Keele Law Review, Volume 6 (2026), 58-78
ISSN 2732-5679

Reassessing Democratic European Governance in the AI Era: The Path to Artificial Constitutionalism

Elena Girasella*

Abstract

The increasing reliance on Artificial Intelligence (AI) in public administration, law enforcement, and policymaking raises critical constitutional questions concerning legitimacy, transparency, and the rule of law. Although AI-driven decision-making promises greater efficiency and impartiality, it simultaneously risks undermining democratic principles by shifting sovereignty from public institutions to private corporations that design, develop, and control these powerful technologies. Building on the current state of doctrinal scholarship and jurisprudence, a focused analysis of the European AI Act illustrates that AI must remain an instrument for strengthening democratic governance rather than eroding it. The question, therefore, is not whether democracy can endure in the age of AI, but how democratic Member States can harness technological innovation while safeguarding their foundational constitutional values. Addressing these challenges proactively offers the possibility of shaping an AI-driven future that remains consistent with European democratic ideals, reaffirming, not redefining, the constitutional order in the digital age.

I. Introduction

Debates on the regulation of artificial intelligence are increasingly framed in terms of the uncertainty of its impact, which is commonly articulated through the language of risks and opportunities.[1] Much of this discourse takes as a reference both the current state of technological progress and the democratic character of contemporary political systems. Yet, from a constitutional standpoint, many questions remain unresolved, giving rise to an extensive debate among legal scholars concerning the potential dangers and promises that advanced Artificial Intelligence (hereinafter AI) systems may pose to democratic governance.[2]

One of the most pressing issues in this regard concerns the protection of fundamental

* PhD in Political Science, University of Messina, Italy.

[1] For a scientific assessment that highlights opportunities, such as enhanced decision-making; increased transparency and citizen engagement; and threats, including manipulation and misinformation; surveillance and privacy invasion; and bias and discrimination, see ISSIP (ed), 'White Paper AI Impacts on Global Democracy. From a perspective centring service innovation' (2025) <https://issip.org/wp-content/uploads/2025/06/WP_AI_Challenges-to-Global-Democracy_2025-revised-FINAL_June-2025.pdf> accessed 03 November 2025. For a more comprehensive perspective, Jeroen Temperman and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023). In the making of the European regulation, see also '*The GenAi approach: opportunities and challenges*', a dedicated paragraph of the wide publication requested by the European JURI Committee, Giovanni Sartor and Thiago Raulino Dal Pont, *Artificial Intelligence for Monitoring the Application of EU Law* (European Parliament 2025).

[2] A comprehensive analysis in Oier Mentxaka and others, 'Aligning trustworthy AI with democracy: a dual taxonomy of opportunities and risks' [2025] arXiv <https://arxiv.org/pdf/2505.13565> accessed 03 November 2025.

rights. This is the issue that this study seeks to address, taking it as the very purpose of constitutionalism itself.[3]

AI technologies hold significant potential to advance the safeguarding of civil liberties and to strengthen protections for vulnerable groups. Algorithms capable of detecting discriminatory practices, ensuring equal access to services, or providing enhanced legal aid could, in principle, deepen the reach of constitutional guarantees. However, the same technologies can also present new risks. Predictive policing, surveillance systems, and biased decision-making algorithms threaten to erode privacy, equality, and non-discrimination.[4] This tension underscores the need for constitutional democracies to design frameworks that harness AI's capacity to enhance rights protections while imposing strict limits to prevent abuses.

Closely connected to this issue is the relationship between AI and the rule of law.[5] AI systems could contribute to the reinforcement of legal order by streamlining administrative processes, monitoring compliance with constitutional procedures, and enhancing transparency in public decision-making. Digital tools such as automated case management or predictive analytics in law enforcement are already being tested in this direction. Nevertheless, the opacity of certain algorithmic processes, especially those that function as 'black boxes', raises concerns about accountability and due process.[6] If the rationale behind AI-driven decisions cannot be adequately explained, the very principle of transparency that underpins the rule of law is put at risk. The challenge, therefore, lies in reconciling efficiency with constitutional guarantees of clarity, oversight, and accountability.

