[40] C. I. Nagy, *The Diagonality Problem of EU Rule of Law and Human Rights: Proposal for an Incorporation à l'européenne*, in *German Law Journal*, 21(5), 2020, 838 ff.; O. Polański, *Poland : another episode of «rule of law backsliding» - Judgment P 7/20 and a threat to the integrity of the EU legal order*, in *Public Law*, 2022, 153 ff.; K. L. Scheppele *et al.*, *EU Values Are Law, after All: Enforcing EU Values through Systemic Infringement Actions by the European Commission and the Member States of the European Union*, in *Yearbook of European Law*, 39, 2020, 3 ff.

[41] As stressed from the digital point of view by G. De Gregorio-S. Demková, *The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe*, in C. van Oirsouw *et al.* (eds.), *European Yearbook of Constitutional Law 2023: Constitutional Law in the Digital Era*, The Hague, 2024, 223 ff.

[42] It goes beyond the scope of this paper to analyse the crucial and critical problem of the general erosion of the rule of law, since the focus rests upon its integration with the technology and, moreover, the AI perspective. However, on the notion of "rule of law backsliding" and the ongoing "rule of law crisis" in the EU, see *ex multis* N. Canzian, *The European Principle of Judicial Independence: The Case of Poland*, in *Quaderni costituzionali*, 2, 2020; A. von Bogdandy *et al.*, *Un possibile «momento costituzionale» per lo Stato di diritto europeo: i confini invalicabili*, in *Quaderni costituzionali*, 4, 2018, 855 ff.; B. Bakó, *Hungary's Latest Experiences with Article 2 TEU: The Need for 'Informed' EU Sanctions*, in A. von Bogdandy *et al.* (eds.), *Defending Checks and Balances in EU Member States: Taking Stock of Europe's Actions*, Heidelberg, 2021, 35 ff.; M. Wiącek, *Constitutional Crisis in Poland 2015–2016 in the Light of the Rule of Law Principle*, in A. von Bogdandy *et al.* (eds.), *Defending Checks and Balances in EU Member States: Taking Stock of Europe's Actions*, Heidelberg, 2021, 15 ff.

[43] Nonetheless, as referenced by Schroeder, «the Commission and the courts when enforcing the rule of law vis-à-vis a certain Member State, however, cannot simply refer to art. 2 TEU and content themselves to an "I know it when I see it" approach». See W. Schroeder, *The Rule of Law As a Value in the Sense of Article 2 TEU: What Does It Mean and Imply?*, in A. von Bogdandy *et al.* (eds.), *Defending Checks and Balances in EU Member States: Taking Stock of Europe's Actions*, Heidelberg, 2021, 106.

19(1) TEU obliges Member States to ensure remedies sufficient to guarantee effective judicial protection in fields covered by Union law; and art. 47 of the Charter secures the individual right to «challenge in court the legality of any decision or any other national measure relating to the application of any Union act to them»[44] before an independent and impartial tribunal. The Court of Justice has treated these provisions as enforceable standards, most famously in *Associaçao Sindical dos Juizes Portugueses contra Tribunal de Contas* (C-64/16),[45] where it held that art. 19(1) TEU concretises the rule of law value in art. 2 and binds Member States whenever their courts may rule on EU law. In *Rosneft* (C-72/15),[46] the Court declared that «the very existence of effective judicial review designed to ensure compliance with provisions of EU law is of the essence of the rule of law».
The lesson from these debates is that the rule of law is best understood not as a final state but as a dynamic principle that operates simultaneously at different levels. For European constitutionalism, it is also a structural principle that serves as the means for securing fundamental rights and constraining arbitrariness. This layered conception provides the bridge for analysing the impact of artificial intelligence. For if AI redistributes how power is exercised,[47] by embedding normative choices in technical design and by reconfiguring administrative and private decision-making, the rule of law is the measure by which we can determine whether these exercises of power remain legally constrained and rights protective.

2.1. The EU's Conception of Rule of Law: A Means, Not a Goal

The preceding discussion has shown that the rule of law cannot be reduced to a single, unitary formula. As described, it is a layered concept encompassing legality, certainty, equality, participation and access to judicial protection. Specifically, what emerges is that, if the rule of law functions as a means of ensuring that rights are real and arbitrariness constrained, the European Union provides a paradigmatic illustration of how that principle can be constitutionalised.[48] While art. 2 TEU elevates the rule of law to a foundational value, art. 19(1) TEU obliges Member States to provide remedies sufficient to secure effective judicial protection, and art. 47 of

[44] G. Pitruzzella, *Stato di diritto, indipendenza delle corti e sovranità popolare: armonia o conflitto*, cit., 6.

[45] See ECJ, Case C-64/16, *Associação Sindical dos Juízes Portugueses (ASJP) v Tribunal de Contas*, 27 February 2018, cit.

[46] See ECJ, Case C-72/15, *PJSC Rosneft Oil Company v Her Majesty's Treasury and Others,* 28 March 2017, §73.

[47] See F. Pasquale, *Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication*, in A. Reichman *et al.* (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge UK, 2021, 42 ff.; S. Rosengrün, *Why AI is a Threat to the Rule of Law*, in *Digital Society*, 1, 2022, 2 ff.

[48] A. von Bogdandy *et al.*, *Un possibile «momento costituzionale» per lo Stato di diritto europeo: i confini invalicabili*, cit.; G. Pitruzzella, *Stato di diritto, indipendenza delle corti e sovranità popolare: armonia o conflitto*, cit., 7.

the Charter enshrines an individual right to a remedy.[49] Taken together, these provisions show that formal legality and substantive protection are not alternatives. Formal legality without substantive protection would mean stability without justice; substantive rights without formal legality would mean aspirations without enforceability.[50]

It is, however, the Court of Justice that has transformed the rule of law from a value to an enforceable standard by reading it through the combined lenses of art. 19(1) TEU and art. 47 CFR.[51] Specifically, judicial independence, impartiality and access to remedies have been recognised as structural requirements of art. 19(1) TEU, indispensable for the right to effective judicial protection.[52] In a series of cases against Poland,[53] the Court confirmed that measures undermining irremovability, equality between judges or the freedom to make preliminary references breach the rule of law. In *Repubblika*,[54] it made clear that these guarantees are not mere accession conditions but permanent obligations. Other decisions, such as *LM*,[55] linked the rule of law directly to individual rights. From this line of case law emerges a doctrinal triangle: art. 2 TEU formulates the value, art. 19(1) TEU imposes the obligation, and art. 47 CFR secures the individual right. Together, they constitutionalise the rule of law as both a structural principle of the Union and a justiciable entitlement for individuals.[56]

---

[49] See, for instance, ECJ, Case C-362/14, *Schrems v. Data Protection Commissioner*, §60, «the European Union is a "union based on the rule of law"».

[50] Bast and von Bogdandy describe the rule of law as a "structural principle" of the Union, one that pervades the legal order and ensures the conditions under which rights can be vindicated. Their analysis makes clear that the rule of law has no independent existence apart from the guarantees it furnishes for legality, equality and judicial review. Similarly, Casolari has argued that the protection of fundamental rights in EU law is mediated through rule-of-law structures: without legality, clarity and review, rights remain aspirational. This underscores that the rule of law is not an ornament in the Union's constitutional architecture but the mechanism through which values are translated into enforceable claims. See A. von Bogdandy *et al.*, *A Potential «Constitutional Moment» for the European Rule of Law: The Boundaries Not to Be Crossed*, in *Quaderni costituzionali*, cit., 7.

[51] S. Peers *et al.*, *Article 47*, in *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, 2021, 1245 ff.; K. Gutman, *The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?*, in *German Law Journal*, 20(6), 2019, 884 ff.

[52] S. Prechal, *Article 19 TEU and National Courts: A New Role for the Principle of Effective Judicial Protection?*, in G. Gentile *et al.* (eds.), *Article 47 of the EU Charter and Effective Judicial Protection, Volume 1: The Court of Justice's Perspective*, United Kingdom, 2022.

[53] ECJ, C-619/18, *European Commission v Republic of Poland,* 24 June 2019 (on the independence of the Supreme Court); Case C-192/18, *European Commission v Republic of Poland* (on the independence of ordinary courts), 5 November 2019; Case C-791/19, *European Commission v Republic of Poland* (on the disciplinary regime for judges), 15 July 2021.

[54] In ECJ, Case C-896/19, *Repubblika v Il-Prim Ministru*, 20 April 2021, the Court stressed that judicial independence and effective remedies are not mere accession requirements but permanent obligations under art. 2 TEU

[55] In Case C-216/18 PPU, *Minister for Justice and Equality v LM* (Celmer), 25 July 2018, the Court further held that systemic deficiencies in judicial independence in a Member State may justify refusal to execute a European Arrest Warrant, thereby linking the rule of law directly to individual rights.

[56] As Smuha observes, rule-of-law discourse must incorporate human rights and

Ultimately, legislative and policy practices have reinforced this transformation. The Venice Commission's Rule of Law Checklist has provided a shared vocabulary for monitoring compliance,[57] while Regulation (EU) 2020/2092[58] and the Recovery and Resilience Facility have operationalised conditionality by linking access to EU funds to verifiable safeguards.[59] Most recently, the EU has embedded these benchmarks in its own institutional practice through the annual Rule of Law Report.[60] As clarified in the 2025 Communication on the methodology, the Report translates art. 2 TEU into concrete indicators covering legality, legal certainty, prevention of abuse of power, equality and access to justice. By structuring an annual cycle of monitoring around these benchmarks, the Commission has confirmed that the rule of law is conceived not as an aspiration but as a set of verifiable conditions for rights protection.[61] This development aligns EU practice with the Venice Commission's Checklist, demonstrating a convergence between constitutional theory, judicial enforcement, and policy monitoring.[62]

This evolution provides the benchmark for new regulatory domains. If that is the European Union's constitutional grammar, then any serious engagement with AI must show how the same conduits are maintained when decisions are generated by systems that learn, adapt and obscure their reasoning. That is the challenge of autonomy.

3. Rule of Law and AI: The Challenge of Autonomy

The preceding section reconstructed the Union's understanding of the rule of law as both structural and instrumental, anchored in legality, judicial independence, and effective remedies. That "constitutionalisation" provides the benchmark against which new forms of governance must be

accountability if it is to impose real constraints on emerging forms of power, in N. A. Smuha (ed.), *From Rule of Law to Algorithmic Rule by Law*, cit., 2.

57 G. Repetto, *The constitutional relevance of the ECHR in domestic and European law*, Cambridge-Antwerp-Portland, 2013.

58 Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget. See also *Rule of Law Conditionality Regulation: European Implementation Assessment | Think Tank | European Parliament*, 2025.

59 D. Kochenov, *EU Enlargement and the Failure of Conditionality*, The Hague, 2008; for a critical standpoint, see A. Baraggia, *Democratic Blackmail. The Use of Conditionality to Protect the Rule of Law*, in *Quaderni costituzionali*, 2, 2023, 355 ff.

60 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "2025 Rule of Law Report. The rule of law situation in the European Union", Strasbourg, 8.7.2025 COM(2025) 900 final.

61 As mentioned *supra,* a means more than a goal. See T. Tridimas, *The General Principles of Law in the European Union Legal Order*, cit., 6.

62 Not in contrast with the concept of autonomy of EU Law, as also reaffirmed in K. Lenaerts, *Upholding the Rule of Law through Judicial Dialogue*, in *Yearbook of European Law*, 38, 2019, 3 ff.

assessed.

Artificial Intelligence is the most immediate test of this standard: in particular, the emergence of AI autonomy marks a pivotal shift in the landscape of digital governance, with far-reaching implications for constitutional principles and regulatory frameworks. Consider automated decision-making systems in welfare or credit scoring: [63] when opaque algorithms determine access to essential services, individuals may be unable to understand or contest the reasons behind outcomes, undermining both autonomy and effective redress.[64] Even more directly, generative AI tools deployed in political campaigning illustrate how AI can manipulate individual preferences at scale, blurring the line between free choice and engineered behaviour.[65] These dynamics expose how AI risks converting the law's role from a framework for autonomous agency into a tool of subtle coercion.

By redistributing where and how decisions are made, AI systems bring into play precisely the guarantees the European Union has attached to the rule of law, as outlined *supra*.

As remarked also elsewhere, «the autonomy of AI systems challenges traditional notions of accountability and oversight, prompting scholars and policymakers to seek new frameworks that can properly regulate these technologies while upholding constitutional values such as democracy, the rule of law, and fundamental rights. For example, the lack of transparency of some AI decisions may pose a direct challenge to the constitutional principle of due process, which requires that decisions, particularly those affecting the rights of individuals, be understandable and appealable».[66]

One way of understanding this evolution is through the different phases of digital constitutionalism.[67] Specifically, the first era revolved around addressing the power of platforms like Google, Facebook, and Amazon, ensuring they remained accountable within a framework of fundamental rights and democratic oversight. This era, often described as the first phase of was largely reactive, as courts like the ECJ played a pivotal role in translating traditional constitutional principles to the digital sphere.[68] However, as the algorithmic society gave way to the rise of AI-driven au-

[63] These are some of the most critical sectors which are indeed classified by the Regulation (EU) 2024/1689, as mostly "high risk", therefore, subject to most of the obligations under the AI Act.