The separation of powers also comes into question in light of AI's increasing role in governance. Technological applications have the capacity to affect the legislative, executive, and judicial branches alike. Legislatures may employ AI to assist in drafting laws or conducting policy analyses, executives may rely on it to enhance service delivery

---

[3] On the contrary, the question of recognising rights for artificial intelligence as legal subjects, especially in light of so-called generative super-artificial intelligence, is entirely beyond the scope of this work. See, Andrea Bertolini and Francesca Episcopo, 'Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective' (2022) 9 Frontiers in Robotics and AI 1; Claudio Novelli and others, 'AI as legal persons: past, patterns, and prospects' (2025) 52(4) Journal of Law and Society 533; Rosa Maria Ballardini and Robert van den Hoven van Genderen, 'Artificial Intelligence and Intellectual Property Rights: The Quest or Plea for Artificial Intelligence as a Legal Subject' in Taina Pihlajarinne and Anette Alén-Savikko (eds), *Artificial Intelligence and the Media: Reconsidering Rights and Responsibilities* (Edward Elgar 2022) 192–214.

[4] In example, see the Wisconsin Supreme Court sentence on the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) algorithm in the American criminal justice system, *State v. Loomis,* 881 N.W.2d 749 (Wis, 2016); Among scholarly contributions, Ludvig Beckman, Jonas Hultin Rosenberg and Karim Jebari, 'Artificial intelligence and democratic legitimacy. The problem of publicity in public authority' (2024) 39 AI & Society 975.

[5] The reference to the rule of law in this contribution is grounded in the assumption that even the most recent instances of democratic backsliding should not undermine the ideal of the rule of law, which «is like the law of gravity: it is the rule of law that ensures that our world and our societies remain bound together and that order prevails over chaos. It unites us around common values and anchors us in the common good», United Nations General Assembly, 67th session, 3rd plenary meeting, UN Doc A/67/PV.3 (24 September 2012), 2. For further analysis consistent with the methodological approach adopted here, and specifically aimed at examining the concept of the rule of law in light of the most recent developments in Europe, see Luca Pantaleo and Marco Siddi, *The rule of law crisis and democratic backsliding in the EU. Open questions and outstanding challenges* (G. Giappichelli Editore 2025); Pieter-Augustijn Van Malleghem, 'Legalism and the European Union's rule of law crisis' (2024) 3(1) *European Law Open* 50; Martin Belov (ed), *Rule of Law in Crisis: Constitutionalism in a State of Flux* (Routledge 2023).

[6] Stanley Greenstein, 'Preserving the rule of law in the era of artificial intelligence (AI)' (2022) 30 *Artificial Intelligence and the Rule of Law* 291.

and regulatory enforcement, and judicial bodies may turn to AI tools for legal research or case prediction.

These applications promise efficiency and innovation, yet they also risk blurring the boundaries between institutional functions and diminishing the scope for human deliberation. A constitutional order founded on checks and balances must therefore carefully assess the extent to which AI complements, rather than AI replaces human decision-making within each branch of government.[7]

Finally, the question of popular sovereignty emerges as perhaps the most fundamental constitutional concern. AI offers opportunities to strengthen democratic participation by providing platforms for more inclusive deliberation, analysing citizen preferences with greater precision, and combating the spread of misinformation. At the same time, these technologies can be weaponized to manipulate public opinion, polarize debate, and undermine electoral integrity through practices such as micro-targeted political advertising. In this respect, the promise of AI to foster more meaningful participation coexists uneasily with its potential to distort the democratic process.[8]

Constitutional frameworks must therefore grapple with how to integrate Artificial Intelligence into democratic life in ways that strengthen rather than weaken both the principle of popular sovereignty and that of State sovereignty, particularly in light of the privatization of sovereignty itself brought about by the private ownership and control of AI technologies.