[64] T. Aimen, *Cognitive freedom and legal accountability: Rethinking the EU AI act's theoretical approach to manipulative AI as unacceptable risk*, in *Cambridge Forum on AI: Law and Governance*, 1, 2025, 20 ff.

[65] M. Groh *et al.*, *Human detection of political speech deepfakes across transcripts, audio, and video*, in *Nature Communications*, 15(1), 2024, 7629 ff.

[66] O. Pollicino, *Regolare l'Intelligenza Artificiale: la lunga via dei diritti fondamentali*, in O. Pollicino *et al.* (eds.), *La disciplina dell'intelligenza artificiale*, Milan, 2025. The quoted text was translated by the authors.

[67] For accounts that frame the evolution of digital constitutionalism in terms of successive phases, see O. Pollicino, *Potere digitale*, in M. Cartabia - M. Ruotolo (eds.), *Potere e Costituzione. Enciclopedia del diritto: i tematici*, Rome, 2023.

[68] The aspects hereby mentioned have been further analysed in O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, London, 2021.

tonomy, the regulatory focus expanded.[69] No longer confined to holding platforms accountable, governance now faces the challenge of managing systems capable of self-learning, adaptation, and decision-making beyond explicit human instructions.

Consequently, a second phase, oriented towards the development of regulatory frameworks, started, e.g., with the General Data Protection Regulation (GDPR)[70]: it was specifically designed to impose checks on the power of these platforms, ensuring that they did not violate individual rights.

Moreover, since the second half of the 2010s, the EU has adopted a series of sector-specific legislative measures aimed at introducing new obligations for providers – and especially for hosting service providers – in order to make them more responsible for combating illegal conduct and material online. Thus, with the Directive (EU) 2018/1808,[71] the legislator amended the regulation of audiovisual media, introducing a series of obligations for providers of video-sharing platforms; the Directive (EU) 2019/790 innovated in the field of copyright to adapt the sector legislation to the new challenges of the Internet;[72] the Regulation (EU) 2021/784 introduced a specific discipline aimed at combating online terrorist content.[73]

Moreover, in 2022, with the approval of the Digital Services Act (DSA) a general and, so to speak, "horizontal" reform of the European regulatory framework on the moderation of online content was finally carried out.[74]

Hence, the second phase represents a procedural turn, where the focus shifted towards creating robust mechanisms for ensuring transparency, accountability, and the enforcement of digital rights, by giving more and more supervisory powers to the European Commission.[75]

This evolution represents a profound transformation in the regulatory landscape: one that demands a shift from principles of algorithmic governance to those capable of addressing the complexities of AI autonomy.

---

[69] O. Pollicino, *Potere digitale*, cit., 10.

[70] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[71] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, 2018 O.J. (L 303) 69.

[72] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the digital single market and amending Directives 96/9/EC and 2001/29/EC.

[73] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, 2021 O.J. (L 172) 79.

[74] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

[75] P. Van Cleynenbreugel, *The Commission's digital services and markets act proposals: First step towards tougher and more directly enforced EU rules?*, in *Maastricht Journal of European and Comparative Law*, 28(5), 2021, 667 ff.

Autonomous systems, unlike traditional automated processes, introduce novel challenges due to their ability to function without human oversight, relying on self-learning mechanisms and adaptive algorithms. While these capabilities enable unprecedented efficiency and innovation, they also pose risks to transparency, accountability, and the protection of fundamental rights. These challenges are particularly acute in areas like law enforcement, where AI's capacity for autonomous decision-making directly impacts privacy, non-discrimination, and other core rights.[76] The pervasive influence of the algorithmic society extends beyond information management into various other contexts, such as healthcare, labour, justice, and public security. In these sectors, too, we witness the widespread adoption of automated decision-making systems, which not only reinforce the role of algorithms but also highlight the increasingly intertwined relationship between public and private entities. This growing presence of private actors in traditionally public domains underscores a significant shift in governance structures.[77]

However, as we transition from an algorithmic society to one increasingly driven by AI, this shift takes on even greater complexity. Moreover, the development of the AI regulatory framework discussed in this chapter was a direct response to the profound effects these systems were having on fundamental rights and societal norms. These regulations often emerged as reactive measures, spurred by public outrage over specific incidents where AI technology demonstrated its capacity to infringe on human rights.

A particularly prominent example is the use of COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), an algorithm used in the U.S. criminal justice system to evaluate the likelihood of recidivism. This tool faced significant criticism for perpetuating racial bias, disproportionately labelling Black defendants as high-risk compared to their white counterparts.[78] Such bias undermined the fundamental rights to equality and a fair trial, as COMPAS-influenced decisions directly impacted sentencing and parole outcomes.[79] The opaque nature of the algorithm exacerbated the problem, as individuals had little insight into or recourse against the automated decisions.[80] This lack of transparency in decision-making processes posed serious concerns about due process and the right to a fair and impartial trial, two cornerstones of justice in democratic societies.[81]

---

[76] L. Violante, *Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi*, in *BioLaw Journal - Rivista di BioDiritto*, 1, 2022, 145 ff.

[77] The shift powerfully described by Balkin as the "Algorithmic Society", J. M. Balkin, *Free speech in the algorithmic society: Big data, private governance, and new school speech regulation*, in *UCDL rev.*, 51, 2017, 1149 ff.

[78] *State v. Loomis*, 881 N.W.2d 759 (Wis. 2016).

[79] J. Angwin-J. Larson-S. Mattu-L. Kirchner, *Machine Bias*, in *ProPublica*, 23 May 2016.

[80] F. Lagioia *et al.*, *Algorithmic fairness through group parities? The case of COMPAS-SAPMOC*, in *AI & Society*, 38(2), 2023, 459 ff.

[81] As observed by Simoncini, the outcome of the US Supreme Court did not spark a violation on the right to "due process". Even though the use of these tools may, in fact, give rise to constitutionally relevant issues, but, in the present case, it reiterates the diriment argument of non-exclusivity: the algorithm was not the sole reason for the

Another high-profile incident was the Clearview AI scandal, which revealed that the company had scraped billions of images from social media without user consent to build a facial recognition database for law enforcement use.[82] The widespread deployment of this technology, often without adequate public oversight, raised serious concerns about the right to privacy and data protection. Clearview AI's practices were particularly alarming as they infringed on individuals' control over their personal data, enabling unwarranted surveillance and tracking without their knowledge or consent.[83] This form of pervasive surveillance also had broader implications for freedom of expression and assembly, as individuals might hesitate to exercise these rights under the belief they were being constantly monitored. The case sparked international debates on the ethical use of facial recognition technology and highlighted its potential for misuse by both public and private entities.[84]
In addition to these cases, the rise of generative AI has introduced new regulatory challenges, as demonstrated by the OpenAI case in Italy in 2023.[85] Italy's Supervisory Authority temporarily banned OpenAI's ChatGPT due to concerns over the unlawful collection and processing of personal data, and the lack of adequate mechanisms to prevent minors from accessing the platform. The case raised questions about how generative AI systems collect, store, and use personal information, especially when operating at such large scales.[86] The *Garante* ordered OpenAI to implement stronger privacy safeguards and transparency measures, including age verification tools and greater user control over their data. The incident attracted widespread attention, marking the first regulatory action taken against a major generative AI system in Europe. As a consequence of this huge societal echo, the regulation of such systems entered the radar of the European legislator, which eventually included specific provisions in the first European law on AI.[87]

---

decision and, hence, was found to not being violating the principle of "due process". A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal-Rivista di BioDiritto*, 15(1), 2019, 63 ff.

[82] The case was addressed by numerous authorities: especially the Italian Supervisory Authority (SA, Garante) fined the US-based company Clearview AI EUR 20 million after finding it applied what amounted to biometric monitoring techniques also to individuals in the Italian territory, and it impeded the processing of biometric data of Italian citizens. Italian SA, Injunction Order against Clearview AI - 10 February 2022, Register of Measures, No. 50 of 10 February 2022. A similar direction was followed by the French Supervisory Authority (CNIL), Deliberation of the restricted committee N° SAN-2022-019 of 17 October 2022 concerning Clearview AI.

[83] The case and its far-reaching data protection and fundamental rights implications have also been analysed in this contribution:

[84] K. Hill, *The Secretive Company That Might End Privacy as We Know It,* in *The New York Times,* 18 January 2020.

[85] Italian SA, Measure of 30 March 2023, Register of Measures, No. 112 of 30 March 2023.

[86] G. Riva, *Diritto e Intelligenza Artificiale Generativa: L'istruttoria Del Garante per La Protezione Dei Dati Italiano Su OpenAI e ChatGPT*, in *Ciberspazio e diritto : rivista internazionale di informatica giuridica*, 25(1), 2024 153 ff.

[87] European Parliament, Amendments adopted by the European Parliament on 14 June

Henceforth, the episodes involving COMPAS, Clearview AI, and OpenAI highlight the urgent need for comprehensive AI regulations, particularly in light of the growing autonomy of these systems. AI's ability to function independently – learning, adapting, and making decisions with minimal human intervention – raises profound concerns about safeguarding fundamental rights. Issues such as discrimination, bias, privacy violations, and data security are exacerbated by the opacity and unpredictability inherent in autonomous AI systems. These cases reveal a pattern of reactive regulation, where lawmakers address specific incidents only after harm has occurred, rather than proactively anticipating the broader challenges posed by AI's autonomous capabilities. This reactive approach has created a precarious "cat-and-mouse" dynamic, with legislators scrambling to address the consequences of increasingly autonomous systems while struggling to develop long-term, comprehensive frameworks. As AI continues to evolve, this cycle of reactionary governance risks leaving significant gaps in oversight, exposing society to ongoing and unforeseen vulnerabilities. By failing to account for the unique challenges of AI autonomy, current regulatory efforts may fall short of effectively addressing the transformative and disruptive potential of these technologies.

4. Understanding Autonomy: The Technical Perspective

The growing autonomy of AI systems is indeed visible also from a technical perspective: AI's evolution from symbolic systems to machine learning and agentic architectures reshapes how power is exercised.[88] Early symbolic AI was rule-based: deductive instructions, written in logical languages, applied to data to produce transparent and predictable outputs.[89] Such systems posed legal questions, the validity of the legal basis, fairness of outcomes, but within relatively inspectable structures. Thus, contemporary AI is largely sub-symbolic.[90]

2023 on the proposal for an Artificial Intelligence Act, COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), Amendment 168.

[88] Transatlantic Reflection Group on Democracy and the Rule of Law in the Age of "Artificial Intelligence", *A manifesto on enforcing law in the age of «artificial intelligence»*, in *European Law Journal : Review of European Law in Context*, 29(1–2), 2023, 249 ff.

[89] It is to note now that, then, the so-called intelligence of the system is associated with this ability to learn, and not just symbolise and, therefore, reproduce behaviours. This distinction is crucial to understanding the shift from automation and autonomy that is pursued by the AI Act. On this ability to infer and the elements characterising symbolic AI S. Harnad, *The Symbol Grounding Problem*, in *Physica D: Nonlinear Phenomena*, 42, 1–3, 1990, 335 ff.; S. Leonelli, *What distinguishes data from models?*, in *European Journal for Philosophy of Science*, 9(2), 2019, 22 ff.; S. Wachter-B. Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI Survey: Privacy, Data, and Business*, in *Columbia Business Law Review*, 2, 2019, 494 ff. For a purely technical perspective, see M. L. Minsky, *Logical Versus Analogical or Symbolic Versus Connectionist or Neat Versus Scruffy*, in *AI Magazine*, 12(2), 1991, 34 ff.

[90] A. Akbari, *Facial Recognition Technologies 101: Technical Insights*, in M. Zalnieriute-R. Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State*,

The modern AI techniques, such as sub-symbolic AI approaches, encompass a variety of processes.[91] Machine learning, deep learning and neural networks no longer rely on preset rules but extract patterns from large datasets. These techniques identify correlations, infer rules, and generate behaviour that appears autonomous. Generative AI,[92] building on deep neural architectures, produces novel content – i.e., text, images, code – by modelling linguistic and statistical patterns. The most recent development is agentic AI, designed to pursue complex goals autonomously using reinforcement learning and adaptive decision-making, with limited human input.[93]

Moreover, machine learning can be "supervised", or "unsupervised". The supervised approach systems are trained on labelled datasets where inputs are paired with known outputs. For example, in facial recognition, the system might be trained using pairs of images labelled as "same person" or "different person" to learn how to compare facial features accurately.[94] In a context which is, instead, "unsupervised", it is the system that should identify patterns or clusters within the data on its own. Saying it differently, such connections are made without receiving instructions or learning from external sources, as in the supervised learning environment. In the biometric identification context, the use of unsupervised learning might involve group analysis distinguishing people for biometric features – long neck, big mouth, small eyes – or emotions, like happiness or anger, without knowing these features before or the exact names for these emotions. Therefore, the human "gives" to the system the data, without labelling "what we are looking for".

Finally, the third category is "reinforcement learning". This approach trains systems by rewarding desired behaviours and penalising undesired ones: «[it] is used when neither the samples nor the answers are available as a batch in the beginning».[95] These systems are, for instance, used for playing video games by maximising their score through trial and error. Another example might be that of self-driving cars. It starts with no knowledge of how to drive, but it learns by trial and error. The system is rewarded for actions like staying in the correct lane, stopping at traffic lights, and avoiding collisions, while penalties are applied for running red lights or hitting obstacles.

Cambirdge MA, 2024.

[91] Among others, P. Wang-E. Fan, *Comparative Analysis of Image Classification Algorithms Based on Traditional Machine Learning and Deep Learning*, 141, 2021, 61 ff.

[92] Art. 3(63) AI Act defines a "general-purpose AI model" as «an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market».

[93] P. Bornet-J. Wirtz, *Agentic artificial intelligence: harnessing AI agents to reinvent business, work, and life*, Ebook, 2025.

[94] *Ibid.*

[95] A. Akbari, *Facial Recognition Technologies 101: Technical Insights*, cit., 14.

A particular branch of machine learning is that of "deep learning".[96] This latter one is a specialised subset that uses neural networks to model complex, high-dimensional data. One of the most renowned uses of deep learning systems is specifically to create systems that can understand and analyse human language. Those systems present numerous and different applications, for instance, in the content moderation sector[97], as well as potential challenges due to their complexity and, *ça va sans dire,* opacity.
Key architectures in deep learning include: i) Convolutional Neural Networks (CNNs), ideal for image processing tasks, CNNs are widely used in facial recognition and medical imaging; Recurrent Neural Networks (RNNs), designed for sequential data, RNNs excel in tasks like speech recognition and time-series analysis; iii) Transformer Models, these are at the heart of large language models (LLMs) like OpenAI's GPT-4, enabling advanced natural language processing and generation. In this sense, deep learning has transformed AI by enabling systems to tackle tasks that were previously thought to be impossible, such as real-time language translation and autonomous driving. However, it also introduces challenges. Neural networks often function as "black boxes," making it difficult to interpret how they arrive at their decisions.
These technical shifts have direct constitutional implications. Symbolic AI challenged legality but remained tethered to explicit rules. Sub-symbolic and agentic AI redistribute decision-making into opaque technical architectures, diminishing foreseeability and accountability. When systems "learn" and adapt beyond their initial programming, it becomes harder to attribute responsibility, human oversight is reduced to auditing, and contestability is weakened. Autonomy in AI thus produces new rule-of-law concerns: ensuring legality, foreseeability, and effective remedies when decisions are no longer authored but generated.
Therefore, while early algorithmic systems primarily served to assist human decision-making by analysing vast amounts of data,[98] AI-driven systems now possess the capability to make decisions autonomously, for their technical advances described *supra.*[99]
This change is more than a technical enhancement; it alters the dynamics of governance, as AI assumes responsibilities traditionally held by hu-

[96] «Deep-learning methods are representation-learning methods with multiple levels of representation at one level (starting with the raw input) into a representation at a higher, slightly more abstract level. With the composition of enough such transformations, very complex functions can be learned. For classification tasks, higher layers of representation amplify aspects of the input that are important for discrimination and suppress irrelevant variations […] The key aspect of deep learning is that these layers of features are not designed by human engineers; they are learned from data using a general-purpose learning procedure», Y. LeCun *et al.*, *Deep learning*, in *Nature*, 521(7553), 2015, 436 ff.

[97] O. Pollicino-P. Dunn, *IA e valori democratici*, in *Intelligenza Artificiale e Disinformazione*, Milan, 2024.

[98] K. Yeung, *Algorithmic regulation: A critical interrogation*, in *Regulation & Governance*, 12(4), 2018, 505 ff.

[99] There are many areas in which AI is used and which affect the fundamental rights of individuals. Among others, it is to mention the law enforcement sector S. van Schendel, *Regulating Risk Profiling by Law Enforcement: A Task for Data Protection Law, Non-Discrimination Law and Criminal Procedural Law*, Tilburg, 2024.

mans, including tasks that directly affect constitutional rights such as freedom of expression, privacy and data protection.
Moreover, this change is reflected by the definition that the AI Act adopted for AI systems[100], AI as «a machine-based system designed to operate with varying levels of autonomy.»[101] In this context, autonomy refers to the ability of AI systems to act independently of human intervention, making decisions or taking actions without requiring constant oversight.[102] Adaptiveness, on the other hand, highlights the self-learning capabilities of these systems, allowing them to evolve, improve, or modify their behaviour over time as they interact with data and environments.
However, what truly distinguishes AI from conventional software is its ability to "infer", as also mentioned by the very definition of AI systems in Regulation (EU) 2024/1689. While traditional software operates through predefined, step-by-step instructions set by developers, AI systems possess the capacity to analyse data, draw conclusions, and make decisions without explicit human direction. This ability to infer empowers AI systems to engage in higher-order tasks like learning, reasoning, and modelling, moving far beyond basic data processing.[103]
This perspective underscores the complexity of AI systems compared to traditional software. AI's ability to continuously learn, reason, and improve makes it a transformative technology that requires specific regulatory oversight.[104]
Such an evolution – that in technical terms marked the passage from symbolic to sub-symbolic AI – is specifically characterised by the shift from algorithmic governance to AI-driven one: this passage represents a profound transformation of the regulatory landscape.[105]
As a matter of fact, the term "algorithmic governance" traditionally refers to the use of automated decision-making (ADM) systems that process

---

[100] It is to note that the AI Act does not define AI, but just AI systems.

[101] AI Act, art. 3, para. 1, no. 1). As mentioned *supra,* this definition is borrowed by the OECD.

[102] AI Act, Recital 12.

[103] AI Act, Recital 12, «include machine learning approaches that learn from data how to achieve certain objectives; and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved», with either implementation going «beyond basic data processing» and enabling «learning, reasoning or modelling». Hence, the AI Act further elaborates on the techniques that enable this inference capability. Two main approaches are identified: machine learning methods, which allow systems to learn from data and adapt to achieve certain objectives, and logic- or knowledge-based approaches, which use encoded rules or symbolic reasoning to solve tasks. Both approaches enable AI systems to function in a way that is not only independent but also dynamic, adapting to new data and situations.

[104] As autonomy increases, assigning responsibility becomes gradually difficult, given the diminished importance or relevance or «control over the system due to its high degree of autonomy and capacity for self-learning», cit. A. Jedličková, *Ethical Approaches in Designing Autonomous and Intelligent Systems: A Comprehensive Survey towards Responsible Development,* in *AI & Society*, 2024.

[105] «Algorithmic technologies are not only instruments to exercise powers, which can interfere with fundamental rights, but can also be considered as rule-makers», in G. De Gregorio, *The Normative Power of Artificial Intelligence*, 2023, cit.*,* 2.

large volumes of data based on pre-defined criteria.[106] ADM, in this context, involves using algorithms, a sequence of steps expressed in mathematical or logical terms, embedded within decision-making processes.[107] These systems range from fully automated decisions to hybrid approaches – i.e., purely automated decisions, automated triage, automated suspects and automated trials[108] – where algorithmic outputs assist human decision-making.[109] However, a recurring challenge lies in ensuring that these outputs do not merely shift responsibility away from human actors or obscure accountability through their complexity and opacity.[110]

While ADM systems have traditionally involved structured, rule-based automation, the emergence of AI introduces a layer of autonomy and adaptability, enabling systems to learn and evolve beyond static criteria. Unlike traditional algorithms, AI systems leverage advanced methodologies, such as machine learning, to generate outputs that are not always easily explainable, raising significant concerns about transparency, fairness, and accountability.[111] This shift from structured automation to autonomy represents a profound challenge for constitutional law, which has not yet fully adapted to address the opacity, adaptability and unpredictability of these systems.[112] Moreover, as Demkova highlights, the right to human oversight and the ability to contest algorithmic decisions are safeguards that must be robustly implemented to mitigate the risks associated with ADM systems and uphold fundamental rights.[113] Especially, as also underscored by Pasquale, the risk of the rising AI autonomy is that of eroding individuals,

---

106 S. Demková, *Automated Decision-making and Effective Remedies: The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice*, Chelthenham, 2023; S. Lomborg *et al.*, *Automated decision-making: Toward a people-centred approach*, in *Sociology Compass*, 17(8), 2023, 13097 ff.

107 M. Busuioc, *Accountable Artificial Intelligence: Holding Algorithms to Account*, in *Public Administration Review*, 81, 2020.

108 According to scholarly analysis, ADM can be classified as: solely automated decisions, automated triage, automated suspicion, and automated evidence. For a taxonomy of ADM see F. Palmiotto, *When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis*, in *German Law Journal*, 25(2), 2024, 210 ff.

109 Explanation and reasoning are the key aspects that, as a matter of fact, trigger the put into place of these technologies in the public actors' duties. On the duty of reasons of administrative law, see M. Fink-M. Finck, *Reasoned A(I)dministration: explanation requirements in EU law and the automation of public administration*, in *European Law Review*, 47(3), 2022, 376 ff.

110 It is possible to distinguish between outputs. The classification is based on the position of the "data subject" and its relationship to the output of ADM. The first category of possible outputs of ADM includes evaluations, rankings, predictions, recommendations or classification of content. The ADM lists, classifies, ranks, filters, ranks or recommends. The second category of output concerns decisions made by the WMD concerning the person concerned. In these cases, the person interacting with the ADM is directly affected.

111 L. Edwards-M. Veale, *Slave to the Algorithm? Why a «right to an explanation» is probably not the remedy you are looking for*, in *Duke Law & Technology Review*, 16, 2017, 18 ff.

112 For a technical point of view, M. Soori *et al.*, *Artificial intelligence, machine learning and deep learning in advanced robotics, a review*, in *Cognitive Robotics*, 3, 2023, 54 ff.

113 S. Demková, *Automated Decision-Making and Effective Remedies : The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice*, cit., 16.

trivialising concepts, like the rule of law, «a system of social relationships and legitimate governance, not simply the transfer and evaluation of information about behaviour».[114]

From a technical point of view, the opacity of ADM systems, often described as a "black-box", *supra*, complicates efforts to ensure transparency and accountability, both of which are foundational to constitutional governance. In turn, in the legal environment, it has been advocated for a "right to explanation" of the automated decision, based on an interpretation of art. 22 of the GDPR. While this provision seeks to provide transparency by requiring meaningful information about the logic, significance and consequences of ADM usage, however, it has been criticised for its vagueness and limited practical applicability.[115] This complexity, paired with the risk of superficial compliance by organisations, underscores the inadequacy of current mechanisms to ensure accountability.

Recently, the legal debate has been coupled also with the technical one, resulting in a shift from concepts like "explainable AI" or xAI:[116] since the explanations, while necessary, do not always lead to genuine understanding, it is urged, instead, to strive for "understandable AI" (uAI), meaning going beyond mere explanation to focus on fostering understanding.[117] Particularly, from a technical perspective, this shift can be achieved by building a framework that includes incoming propositions, knowledge bases, knowledge fusion, and confidence-change mechanisms to foster genuine understanding. This system will ensure that explanations are aligned with the users' existing knowledge base and cognitive processes.[118] Saying it in simple words, on the one hand, the purpose of xAI is to explain the internal workings of the model — for instance, by breaking down decisions into understandable components, creating *post-hoc* explanations, or simplifying

---

[114] F. Pasquale, *A Rule of Persons, Not Machines: The Limits of Legal Automation*, in *George Washington Law Review*, 87(1), 2019, 1.

[115] Critics argue that art. 22 does not explicitly mandate full explanations but only "meaningful information," leaving ambiguity about what level of transparency is sufficient. Furthermore, ADM systems, particularly those based on machine learning, make it difficult to offer clear, actionable insights into their decision-making processes. L. Edwards-M. Veale, *Slave to the Algorithm? Why a «right to an explanation» is probably not the remedy you are looking for* (preprint), cit.; M. Fink-M. Finck, *Reasoned A(I)dministration: explanation requirements in EU law and the automation of public administration*, cit.; S. Wachter *et al.*, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 7(2), 2017.