II. Challenging constitutional values in the AI era

When most States were still in the process of adapting their administrative structures to modern Information Technology (IT), Artificial Intelligence had already begun to permeate the sphere of public governance. In this respect, the integration of AI was expected to advance the same goals traditionally associated with digital modernization: efficiency, cost-effectiveness, improved performance, and greater accessibility.

From this perspective, such systems appeared to hold the promise of deepening democracy by making public services more accessible, responsive, and transparent. Yet, rather than serving solely as instruments of democratic progress, they also carry the risk of eroding the very foundations of democracy itself. The narrative of administrative modernisation has long posited that digital systems enable the State to streamline operations, reduce costs, and enhance citizen access to services. This remains deeply attractive to public administrations. The OECD's recent study emphasises that AI is being deployed precisely in core government functions under the promise of a 'digital government journey'.[9]

In that sense, AI even appeared as the natural next step in the ongoing programme of Information Technology (IT) modernization. Technically, novel instruments intended to pursue the same administrative objectives of greater efficiency, cost-saving and improved service delivery. However, the arrival of AI is not merely about speed and scale; it marks a qualitative transformation because an ever larger share of public choices and determinations is being shifted from human officials to algorithmic systems whose

[7] Hans-W Micklitz and others (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021).

[8] Hunt Allcott and others, 'The effects of Facebook and Instagram on the 2020 election: A deactivation experiment' (2024) 121(21) PNAS <www.pnas.org/doi/epdf/10.1073/pnas.2321584121> accessed 03 November 2025.

[9] OECD, *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions* (OECD Publishing 2025).

operational logic, transparency and modes of accountability do not necessarily fit the conventional standards of public administration and public law.[10]

The concept of democracy is not just about procedural access to services, but about public authority acting in ways whose reasons are accessible, whose power is contestable, whose exercise is visible to citizens. The ideal of democracy presupposes that citizens can understand and challenge decisions of public authorities. When such decisions are mediated by opaque AI systems, the public sphere becomes less intelligible, less responsive. As the Council of Europe explanatory report warns: 'Such use of AI systems can undermine democratic values, curb the free will of the people and erode political freedoms'.[11]

Thus, the paradox: systems intended to render everything more accessible, to enhance democracy through digital means, may end up undermining democracy's foundations. The administrative machine becomes more efficient but less transparent; the citizen interface more convenient but less meaningful; the delegation to algorithmic decision-systems faster but less contestable. The challenge becomes how to frame a governance regime such that the promise of AI is realised without sacrificing the normative commitments of public law and democracy.

From a constitutional law perspective, many profound questions remain unresolved, sparking vigorous debate among legal scholars regarding how advanced AI systems might endanger, or enrich, democratic political systems. For a better understanding, we argue that the use of AI in public decision-making must be analysed through the lens of the rule of law.[12] In this perspective, regarding the protection of fundamental rights and those to recognize to minorities above all, Sonia Katyal emphasizes how AI's rise, through privatization, prediction, and automation, poses novel threats to minority protections, necessitating a reinvigoration of judicial review tailored for the AI era.[13]

Meanwhile, Christian Djeffal highlights that AI can either erode or bolster democratic processes, depending on how legal norms guide its development.[14] The idea of embedding constitutional-like constraints into AI systems has been gaining traction. For instance, anthropic concept of Constitutional AI aims to codify principles such as 'helpful', 'honest', and 'harmless' into AI models, but critics argue that such frameworks lack democratic legitimacy and transparency. On the point, Gilad Abiri's proposal for Public Constitutional AI furthers this model by advocating participatory, deliberative processes and the creation of AI 'case law' bolstering both accountability and democratic input.[15]

More deeply about the separation of powers, assuming that AI is increasingly executing functions long reserved for public institutions, raising profound questions about authority and legitimacy, Yiyang Mei and Michael Broyde reframe AI governance as a constitutional question, arguing that algorithmic power must be rooted in participatory authorization, distribution across representative bodies, and the capacity for lawful