[116] Explainable AI refers to methods and techniques in artificial intelligence (AI) that make the functioning of AI models understandable to humans. The primary objective of xAI is to ensure that the decisions and actions made by AI systems can be interpreted and explained, thereby fostering trust, transparency, and accountability. In particular, xAI aims to provide insights into the internal mechanisms of complex AI models, such as neural networks, which are often considered "black boxes" due to their opacity. See K. Grieman, *Explainable AI (XAI)*, in *Law, Death, and Robots: The Regulation of Artificial Intelligence in High-Risk Civil Applications*, London, 2024, 44 ff.

[117] H. Abbass *et al.*, *Editorial: From Explainable Artificial Intelligence (xAI) to Understandable Artificial Intelligence (uAI)*, in *IEEE Transactions on Artificial Intelligence*, 5(9), 2024, 4310 ff.

[118] V. Rodríguez-Doncel *et al.*, *Introduction: A Hybrid Regulatory Framework and Technical Architecture for a Human-Centered and Explainable AI*, in V. Rodríguez-Doncel *et al.* (eds.), *AI Approaches to the Complexity of Legal Systems XI-XII*, Cham, 2021, 1 ff.

the model to make it interpretable;[119] on the other hand, understandable AI goes beyond merely explaining how decisions are made. It emphasizes creating AI systems that foster a deep understanding for users, especially non-experts.[120] uAI focuses on aligning the system's explanations with the user's cognitive processes and prior knowledge to ensure that users not only receive an explanation but also comprehend it fully. In a nutshell, uAI seeks to make AI models and their outputs more intuitive and meaningful to a wider range of users.

The implications from a are such that appeared in a recent ruling by the Constitutional Court of Colombia underscore the importance of human oversight in AI-driven decision-making. In this case, a judge used ChatGPT 3.5 to assist in drafting a legal decision.[121] The court affirmed that while AI can complement human judgment, it must not replace it. The judge did not rely on AI to resolve the case but rather employed it as a tool to assist in writing the decision, based on reasoning provided by the judge. This case illustrates how AI can be integrated into decision-making in a way that respects human authority and maintains a clear boundary between assistance and autonomy.[122]

Coming back to the European Union context, in the *Schufa* ruling by the ECJ, it emerged that what constitutes "automated decision-making" is not only the actual output of algorithmic analysis.[123] The ECJ established that even if a human is involved in the final decision-making process – e.g., a bank deciding whether to grant a loan – if an automated system, as a credit scoring algorithm, plays a key role in influencing that decision, it may still qualify as automated decision-making under data protection laws.[124] This ruling drew attention to a crucial matter: it is to be considered from a legal stand, not only the "algorithmic output", but the result as a whole, even though a human is involved in the final stage.[125] Essentially, the court found that while the final decision to grant or deny credit may involve human intervention, the credit score itself plays a crucial role in that decision-making process. As such, the automated calculation of the credit score is an integral part of the overall automated decision-making process. Henceforth, the turn from algorithmic governance to AI governance rep-

[119] H. Abbass *et al.*, *Editorial: From Explainable Artificial Intelligence (xAI) to Understandable Artificial Intelligence (uAI)*, cit., 17.

[120] B. D. Mittelstadt *et al.*, *The ethics of algorithms: Mapping the debate*, in *Big Data & Society*, 3(2), 2016, 679 ff.

[121] República de Colombia Corte Constitucional, Ruling T-323/2024, in particular §§ 422-424.

[122] *Ibid.*, § 424, lett. i).

[123] See Case C-634/21, *OQ v. Land Hesse,* 7 December 2023, cit.

[124] L. A. Bygrave, *Article 22 Automated individual decision-making, including profiling*, in C. Kuner *et al.* (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, 2020.

[125] A. Aza, *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context*, in *Industrial Law Journal*, 2024, 35; G. Fasano, *L'interpretazione estensiva della nozione di "decisione automatizzata" ad opera della Corte di giustizia: una prospettiva più ampia ma ancora fragili tutele per le libertà fondamentali*, in *Rivista italiana di informatica e diritto*, 6(2), 2024, 15 ff.

resents a profound transformation in the regulatory landscape, where this shift is essentially driven by the increasing reliance on technological autonomy.[126] This transition, fueled by the increasing reliance on autonomous and adaptive AI systems, fundamentally alters the dynamics of accountability and oversight, necessitating a rethinking of regulatory structures. For the European Union, the central question is whether its regulatory architecture can translate the classical guarantees of the rule of law – legality, fairness, transparency, oversight and remedies – into operational duties fit for AI. The AI Act presents itself as the constitutional response: a framework intended to prohibit practices deemed incompatible with rights, to discipline high-risk systems, and to embed transparency, oversight and accountability into the AI lifecycle. The question is whether this response restores the conduits of the rule of law where autonomy obstructs them, or whether it codifies a compliance regime framed by market integration rather than by rights protection.

5. The AI Act: A Constitutional Response?

The AI Act is a landmark piece of legislation by the European Union, designed to create a "new" legal framework for AI technologies. As a matter of fact, the AI Act promise relied on the idea of building a legal framework of «rules for AI available in the Union market or otherwise affecting people in the Union [that] should therefore be human-centric, so that people can trust that the technology is used in a way that is safe and compliant with the law, including the respect of fundamental rights».[127]
The Regulation, even though of pioneering importance, is not the only attempt at regulating AI. Almost contemporary to the EU, the Council of Europe worked and published its Framework Convention on Artificial Intelligence,[128] establishing rules applicable only to public actors, being the first binding treaty on AI, focusing on protecting human rights, democracy and the rule of law.[129] The growing momentum in regulating AI reflects the increasing global recognition of the profound impact that AI technologies can have on society, necessitating comprehensive legal frameworks to address the ethical, social, and legal challenges posed by these rapidly advancing systems.

---

126 As observed by De Gregorio, «algorithmic technologies are not only instruments to exercise powers, which can interfere with fundamental rights, but can also be considered as rule-makers», in G. De Gregorio, *The Normative Power of Artificial Intelligence*, cit.

127 Explanatory Memorandum published within the proposal for a Regulation of the European Parliament and of the Council, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 21.4.2021, COM(2021) 206 final.

128 Council of Europe (CoE), Framework Convention on artificial intelligence, human rights, democracy and the rule of law, published on 17 May 2024, and open for signatures since 5 September 2024, Council of Europe Treaty Series - No. 225.

129 The Framework Convention has a broader scope of application than the AI Act since it was negotiated by the COE's Member States, together with Ministers or high-level representatives from the Governments of the United States, Canada, Mexico, Japan, Israel, Ecuador, Peru, Uruguay, and Argentina.

On the one hand, the regulatory push highlights the urgent need for international cooperation and alignment to ensure that AI development and deployment are guided by common ethical and legal principles. On the other hand, with the simultaneous efforts by various international bodies, it will be more complex for the European Union to establish undisputed leadership in AI regulation, as it previously did with the General Data Protection Regulation (GDPR)[130] and, to a lesser extent, the Digital Services Act (DSA).[131] The shared efforts in the regulation of AI may dilute the EU's capacity to dominate the conversation entirely, making it essential for the EU to maintain a competitive edge in shaping global AI governance.[132]
Nonetheless, keeping with the tradition already established by other EU regulations, especially the GDPR and the DSA,[133] the AI Act is rooted in a risk-based approach, categorising AI systems into different tiers based on the level of risk they pose, ranging from minimal to prohibited.[134] This approach is intended to safeguard fundamental rights, promote transparency, and build trust in AI systems while maintaining a competitive and harmonised single market within the EU.[135]
The AI systems are categorised into four tiers. At the top of the hierarchy are AI systems that are deemed to have such severe impacts on individual rights that they are outright banned. These include for instance, systems of biometric recognition used in real-time in public spaces for purposes of identification by law enforcement authorities,[136] social scoring systems, or those that use subliminal techniques to manipulate individuals or groups in ways that may cause them harm.[137]
The second level is occupied by high-risk systems.[138] This category covers systems that, while not prohibited, pose significant risk to safety, fundamental rights, and societal interests. The AI Act specifically outlines high-risk sectors in Annex III, including areas such as biometric identification, critical infrastructure, education and vocational training, employment and worker management, access to essential private and public services, law

[130] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

[131] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act).

[132] F.P. Levantino-F. Paolucci, *Advancing the Protection of Fundamental Rights Through AI Regulation: How the EU and the Council of Europe are Shaping the Future*, in *European Yearbook on Human Right*s, Leiden, 2025.

[133] P. Dunn-G. D. Gregorio, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, 59(2), 2022.

[134] In particular, Annex III further specifies art. 6 of the AI Act and lists the AI systems which are considered "by default" by the EU legislator "high risk".

[135] AI Act, art. 3, para. 1, no. 2), «risk means the combination of the probability of an occurrence of harm and the severity of that harm».

[136] AI Act, Annex II details the crime for which such AI systems can be put into place.

[137] AI Act, art. 5.

[138] AI Act, art. 6 and Annex III.

enforcement, migration, asylum, and border control, and judicial administration. This is the most comprehensive category in the AI Act, with the majority of the regulation dedicated to ensuring that these systems are transparent, fair and accurate.[139]

The third level is occupied with limited-risk AI systems.[140] These systems are designed for human interaction, the creation or manipulation of content (including deepfakes),[141] and image or audio generation systems. While not classified as high-risk, they still pose certain challenges, particularly regarding transparency. As a result, they are subject to specific transparency obligations, ensuring that users are aware when interacting with AI systems.[142]

At the base of the hierarchy are AI systems with minimal risk, which are largely exempt from stringent requirements. Providers of these systems are encouraged to adhere to voluntary codes of conduct and governance mechanisms, promoting self-regulation.[143]

Typically, the risk-based approach is illustrated as a pyramid, with minimal risks at the base and progressively greater risks as you move upward. However, the AI Act can be more aptly compared to an elevator than a pyramid for two key reasons.

First, it is up to the providers themselves to document and determine whether a system does not qualify as high-risk under a self-pre-assessment of the system.[144] By the way, this specific aspect contains potential loopholes regarding the consistency and robustness of compliance, as it places a considerable burden on providers to police themselves potential conflicts of interest.[145] Second, certain obligations designed for lower-risk systems also extend to higher-risk categories. A clear example of this is art. 50's transparency requirement, which applies not only to systems classified as limited risk but also to high-risk systems like those used for emotion recognition.[146]

The most striking illustration of this "elevator mechanism" can be seen in the regulation of General Purpose AI (GenAI) systems. These systems follow a tiered structure. Defined as «an AI system based on a general-purpose AI model, capable of serving multiple purposes, both for direct use and for integration into other AI systems» (art. 3, no. 66), GenAI systems present unique regulatory challenges due to their broad applicability. These models are subject to a risk-based approach, with systems classified as having systemic risks facing stricter regulation compared to those with-

[139] AI Act, arts. 8-27.

[140] AI Act, art. 50.

[141] AI Act, art. 50, para. 4.

[142] AI Act, Recital 132.

[143] AI Act, Recital 165.

[144] AI Act, art. 6, para. 3.

[145] S. 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*, in *Yale Journal of Law and Technology*, 26(3), 2024.

[146] AI Act, art. 50, para. 3.

out systemic risks.[147]

Although GenAI models are integral to these systems, they do not constitute AI systems on their own. The AI Act's provisions apply to GenAI models only when they are integrated into a functioning AI system. The obligations for GenAI model providers kick in once these models are placed on the market and continue even when integrated into an AI system. However, these obligations do not apply when the model is used solely for internal processes that do not affect individual rights or provide products or services to third parties. On the other hand, GenAI models with systemic risks are always subject to the AI Act's obligations due to their potentially significant adverse effects.[148]

In essence, the AI Act treats GenAI systems as AI systems, and when a general-purpose AI model is integrated into an AI system, this integrated system is classified as a GenAI system if it gains the ability to serve a variety of purposes.[149] High-risk AI systems, including high-risk GenAI systems, are subject to extensive obligations under the AI Act, such as conducting a Fundamental Rights Impact Assessment (FRIA).[150] This assessment requires deployers to consider the protection of fundamental rights, thereby compelling both public and private actors to evaluate the potential impact of AI systems on these rights.

Nonetheless, this regulatory architecture poses significant challenges for deployers, who may face difficulties in ensuring comprehensive compliance. The complexity of evaluating AI's impact on diverse fundamental rights, coupled with the flexibility of GenAI systems to serve various functions, can make it hard for actors to anticipate all potential risks and to tailor safeguards accordingly. Moreover, the reliance on self-assessment increases the risk of underreporting or misjudging these impacts, especially when there is limited external oversight to ensure that the FRIA process is thoroughly and objectively conducted.[151] This raises concerns about whether AI systems, particularly those classified as high-risk, will be deployed with adequate safeguards in place to prevent harm to individuals and society.

Moreover, different from the GDPR and the DSA, which strongly focus on the protection of a couple of fundamental rights mainly – privacy and

---

[147] The classification for systemic risk is further expanded in the guidelines of the "Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act)", published by the European Commission, 18 July 2025. This designation carries significant regulatory consequences, including stricter obligations, that must not be mistaken with prohibited or high risk AI systems, under art. 5 and 6 of the AI Act. While these latter ones are about the ***use*** of the ***system,*** the "systemic risk" notion applies, instead, on different criteria: i) the model displays capabilities matching or exceeding those of the most advanced models on the market; ii) the Commission designates the model as systemic risk based on impact criteria set out in Annex XIII of the AI Act.

[148] AI Act, Recital 112.

[149] AI Act, Recital 100.

[150] O. Pollicino-A. Cosentini, *et al.* *Assessing the Impact of Artificial Intelligence Systems on Fundamental Rights*, in *MediaLaws.eu*, 31 March 2025.

[151] S. 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*, cit., 20.

data protection, the former, freedom of expression, the latter –, the AI Act has a completely different scope of application. As it is evident even from the choice of the legal basis,[152] the regulation on AI is a product safety norm that intersects with a wider range of issues.[153] However, when necessary, the AI Act also integrates the protection of other fundamental rights to address specific concerns, such as the inclusion of provisions related to data protection, especially in contexts where the processing of special categories of personal data is concerned, as is the case with biometric surveillance technologies.[154]

The wide range of cases in which AI can trigger fundamental rights is especially evident in the case of the FRIA: this assessment is a rights-based one, meaning that the deployer is asked to consider the risks that an AI system may pose by pondering every right in the CFREU, especially those «in the areas of education, healthcare, social services, housing, administration of justice».[155] The impact assessment, much like the risk classification, suffers from the Act's over-reliance on self-assessment methodologies. Even though the deployer will have to communicate the results of the FRIA to the Market Surveillance Authority,[156] this approach risks becoming self-serving, as deployers may tailor the assessments to minimise perceived risks or liabilities, rather than conducting a thorough and impartial evaluation.[157] The lack of stringent external oversight exacerbates this issue, leaving room for biased or incomplete evaluations that could fail to adequately safeguard fundamental rights.

The AI Act, despite its pioneering ambition, exhibits an over-reliance on previous regulatory instruments, such as the GDPR, especially, and the DSA to some extent. While these frameworks have been effective within their respective domains, they are ill-equipped to address the distinctive challenges posed by the autonomy of AI systems. This over-reliance highlights the EU legislator's inadequate understanding of the unique risks associated with AI autonomy. As a matter of fact, in the AI Act, despite the promises,[158] the human element is minimally considered, largely relegated to the status of a potential "victim" of AI-induced harm,[159] rather than being envisioned as an integral actor in governance and oversight mechanisms.

This results in a regulatory framework where human involvement is reactive, appearing primarily in the context of mitigating risks rather than ensuring active and meaningful oversight of AI systems. Specifically, this

152 The AI Act is primarily grounded in art. 114 TFEU, which focuses on establishing and ensuring the functioning of the internal market.

153 AI Act, Recitals 1 and 9.

154 AI Act, Recitals 3 and 59.

155 AI Act, art. 27, to be read together with art. 1, Recitals 93 and 96. The quote comes from Recital 96.

156 *Ibid.*

157 M. Ebers, *Truly Risk-Based Regulation of Artificial Intelligence - How to Implement the EU's AI Act*, SSRN Scholarly Paper, Rochester, NY, 2024.

158 AI Act's Explanatory Memorandum, *ibid.*

159 AI Act, art. 27, para. 1, lit. b) and c).

aspect is also reflected in the design of the remedies under the AI Act's arts. 85, 86 and 99, para. 10. Art. 85 enables individuals, or groups of individuals, to launch a complaint with a market surveillance authority «having grounds to consider that there has been an infringement of the provisions of this Regulation».[160] Art. 99, para. 10, recalls that access to effective judicial remedies and due process rights should be granted via procedural safeguards.[161] Eventually, art. 86 also conceives a right for the individual to receive a «meaningful explanation of the role of the AI system in the decision-making procedure and the main elements of the decision taken».[162] This newly introduced right to explanation attempts to address ongoing debates in the academic community,[163] particularly those surrounding the ambiguous nature of information rights under the GDPR. While the GDPR grants individuals access to information about the logic of algorithmic decisions under art. 22, the precise nature of these rights has been subject to interpretation. The AI Act now steps into this debate, providing a more explicit but still somewhat ambiguous formulation of the right to explanation. For example, the lack of clarity around how this right will apply in practice, especially concerning the role of AI-driven decisions in the broader decision-making process, remains a challenge. As this text affirms, these limitations underscore the need for clearer guidance on how AI systems should integrate human oversight and provide accountability in decision-making processes.

Hence, the human element is often relegated to mitigating harm only after it has occurred, rather than being proactively engaged in ensuring that AI systems operate within the bounds of fairness and legality from the outset. This reactive approach weakens the potential for robust due process protections, as it limits opportunities for individuals to challenge AI-driven decisions before they lead to detrimental consequences.

Moreover, the AI Act should not only ensure an effective and efficient right to remedies that allows individuals to contest the specific decisions made by an AI system but also extend accountability to the deployers of AI systems. This would involve holding the responsible entity accountable for its decision to implement AI in a particular context. In other words, procedural protections should go beyond merely challenging an AI decision and should encompass scrutiny of whether the decision to use AI in a given situation was appropriate and justified. This dual layer of responsibility – both for the decision and the deployment – would ensure a more comprehensive framework for safeguarding fundamental rights.

Besides, the AI Act fails to adequately account for the specific contexts in which AI technologies are deployed, leading to the potential for misinterpretation by Member States: this misalignment risks over-regulation in certain areas and insufficient attention in others, creating uneven en-

[160] *Ibid.,* art. 85.

[161] Thus, Recital 27 specifies that «Without prejudice to the legally binding requirements of this Regulation and any other applicable Union law, those guidelines contribute to the design of coherent, trustworthy and human-centric AI, in line with the Charter and with the values on which the Union is founded».

[162] *Ibid.*

[163] The referral is also to para. 2.1 of the present paper.

forcement and regulatory fragmentation across the Union.[164] One of the most glaring oversights is the Act's deliberate exclusion of AI in military applications from its regulatory scope.[165] By neglecting to address this crucial domain, the EU has left a significant gap in oversight, allowing the deployment of military AI technologies to proceed without the rigorous safeguards applied to civilian sectors.

The next section will, then, further unpack these critical aspects, trying to figure out what of the current system risk to harness the rule of law using as a litmus test the conceptualisation of the Venice Commission.

6. Testing the Rule of law in Context: Drawing from the Venice Commission

Having set out the general architecture of the AI Act, the crucial step is to test its provisions against the Union's own understanding of the rule of law. As argued in paragraph 2, the rule of law in the EU is not a lofty aspiration but a *functional principle*: a means of ensuring that fundamental rights are guaranteed through legality, foreseeability, accountability and remedies. In this sense, besides the scholarship analysis of the rule of law, a concrete benchmark arrives from the Venice Commission.[166] In this context, the Venice Commission also adopted a Checklist as «a tool for assessing the Rule of Law in a given country from the viewpoint of its constitutional and legal structures, the legislation in force and the existing case-law. […] The checklist is mainly directed at assessing legal safeguards […] The checklist is meant as a tool for a variety of actors who may decide to carry out such an assessment».[167] However, as the Explanatory Note recalls, the Checklist does not seek to redefine the concept, but to «make it justiciable and assessable», by breaking down the rule of law into concrete benchmarks that can be tested across legal systems. The goal is to move from the invocation of the rule of law as a political aspiration to its evaluation as a functional guarantee.

The Commission identified five clusters of requirements that together give content to the rule of law: legality, legal certainty, prevention of abuse of power, equality before the law and non-discrimination, and access to justice before independent courts. These criteria are not random: they correspond to the elements without which the rule of law ceases to operate as a *means* of protecting rights. As the next paragraph will develop, legality ensures that power is exercised through properly enacted law, rather than discretion or administrative practice; legal certainty makes the law

---

164 For instance, Italy adopted the law 132/2025 for the implementation of the AI Act, that includes a modification of the criminal code to include art. 612-quater, "Unlawful dissemination of content generated or manipulated by artificial intelligence systems", which provides for a penalty of one to five years' imprisonment.

165 AI Act, art. 2, para. 3.

166 "Report on the Rule of law", adopted in Venice, March 25-26, 2011 - CDL-AD (2011)003rev., and the "Rule of Law Checklist", adopted in Venice, March 11-12, 2016 - CDL-AD(2016)007.

167 *Ibid.,* paras. 23-28.

foreseeable and knowable, allowing individuals to orient their conduct; prevention of abuse of power guards against arbitrariness by requiring that discretion be constrained and accountable. Finally, equality secures fairness and prevents exclusionary or discriminatory outcomes, and access to justice guarantees that individuals have remedies before independent courts, without which all other principles remain aspirational.

The impact of the Checklist is not just limited to the CoE domain, since it has become a reference in European constitutional discourse because it translates a principle of high abstraction into criteria that can be applied to concrete cases.[168] Thus, it fits the approach of this paper: treating the rule of law not as a symbolic goal, but as a practical yardstick to test whether regulatory frameworks, such as the AI Act, actually secure remedies.[169] As mentioned *supra,* the Venice Commission Checklist is also referenced by the 2025 Rule of Law Report methodology, which illustrates how these benchmarks are now entrenched in Union practice.[170] Each of the five dimensions, legality, certainty, abuse of power, equality, and access to justice, is compatible with the concrete indicators for Member State assessment used by the European Commission. This convergence between the Venice Commission and the Commission's own reporting architecture underscores the appropriateness of using the same framework to evaluate the AI Act. Just as the Report measures whether Member States provide the institutional conditions for the rule of law to function, the question here is whether the regulatory instrument for Artificial Intelligence, the AI Act, embeds the operational guarantees that make remedies effective in the algorithmic domain.

For all of these reasons, the analysis that follows applies these five dimensions to the AI Act in order to find potential answers to whether, element by element, the Regulation meets the functional standard as inspired by the Venice Commission's understanding of the rule of law, or whether it remains confined to formal legality without delivering the substantive guarantees of the rule of law.

---

168 *Council conclusions on fundamental rights and rule of law and on the Commission 2012 Report on the Application of the Charter of Fundamental Rights of the European Union,* Justice and Home Affairs Council Meeting, Luxembourg, 6-7 June 2013, part c, available at *consilium.europa.eu*: Moreover, in the "Resolution of the Italian Parliamentary Assembly", no. 2187/2017, it is specified that the Venice Commissione «invite international and regional organisations, including the Council of Europe as a whole and the European Union, to refer regularly to the Rule of Law Checklist in their relevant work. In this connection, the Assembly congratulates the Secretary General of the Council of Europe on having taken the Rule of Law Checklist into account in his 2017 annual report on the situation of democracy, human rights and the rule of law in Europe, and urges him to do so systematically in all his future annual reports», §6.4.

169 On the relationship between the EU and the CoE on the regulation of AI, see F. P. Levantino-F. Paolucci, *Chapter 1 Advancing the Protection of Fundamental Rights through AI Regulation,* cit., 19.

170 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "2025 Rule of Law Report. The rule of law situation in the European Union", Strasbourg, 8.7.2025 COM(2025) 900 final; European Commission, "Methodology for the preparation of the Annual Rule of Law Report", 2025.

6.1. Legality

The first benchmark of the Checklist is legality, understood as the requirement that all public power must be exercised on the basis of clear, accessible and foreseeable law, properly enacted by parliament and subject to review. Applied to the AI Act, legality raises two questions: the adequacy of the Act's own legal basis at the Union level,[171] and the sufficiency of legal bases for the deployment of AI in Member States.[172]

At the Union level, the AI Act rests exclusively on art. 114 TFEU, the internal market harmonisation clause. Formally, this satisfies legality: the EU acted within a recognised competence, the Act was adopted by the ordinary legislative procedure, and it takes the form of a binding regulation. Yet the reliance on art. 114 is constitutionally ambivalent.[173] Framing the AI Act as an internal market instrument places its legitimacy on the logic of product safety and market integration, not on the direct protection of fundamental rights. This contrasts with other potential legal bases, such as art. 16 TFEU on data protection or art. 19 TFEU on non-discrimination, which were not chosen as primary ones.[174] The result is that the Act's rights-protective provisions are juridically tethered to a market rationale. This may result in a "rule by law" loophole: the use of legal form to mask the absence of substantive protection. There is a danger that the AI Act's legality is of this kind, formally valid, but substantively limited.[175]

These limitations are indeed visible also at the national level. The AI Act imposes obligations on providers and deployers but does not require that Member States anchor the use of AI in sensitive sectors in primary legislation.[176] Welfare authorities can deploy fraud-detection algorithms, border agencies can rely on biometric recognition,[177] among others, and courts may experiment with AI,[178] often on the basis of administrative orders or ministerial decrees rather than statutes. From the perspective of the rule

[171] As noted also elsewhere, the use of art. 114 TFEU has been considered by scholarship a "catch them all" solution. See O. Pollicino-F. Paolucci, *Digital Constitutionalism*, in L. Floridi-M. Taddeo (eds.), *A Companion to Digital Ethics*, Hoboken, 2025, 313 ff.

[172] See also O. Pollicino-G. Muto, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, in *Rivista di Diritto dei Media*, 1, 2025, 393 ff.

[173] E. Longo, *Grounding media freedom in the EU: the legal basis of the EMFA*, in *Rivista Italiana Di Informatica e Diritto (RIID): Periodico Internazionale Del CNR-IGSG*, 1, 2025, 2 ff.

[174] See the Explanatory Memorandum to the Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, {Sec(2021) 167 Final} - {Swd(2021) 84 Final} - {Swd(2021) 85 Final}, in part. §2, on the legal basis.

[175] On the difficult interplay between data protection and GenAI see M. Bassini, *DeepSeek, or OpenAI Reloaded? An 'Italian-Style Approach' in Tackling Data Protection in Generative AI*, in *AIRe*, 2(1), 2025, 88 ff.

[176] B. Paola *et al.*, *Le assemblee rappresentative nell'era dell'intelligenza artificiale. Profili costituzionali*, in *Le assemblee rappresentative nell'era dell'intelligenza artificiale. Profili costituzionali*, Milan, 2025, 1 ff.

[177] N. Vavoula, *Regulating AI at Europe's Borders*, in *Verfassungsblog*, 13 December 2024.

[178] See Annex III, AI Act. V. Hendrickx, *Rethinking the judicial duty to state reasons in the age of automation?*, in *Cambridge Forum on AI: Law and Governance*, 1, 2025, 26 ff.

of law, as also conceived by the Venice Commission, this is insufficient: legality demands that such exercises of power have a clear legislative basis, accessible to the public, defining scope, purposes, and safeguards. In its absence, legality risks becoming a purely technical compliance with regulatory checklists, rather than law in the substantive sense.
The Act also strains legality by heavily relying on delegated acts and private standardisation. Art. 97 empowers the Commission to amend Annex III, which lists high-risk AI use cases, through delegated acts.[179] This means that the scope of the Act's strictest obligations can be expanded or narrowed without new legislation. While subject to *ex post* control by Parliament and Council, this delegation nonetheless places significant discretion in the executive. Similarly, the Act relies on harmonised technical standards developed by private standardisation bodies (CEN/CENELEC, ETSI).[180] Providers who comply with these standards are presumed to meet legal requirements. In practice, therefore, the content of obligations such as "appropriate accuracy" or "adequate bias testing" may be determined by technical committees dominated by industry actors. On this view, the AI Act satisfies legality in form but risks undermining it in substance.

6.2. Legal Certainty

With respect to the second benchmark, legal certainty, which demands that laws be clear, foreseeable and stable, enabling individuals to understand and predict legal consequences, in the AI context, this benchmark maps onto issues of scope, transparency, and intelligibility.
The AI Act makes an effort to clarify its scope through a tiered risk model, as mentioned *supra*: prohibited AI practices, high-risk AI, limited-risk AI, and minimal-risk AI. Annex III provides a detailed list of high-risk uses, including biometric identification, recruitment, credit scoring, and access to essential services. This categorisation promotes certainty at the macro level, harmonising what counts as risky across the Union. Yet several uncertainties remain.[181] The very definition of "AI system" in art. 3 is broad, encompassing statistical approaches, machine learning, and knowledge-based methods. This breadth is intended to be future-proof,[182] but risks leaving developers unsure whether their systems fall within the Act. More seriously, the scope of "high-risk AI" is not fixed: the Commission can amend Annex III by delegated acts. As a result, providers may face regulatory uncertainty, unsure whether their systems could later be

[179] See also art. 7, AI Act.

[180] M. Cantero Gamito-C. T. Marsden, *Artificial intelligence co-regulation? The role of standards in the EU AI Act*, in *International Journal of Law and Information Technology*, 32(1), 2024, 11 ff.

[181] P. Dunn-G. De Gregorio, *The Ambiguous Risk-Based Approach of the Artificial Intelligence Act: Links and Discrepancies with Other Union Strategies*, CEUR Workshop Proceedings, 2022.

[182] European Commission, "Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)", Brussels, 29.7.2025, C(2025) 5053 final.

reclassified as high-risk.[183] What appears as legal certainty at the level of categories thus masks a dynamic scope that may destabilise predictability. Beyond scope, transparency and explanation are essential to legal certainty. Art. 13 requires providers of high-risk AI to design systems so that users can interpret outputs. Art. 52 mandates informing individuals when they interact with AI. Most significantly, art. 86 establishes a right to explanation for individuals significantly affected by high-risk AI decisions. On paper, this aims to foster certainty: individuals can foresee and understand how decisions are made. But in practice, the provision is limited.[184] It applies only to high-risk AI, only subsidiarily where no other law already grants such a right, and excludes certain domains such as law enforcement biometrics.[185] Moreover, explanations risk being formalistic rather than intelligible. Machine learning systems, especially deep learning models, produce outputs through complex, opaque processes that «rarely correspond to humanly comprehensible reasoning steps».[186] The *Schufa* decision under the GDPR illustrates the problem: while individuals were informed of their credit scores, they could not understand how those scores were calculated, undermining their ability to contest them.[187] The AI Act risks reproducing this dynamic, granting explanations in name but not in substance.[188]

Even more striking is the Commission's pervasive reliance on guidelines. While the AI Act entered into application on 2 August 2024, the European Commission has already published guidelines for the interpretation of the AI systems definition under art. 3, on art. 5 on prohibited practices, on the obligations for general-purpose AI models and systemic risk,[189] and guidelines on high-risk obligations are currently under elaboration.[190] These

[183] For the interplay between high risk and prohibited risk, see European Commission, "Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), Brussels, 29.7.2025 C(2025) 5052 final. See, also, A. Calvi *et al.*, *Contribution to "targeted stakeholder consultation on classification of AI systems as high-risk"*, D.pia.lab, 1 July 2025.

[184] S. Demkova, *The EU's Artificial Intelligence Laboratory and Fundamental Rights*, in M. Fink (ed.), *Redressing fundamental rights violations by the EU,* Cambridge UK, 2025.

[185] Allow to recall F. Paolucci, *Constitutional Safeguards in the Age of AI. A Study on the Fundamental Rights Impact Assessment of Facial Recognition Technology*, Milan, 2025.

[186] M. Garnelo-M. Shanahan, *Reconciling deep learning with symbolic artificial intelligence: representing objects and relations*, in *Current Opinion in Behavioral Sciences*, 29, 2019, 17 ff.

[187] ECJ, C-634/21, cit.

[188] F. Doshi-Velez *et al.*, *Accountability of AI Under the Law: The Role of Explanation*, cit.; E. Falletti, *Credit scoring under scrutiny by the Court of justice of the European union: brief remarks on the «SCHUFA Decision»*, in *SSRN*, 14 February 2024, 1 ff.

[189] European Commission, "Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)", Brussels, 29.7.2025, C(2025) 5053 final; European Commission, "Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), Brussels, 29.7.2025 C(2025) 5052 final; European Commission, "Approval of the content of the draft Communication from the Commission – Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act)", Brussels, 18.7.2025 C(2025) 5045 final.

[190] Such guidelines were proceeded by a consultation period, as in A. Calvi *et al.*,

documents, though formally non-binding, become *de facto* authoritative: national regulators and courts will look to them for guidance, and providers who deviate from them risk being found non-compliant. This proliferation of soft law generates a form of "moving target" legality: the rules of the game evolve through guidance notes produced by the Commission or the AI Office, outside of the "regular" legislative process.

In this sense, the basics of legal certainty are challenged, since this principle relies on stability and coherence across the legal system. Here, the AI Act introduces potential friction with existing laws, notably the GDPR. For instance, art. 10(5) AI Act allows the processing of special categories of personal data if necessary to detect and correct bias in high-risk AI systems. Yet under the GDPR, processing data under art. 9 requires strict conditions and safeguards.[191] This tension creates uncertainty for providers: until clarified by guidance or jurisprudence, actors cannot confidently predict how to comply with both regimes.

In sum, the AI Act promotes certainty at a formal level through harmonisation, but its reliance on broad definitions, delegated amendments, opaque technology, and overlaps with other frameworks means that predictability is often illusory. The law appears clear, but may not be intelligible or foreseeable to those most affected. According to the rule of law's standards, legal certainty may be formally satisfied in form but not yet in substance.

6.3. Prevention of Abuse of Power

As highlighted in para. 2 of this paper, one of the main purposes of the rule of law is to ensure that (State)[192] power is contained and subject to review, and governance structures designed to avoid arbitrariness. In the AI Act, this benchmark engages both the design of oversight in AI deployments and the concretisation of the enforcement of such rules at the Union level.[193]

Looking at the provisions of the Regulation, art. 14 requires that high-risk AI systems be designed to allow for effective human oversight. This obligation acknowledges the constitutional intuition that legality requires hu-

Contribution to "targeted stakeholder consultation on classification of AI systems as high-risk", cit., 26.

[191] L. Georgieva-C. Kuner, *Article 9 Processing of special categories of personal data*, in C. Kuner *et al.* (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, 2020.

[192] Nonetheless, the Venice Commission highlights that «the rule of law thus addresses the exercise of power and the relationship between the individual and the state. However, it is important to recognise that during recent years due to globalisation and deregulation there are international and transnational public actors as well as hybrid and private actors with great power over state authorities as well as private citizens», in "Venice Commission Report on the Rule of Law", 2011, cit., §16.

[193] A. M. Corrêa *et al.*, *Better together? Human oversight as means to achieve fairness in the European AI Act governance*, in *Cambridge Forum on AI: Law and Governance*, 1, 2025, 29 ff.

man accountability. Yet its content is underspecified.[194] The Act does not define what "effective" oversight entails, nor does it allocate responsibility clearly.[195] In practice, oversight can become ritualistic: a human operator formally "in the loop" but without the information or authority to meaningfully intervene, also by means of lacking the appropriate training.[196] Literature on algorithmic governance has highlighted this risk, describing human oversight as a liability shield rather than a genuine safeguard.[197] From the rule of law perspective, such nominal oversight fails to prevent abuse. To be substantive, «the effectiveness of oversight mechanisms can only be properly assessed and improved when specific goals are clearly articulated in advance»[198] and concretely reviewable.

Even more problematic is the Act's reliance on codes of practice, particularly for general-purpose AI models.[199] The AI Office is tasked with «the drawing up of codes of practice at Union level in order to contribute to the proper application of this Regulation, taking into account international approaches»,[200] inviting also the providers of such models «to participate in the drawing-up of codes of practice».[201] While co-regulation can bring technical expertise, it also risks regulatory capture.[202] Those subject to the

[194] The critics in A. Calvi *et al.*, *Contribution to "targeted stakeholder consultation on classification of AI systems as high-risk"*, cit., 26.

[195] In particular, Recital 73 states that «appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role. […] Considering the significant consequences for persons in the case of an incorrect match by certain biometric identification systems, it is appropriate to provide for an enhanced human oversight requirement for those systems so that no action or decision may be taken by the deployer on the basis of the identification resulting from the system unless this has been separately verified and confirmed by at least two natural persons». It is likely that, as happened also for other obligations, this will be clarified further by a guideline of the European Commission. As explained above, this ritual might spark clarity, in some cases, but also lack of legal certainty, since guidelines, per their name, are not enforceable.

[196] For a taxonomy critique to the rule of law see J. Laux, *Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of AI governance under the European Union AI Act*, in *AI & Society*, 39(6), 2024, 2853 ff..

[197] M. Fink, *Human Oversight under Article 14 of the EU AI Act*, SSRN Scholarly Paper, Social Science Research Network, Rochester, NY, 2025.

[198] *Ibid.*

[199] The Code of Practice is comprised of three chapters on transparency, copyright and safety and security, and complements the guidelines of the European Commission on the obligations for providers of GPAI models. See European Commission, "Approval of the content of the draft Communication from the Commission – Guidelines on the scope of the obligations for general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act)", Brussels, 18.7.2025 C(2025) 5045 final.

[200] See AI Act, art. 56, para. 1.

[201] *Ibid.*, para. 2.

[202] As noted elsewhere, «today we are witnessing a kind of "code reloaded", in light of the metamorphosis referred to above, whereby digital intermediaries have transformed from economic operators into full-blown private powers, in competition with public

law participate in shaping its substantive requirements, diluting public accountability. The EU's approach to using codes of conduct as a tool for co-regulation, particularly in the digital domain, reflects an effort to bridge gaps in regulatory frameworks where binding legislation may not yet exist or where enforcement proves challenging. This strategy is especially evident in the '2018 Code of Conduct' aimed at combating disinformation, which initially relied on self-regulation. However, while the initial version was criticised for vague obligations and the lack of measurable indicators to assess platform accountability in content moderation efforts, the revised Code introduced in 2022 incorporated more structured guidelines. This shift represents a movement towards co-regulation, where private entities are encouraged to adhere to certain standards while engaging in dialogue with the European Commission. In this sense, the Digital Services Act (DSA) further institutionalises this approach by recognising codes of conduct as essential tools for co-regulation, with the potential for enforcement consequences if platforms fail to comply with these voluntary commitments. Hence, these experiences demonstrate how codes evolve into hybrid norms, less than law, but more than mere self-regulation, creating a grey zone where accountability is diffuse and democratic oversight is thin. These risks are amplified in the AI context. General-purpose AI providers are not passive intermediaries; they are sophisticated actors capable of shaping information environments and altering the parameters of decision-making across multiple domains. They are, as disinformation research shows, «much less neutral, much less passive and yet much more capable»[203] of influencing content and behaviour, even if they do not resemble traditional publishers.[204] Allowing such actors to help define the scope and detail of their obligations under the AI Act blurs the line between regulator and regulated. Particularly, it places constitutional safeguards in the hands of those whose interests may be directly adverse to rights protection.

In this sense, the rule of law requires that powers be exercised under controls external to those being regulated. Codes of practice that invite industry to co-write compliance duties verge on self-regulation, a model that is constitutionally suspect in a field with profound implications for fundamental rights. The AI Act's institutional design compounds these concerns. Alongside codes, it creates a European AI Office within the Commission and a European AI Board composed of national authori-

authorities. Indeed, these operators are distant relatives of the operators that were (not) regulated under European law during the era of digital liberalism». O. Pollicino, *The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism*, in *European Law Journal*, 29, 1–2, 2023.

203 O. Pollicino, *The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism*, *ibid.*

204 As noted by Bassini, «extending constitutional coverage to generative AI content does not prevent state authorities from prohibiting certain types of speech that harm other legal interests (such as individuals' privacy or reputation), but such restrictions would not differ from any other limits on free speech that are constitutionally permissible in the offline world (and also online, via other media)». See M. Bassini, *Speech without a Speaker: Constitutional Coverage for Generative AI Output?*, in *European Constitutional Law Review*, 2025, 1 ff.

ties, both under Commission supervision.[205] While such centralisation may bring coordination, it also concentrates power in the executive. Without strong safeguards, the risk is that a framework intended to prevent abuse of AI power will instead entrench new concentrations of institutional and private power with inadequate checks.

6.4. Equality and Non-Discrimination

The fourth benchmark is equality before the law and non-discrimination. AI systems pose acute risks in this domain, and it is, maybe, the most visible of the five rule of law targets: training data may encode structural biases, machine learning models may replicate them, and outputs may disproportionately burden vulnerable groups.[206]
The AI Act acknowledges these risks by embedding non-discrimination and fairness into its high-risk obligations. Art. 10 requires that training data be relevant, representative, and as free from error and bias as possible: in particular, providers must implement measures to detect and correct biases.[207] Art. 27 introduces the Fundamental Rights Impact Assessment (FRIA),[208] obliging deployers of certain high-risk AI (notably in public services, credit and insurance) to evaluate impacts across the Charter, including equality and non-discrimination. This is an unprecedented innovation: for the first time, the EU requires *ex ante* assessment of all Charter rights in connection with a technology.
Thus, the FRIA is mandatory for deployers of some high-risk AI systems.[209] This obligation extends to deployers governed by public law, private operators providing public services, and operators deploying high-risk systems for the purpose of credit scoring, creditworthiness or risk assessment and pricing of life and health insurance of natural persons.[210] By mandating FRIAs for these actors, the AI Act emphasises the importance of anticipating and mitigating risks to fundamental rights before deploying high-risk AI systems. More specifically, the FRIA must be performed prior to the initial deployment of the high-risk AI system and should be continued during the whole AI life cycle.[211] This entails a thorough evaluation of the

205 C. Novelli *et al.*, *A Robust Governance for the Ai Act: Ai Office, Ai Board, Scientific Panel, and National Authorities*, in *European Journal of Risk Regulation*, f4, 2024, 1 ff.; F. Paolucci, *The enforcement of the Artificial Intelligence Act: Looking Forward to a Commission Implementing Decisions for Protecting Fundamental Rights*, in O. Pollicino *et al.* (eds.), *La disciplina dell'intelligenza artificiale*, Milan, 2025.

206 R. Xenidis, *Beyond bias: algorithmic machines, discrimination law and the analogy trap*, in *Transnational Legal Theory*, 14(4), 2023, 378 ff.

207 As mentioned above, also using special categories of personal data, as per art. 10, para. 5, AI Act.

208 A. Cosentini *et al.*, *Assessing the Impact of Artificial Intelligence Systems on Fundamental Rights*, cit.

209 AI Act, art. 43, Recital 96.

210 AI Act, Annex III, art. 5, lit. b) and c).

211 AI Act, Recital 96, «Whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers

system's potential to adversely affect fundamental rights. For this reason, deployers may rely on previously conducted assessments, including those provided by the system's developer, provided the system's context of use remains unchanged.[212] However, should any significant modifications arise during the system's use, such as changes in its purpose, affected populations, or identified risks, the deployer is obligated to update the assessment to reflect the new circumstances.[213] The AI Act provides limited details on how the FRIA should be conducted, specifying the inclusion of usage descriptions, affected groups of people, and the identification of more vulnerable individuals, as well as potential risks and risk mitigation steps.[214]
The assessment must comprehensively address the following aspects:
System use and purpose: a detailed description of how the AI system will be integrated into the deployer's processes, ensuring alignment with its intended purpose.
Operational parameters: an outline of the timeframe and frequency of the system's deployment.
Affected individuals and groups: an identification of the categories of natural persons and communities likely to be impacted by the system, particularly marginalised or vulnerable groups.
Risk analysis: a detailed evaluation of specific risks of harm that may arise from the system's use, with reference to information provided by the developer in compliance with art. 13 of the AI Act.
Oversight and governance: a description of the human oversight measures that will be implemented, following the developer's guidelines.
Mitigation measures: strategies to address the materialisation of identified risks, including internal governance mechanisms and accessible complaint procedures.
The assessment should then be reported to the market surveillance authority.[215] A standardised template from the AI Office is under elaboration to ensure consistent evaluations.[216] From the listed essential requirements, a potential information asymmetry emerges between deployers and providers. Much of the information, such as operational parameters and instructions for use, must be shared by providers to conduct a proper assessment. It is, therefore, needed that the provider and the deployer cooperate, and it is crucial to point out the possible occurrence of contractual inequality between the two actors.[217] The success of these assessments also relies on

of high-risk AI system therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system. Deployers are best placed to understand how the high-risk AI system will be used concretely and can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use, the persons or groups of persons likely to be affected, including vulnerable groups».

212 AI Act, art. 27, para. 2.

213 *Ibid.*

214 AI Act, art. 27, para. 1, lett. a-f).

215 AI Act, art. 27, para. 3.

216 AI Act, art. 27, para. 5.

217 P.G. Chiara-F. Galli, *Normative Considerations on Impact Assessments in EU Digital Policy*, in *Rivista di Diritto dei Media*, 1, 2024.

the transparency and reliability of exchanged information, with providers supplying accurate and comprehensive data.[218]

Yet the substance is weaker than the form. The FRIA is a self-assessment, and not even subject to penalties:[219] deployers carry it out themselves, with no requirement for independent verification prior to deployment. Results must be communicated to market surveillance authorities, but only after the fact.[220] The risk is that the FRIA becomes defensive paperwork, aimed at minimising liability rather than surfacing risks: without external audit or public scrutiny, the safeguard risks formalism.

Moreover, fairness metrics are inherently contested. Scholars note that different definitions of fairness (equal accuracy across groups, proportionality, lack of disparate impact) can yield divergent outcomes.[221] Providers may choose the metric most convenient to them. The Act does not specify which definitions to use, leaving discretion to private actors and standards bodies.[222] In practice, a system could be certified as compliant despite generating significant disparities in outcomes. Equality, as also happens for other "key" words like transparency and fairness, is thereby proclaimed but not enforced. In particular, while the Regulation does prohibit certain AI uses that offend equality outright – e.g. social scoring by public authorities is banned – yet such prohibitions are limited in scope and do not address subtler systemic inequalities.[223]

From the rule-of-law perspective, therefore, the AI Act's equality provisions risk the same gap as legality and certainty: they satisfy the form of protection without ensuring its substance. The FRIA, in particular, risks devolving into a formalistic exercise unless coupled with independent oversight.

---

218 *Ibid.*

219 Notably, the AI Act does not establish a specific penalty regime for violations of art. 27, which requires providers of high-risk AI systems to carry out a FRIA. Under art. 99 AI Act, penalties are defined for breaches of data quality, risk management, or prohibited AI practices, but no express sanction is foreseen for non-compliance with art. 27 obligations. This omission is a potential weakness of the enforcement framework, since the effectiveness of the FRIA depends on the existence of credible deterrents, otherwise is just a void obligation, besides the submission of a report to the AI Office, according to art. 27, para. 3.

220 P. Chiara-F. Galli, *Normative Considerations on Impact Assessments in EU Digital Policy*, *ibid.*

221 S. Greenstein, *Preserving the rule of law in the era of artificial intelligence (AI)*, in *Artificial Intelligence and Law*, 3- 3, 2022, 291 ff.

222 A. Kouroutakis, *Rule of law in the AI era: addressing accountability, and the digital divide*, in *Discover Artificial Intelligence*, 4(1), 2024, 115 ff.; M. Rotenberg, *Human Rights Alignment: The Challenge Ahead for AI Lawmakers*, in H. Werthner *et al.* (eds.), *Introduction to Digital Humanism: A Textboo,* Cham, 2024, 611 ff.; R. Tarchi-A. Gatti, *Intelligenza artificiale e protezione dei dati personali: problemi di metodo e di procedura*, in *DPCE Online*, 64(2), 2024.

223 In this sense, the consultation of affected groups is vaguely scatched in the AI Act, as argued in O. Pollicino *et al.*, *AI e sostenibilità Verso una compliance integrata. La valutazione di impatto sui diritti umani tra AI Act e direttiva CSDD*, Milan, 2025.

6.5. Access to Justice

The final benchmark is access to justice, understood as the availability of effective remedies before independent courts. This is the linchpin of the rule of law: without remedies, the other guarantees remain aspirational.[224] The AI Act incorporates remedies in three key provisions:[225] art. 85 grants individuals the right to complain to market surveillance authorities if they suspect an infringement; art. 86 establishes a right to explanation when high-risk AI systems significantly affect an individual; finally, art. 99 para. 10 provides, as a closing provision, that penalties must be subject to judicial remedies and due process. These provisions, taken together, mark an effort to ensure that AI governance is tethered to rights of redress. On paper, they demonstrate that the Union recognises remedies as essential. However, if analysed more thoroughly, their substantive adequacy is dubious.[226] First of all, complaints under art. 85 are not judicial remedies. They are administrative petitions that may trigger regulatory investigations, but the authority has broad discretion whether to act. Even if the complaint is upheld, the individual complainant does not automatically receive redress or reversal of the AI-driven decision that harmed them. Moreover, art. 86, the right to explanation, is the most heralded innovation. It responds to longstanding debates over GDPR art. 22 and the ambiguity surrounding a "right to explanation" of automated decisions.[227] The AI Act makes this explicit: individuals significantly affected by high-risk AI outputs are entitled to «clear and meaningful explanations of the role of the AI system in the decision-making procedure and of the main elements of the decision taken».[228] This, in principle, aligns with rule-of-law demands: decisions must be reasoned to be contestable. But in practice, the provision is narrow in scope and potentially hollow. It applies only to high-risk AI, and only where no equivalent right already exists. Most significantly, «clear and meaningful» is left undefined. In the context of deep learning models, where outputs result from opaque statistical correlations, the risk is that explanations reduce to formal statements ("the AI was used; you did not meet the threshold") rather than substantive reasons. Such statements do not equip individuals to contest outcomes. This explanation does not suf-

224 M. Cartabia, *The Rule of Law and The Role of Courts*, in *Italian Journal of Public Law*, 10(1), 2018.

225 See also Recital 170, « Union and national law already provide effective remedies to natural and legal persons whose rights and freedoms are adversely affected by the use of AI systems. Without prejudice to those remedies, any natural or legal person that has grounds to consider that there has been an infringement of this Regulation should be entitled to lodge a complaint to the relevant market surveillance authority».

226 M. Eliantonio, *Composite Procedures, the Violation of Fundamental Rights, and the Availability of Sufficient Remedies in the Multi-level EU Judicial Architecture*, in M. Fink (ed.), *Redressing Fundamental Rights Violations by the EU: The Promise of the 'Complete System of Remedies'*, Cambridge UK, 2024, 345 ff.; P. de Hert, *Eu Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the Gdpr in the Spirit of Cooperative Federalism*, in *EU Law Enforcement*, Oxon, 2021.

227 S. Demková, *The EU's Artificial Intelligence Laboratory and Fundamental Rights, ibid.*, p 26.

228 AI Act, art. 86.

fice with the access to justice requirement, which considers not only the mere existence of remedies, but also that they are capable of enabling judicial review. The right to explanation, as discussed, is narrow in scope and potentially unintelligible in practice: while providers must log and document systems, there is no obligation to disclose logs, datasets, or model versions to affected individuals or courts.[229] Moreover, providers routinely invoke trade secrets to shield such information[230].

This problem is not theoretical. In recent cases, it was highlighted by the ECJ how it is complicated for individuals to understand or challenge their credit scores because the algorithmic logic was opaque.[231] Finally, art. 99, para. 10, deals with remedies in enforcement, guaranteeing that providers fined under the Act enjoy due process. This is important for ensuring fairness in sanctions, but it protects the regulated entities, not the individuals whose rights are at stake.

Scholars converge on this point. Namely, Nemitz insists that AI must be used according to the law, or not at all.[232] For them, if AI systems cannot be rendered transparent enough to permit review, they should not be deployed. Keller and Drake argue that algorithmic accountability requires proactive contestation: i.e., remedies must be built into design through visibility, explainability, and contestability. The AI Act nods to these principles but does not embed them robustly. The right to explanation is vague; disclosure obligations are absent; contestability remains more aspirational than real. Measured against the Checklist, therefore, the AI Act satisfies access to justice only in form, since, as explained, remedies are proclaimed but deprived of the material conditions that make them real. This deficiency reverberates across the other benchmarks: legality is undermined if courts cannot verify that AI use rests on a statutory basis; legal certainty collapses if explanations are opaque; prevention of abuse of power is hollow if oversight reduces to rubber-stamping, and courts cannot penetrate trade secret shields; equality is aspirational if discriminatory impacts cannot be proven in litigation. The conclusion we can draw from this comparison is that the current form of the AI regulation under the EU's domain sets some principles in form, but without remedy-capable safeguards, it risks hollowing out the rule of law into *rule by law*.

Taken together, the element-by-element analysis reveals a consistent pattern. On each benchmark of the Venice Commission's Checklist, the AI Act offers formal compliance but leaves substantive guarantees fragile: legality anchored in a market basis, certainty displaced into shifting guidance, oversight reduced to ritual, equality left to self-assessment, and remedies proclaimed but deprived of evidence. What emerges is constitutionalisation in form rather than in substance. If the rule of law is to remain

229 S. Demková, *The EU's Artificial Intelligence Laboratory and Fundamental Rights*, cit., 26.

230 G. Malgieri-G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 7(4), 2017, 243 ff.

231 ECJ, C-203/22, *CK v Dun & Bradstreet Austria GmbH and Magistrat der Stadt Wien,* 27 February 2025.

232 P. Nemitz, *Constitutional democracy and technology in the age of artificial intelligence*, in *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376, 2018, 2018 ff.

a means of rights protection in the digital age, the framework must be refitted to deliver remedies and external controls at the points where AI displaces them. The final section, therefore, turns from diagnosis to prescription, outlining the reforms *de iure condendo* that could align the Act with the Union's constitutional promise.

7. De Iure Condendo

This paper has argued throughout that the rule of law in the European Union is not a decorative value but a structural principle whose function is instrumental: it is the means by which rights are guaranteed, arbitrariness is constrained, and power is rendered accountable. As Bin has aptly put it, «the rule of law requires that laws, not men, govern us; the separation of powers and the principle of legality must guarantee this».[233] When the Union undertakes the constitutionalisation of new technologies, as it has done through the AI Act, the decisive question is not whether rules exist on paper, but whether they are capable of delivering rights protection in practice.

The analysis has shown that when measured against the five benchmarks of the Venice Commission's Rule of Law Checklist, legality, legal certainty, prevention of abuse of power, equality and non-discrimination, and access to justice, the AI Act succeeds in form but fails in substance. Legality is primarily anchored in art. 114 TFEU but detached from rights-oriented Treaty bases. Legal certainty is proclaimed through harmonised categories but undermined by opacity and a proliferation of Commission guidelines. Oversight mechanisms exist but are vague and risk becoming symbolic, while discretion shifts to delegated acts and codes of practice that blur the line between regulator and regulated. Equality is recognised through the FRIA and prohibitions on certain practices, but left to self-assessment without independent verification. Access to justice is formally acknowledged but hollowed out by the absence of intelligible explanations and enforceable disclosure of evidence.

The core finding is that the AI Act constitutionalises AI only in form. It risks hollowing out the rule of law into rule by law: a framework of formal obligations that masks the absence of substantive guarantees. This is not an abstract concern, since automated systems are already determining who receives welfare, who gains access to credit, and who is flagged in policing or migration control. If the safeguards that govern these systems are only nominal, the rule of law itself is trivialised.

Yet this diagnosis also points to the path forward. If the rule of law is to function as a means of rights protection in the age of AI, the framework must be reoriented towards what can be called remedy-capable governance. The Venice Commission's Checklist is particularly useful here because it translates the rule of law into operational benchmarks. By considering them on a policy and future outlook, we can formulate concrete proposals to strengthen the EU's AI governance.

[233] R. Bin, *Lo Stato di diritto*, cit.

On legality, the Union should move beyond the reliance on art. 114 TFEU as the legal basis, and, to some extent, on art. 16 TFEU, data protection. While harmonisation of the internal market is a legitimate aim, the regulation of technologies that shape fundamental rights should also be anchored in rights-oriented Treaty provisions, such as art. 19 TFEU on non-discrimination. Doing so would clarify that fundamental rights protection is not an ancillary effect of market harmonisation but a core objective of the legislation. At the national level, the Union should require that Member States adopt primary legislation to authorise the deployment of AI in sensitive sectors such as welfare, policing, migration and justice.
On legal certainty, the most urgent reform concerns the reliance on Commission guidelines. The proliferation of soft-law documents, while useful for flexibility, undermines foreseeability. If the meaning of "AI system," the scope of prohibited practices, or the definition of "meaningful explanation" depends on guidelines that can be updated unilaterally by the Commission or the AI Office, then the law ceases to be stable and predictable. *De iure condendo*, the Union should confine guidelines to clarifications of technical detail, while ensuring that significant interpretative questions are settled in binding legal acts adopted through accountable procedures. In addition, the scope of art. 86 should be broadened beyond Annex III high-risk systems to encompass all algorithmic decisions with significant effects, thereby ensuring that the right to reasons is not contingent on a regulatory classification. In this sense, legal certainty requires not only clarity of categories but intelligibility of decisions, and this can be achieved only by extending and strengthening explanation rights.
On the prevention of abuse of power, reforms should constrain executive discretion and reduce the risks of regulatory capture. The power to amend Annex III through delegated acts should be narrowly circumscribed, with a preference for legislative revision of the high-risk list where possible. Codes of practice, particularly for general-purpose AI, should not be left to providers to co-draft with minimal oversight. Instead, they should be subject to approval and monitoring by independent authorities, with robust participation by civil society and fundamental rights bodies. As a matter of fact, co-regulation must not become self-regulation; the line must be drawn clearly, with constitutional safeguards external to those being regulated. At the same time, art. 14 on human oversight must be clarified: "effective oversight" should be defined as oversight by officials with legal authority to intervene, whose role is documented and reviewable. Only then can oversight be more than ritual.
On equality, the FRIA is a promising tool but needs reinforcement. *De iure condendo*, the FRIA should be subject to independent verification before deployment, at least in the most sensitive sectors. Self-assessment is inadequate where fundamental rights are at stake. Moreover, the law should establish clear and non-negotiable fairness metrics, developed transparently with input from equality bodies and rights experts, rather than leaving providers to select the most convenient definition. Regular external audits should be mandated to ensure that discriminatory impacts are identified and corrected. In addition, the AI Act should be aligned more closely with equality law: where disparate impacts are shown, the burden of proof

should shift to the deployer to demonstrate that the system is justified and proportionate. Without these reforms, equality will remain aspirational.

On access to justice, the reforms must be most radical. Remedies must be transformed from formal declarations into effective instruments. This means three things. First, explanation rights must be broadened and deepened. They should apply to all significant AI-driven decisions, and they must provide intelligible reasons, not generic statements. Second, disclosure of evidence must be guaranteed. Providers should be legally obliged to preserve logs, datasets and model versions, and to disclose them to courts and regulators when necessary to review legality, with appropriate safeguards for trade secrets but not at the expense of rights. Third, remedies must be strengthened. The FRIA should not only be a self-assessment but a mechanism subject to independent audit with the power to halt deployment if risks are too great. Together, these reforms would make access to justice substantive. Courts would have the tools to review decisions; individuals would have the information to contest them; oversight bodies would have the authority to intervene.

These proposals are not utopian. They build on existing mechanisms in EU law: the integration of rights-based legal bases, the move from soft law to binding acts, as occurred within the Digital Services Act domain, the experience of independent data protection authorities under the GDPR, and the burden-shifting rules in discrimination law. What is needed is the political will to align AI governance with the Union's own constitutional grammar.

Among the other sources hereby analysed, the 2025 Rule of Law Report shows that the Union already possesses an evaluative grammar for the rule of law, structured around verifiable conditions. Extending this logic to AI governance would mean subjecting the AI Act to a similar cycle of monitoring, using benchmarks of legality, certainty, equality and remedies as indicators of constitutional adequacy. In other words, what the Commission does annually for the Member States should also be done for systemic technologies: constitutionalisation cannot be credible unless the rule of law is made measurable and remedy-capable in practice.

In a nutshell, the broader lesson is that artificial intelligence is the Union's most immediate test of the rule of law. It is not merely another technological field but a transformation in decision-making itself. AI determines how rights are allocated and obligations imposed. It mediates access to welfare, employment, credit, education, migration and justice. If the rule of law is hollow in this domain, it will be hollow in practice. If legality is reduced to delegated acts, certainty to shifting guidelines, oversight to rubber-stamping, equality to self-assessment and remedies to formal complaints, then the rule of law ceases to be a means of rights protection and becomes an empty ritual.

Conversely, if the Union strengthens its framework along the lines suggested, it can demonstrate that the rule of law is resilient, adaptable and substantive. It can show that new forms of power, even when embedded in opaque technical systems, are still subject to law, accountable institutions and effective remedies. In doing so, the Union would not only secure its own constitutional integrity but also shape global governance. The AI

Act is already the first of its kind worldwide. If reoriented towards remedy-capable safeguards, it could become a model for others, setting standards for how AI can be governed in a manner consistent with democracy and rights.

The conclusion, then, is both cautionary and forward-looking. The AI Act is an important step, but it is not sufficient. It constitutionalises AI in form but leaves its substance fragile. Unless reinforced with binding legal bases, clear and stable obligations, independent oversight, verified equality safeguards and effective remedies, it risks trivialising the rule of law into rule by law. Yet the path to reform is clear, and the tools are already within the EU's legal and institutional repertoire. The choice is between a kind of constitutionalisation that is symbolic and another that is real. In the age of artificial intelligence, only the latter will preserve the claim to be a community founded on the rule of law.

Abstract

This article examines the European Union's attempt to regulate artificial intelligence through the AI Act against the Union's own constitutional standard of the rule of law. It advances a functional understanding of the rule of law: not as a symbolic goal, but as a means of protecting rights by providing legality, foreseeability, control of discretion, equality and access to justice. Artificial intelligence poses a structural challenge to this grammar, as autonomy and opacity relocate decision-making from promulgated norms to model design, data selection and inference processes that are difficult to scrutinise. Using the Venice Commission's Rule of Law Checklist as an operational benchmark, the article evaluates the AI Act element by element. It finds that legality is anchored in an internal market basis rather than in rights-oriented Treaty provisions; legal certainty is displaced into shifting Commission guidelines; prevention of abuse is compromised by reliance on delegated acts and industry co-regulation; equality is left to self-assessment through the Fundamental Rights Impact Assessment; and access to justice is nominal, with explanation rights narrow and evidence disclosure absent. The cumulative effect is constitutionalisation in form but not in substance, risking a transformation of the rule of law into *rule by law*. The article concludes by outlining *de iure condendo* reforms that could align the EU AI architecture with its constitutional commitment to the rule of law as a means of protecting rights.