[10] Bignami Francesca, 'Artificial Intelligence Accountability of Public Administration' (2022) 70(1) The American Journal of Comparative Law 312.
[11] Ad Hoc Committee on Artificial Intelligence (CAHAI) (ed), 'Feasibility Study' (2020) <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da> accessed 03 November 2025. CAHAI is currently replaced by the Committee on Artificial Intelligence (CAI).
[12] As anchored in Article 2, Consolidated Version of the Treaty on European Union and further operationalised through the Charter of Fundamental Rights, [2016] OJ C-202/1.
[13] Sonia K. Katyal, 'Democracy & Distrust in an Era of Artificial Intelligence' (2022) 151(2) Daedalus 322.
[14] Christian Djeffal, 'AI, Democracy and the Law' in Andreas Sudmann (eds), *The Democratization of Artificial Intelligence: Net Politics in the Era of Learning Algorithms* (Transcript 2019).
[15] Gilad Abiri, 'Public Constitutional AI' (2025) 59(2) Georgia Law Review 601.

resistance when normative boundaries are breached.[16]

A minority strand of legal scholarship emphasizes that the relationship between Artificial Intelligence and the Rule of Law can also be viewed in a positive light. This is exemplified in the work of Stephen Daly, who argues that embracing AI tools could actually help to advance the aims of the Rule of Law, as shown in his examination of the use of AI by tax authorities.[17]

Nevertheless, these positions must be grounded in the recognition that AI systems ought to be designed, monitored, and implemented in accordance with the value-oriented principles of the rule of law, understood in their full axiological dimension.[18]

In this regard, Roger Brownsword advises how 'The regulatory stewards should have some independence from the political branch, but not of course that they should be exempt from the Rule of Law's culture of accountability and justification'.[19]

This brief survey gives us the general sense of the issue.

What emerges with broad scholarly consensus is that authority over decision-making, traditionally reserved for public institutions, is increasingly being transferred to private actors, particularly in strategically sensitive sectors such as defence and critical digital infrastructure.[20] In contexts where artificial intelligence systems developed by commercial entities are deployed to support, guide, or even automate decisions related to military operations and security management, the conventional *locus* of accountability is displaced from democratic institutions to corporate discretion. This shift engenders significant constitutional and normative challenges, as it tests the capacity of existing legal frameworks to uphold transparency, proportionality, and effective oversight while simultaneously embedding private power at the core of decisions with profound societal consequences.

It is within this context that the concept of 'artificial constitutionalism' becomes relevant. Rather than opposing technological transformation, artificial constitutionalism seeks to reaffirm and operationalise constitutional principles from within the evolving AI landscape. This approach places responsibility both on States and on the private entities that develop and deploy AI systems.

With regard to the commitment of States, the signing in Vilnius the 5 September 2024 of the 'Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law' can be welcomed as a significant step forward. The purpose of this landmark instrument of soft law is precisely to ensure, as stated in

---

[16] Yiyang Mei and Michael Broyde, 'Reclaiming Constitutional Authority of Algorithmic Power' [2025] arXiv <https://arxiv.org/abs/2508.11699> accessed 03 November 2025.

[17] Stephen Daly, 'Artificial Intelligence, the Rule of Law and Public Administration: The Case of Taxation' (2024) 83 Cambridge Law Journal 437.

[18] On the Eurocentric conception of the rule of law and its contemporary crisis, Gaetano Silvestri, 'Lo Stato di diritto nel XXI *secolo'* (2011) 2 AIC 1.

[19] Roger Brownsword, 'Law Disrupted, Law Re-Imagined, Law Re-Invented' [2019] Technology and Regulation 10, 29.

[20] This contribution does not address the issue of the interplay between public and private interests in the global competition over the proprietary use of Artificial Intelligence. The argument proceeds on the assumption that, although at first glance the impact of AI appears to have prompted States to compete for supremacy in asserting their 'artificial sovereignty', a deeper examination reveals a reversal of this dynamic. For further discussion and detailed analysis, see Jhon Mikler, *The Political Power of Global Corporations* (Cambridge Polity Press 2018); Lucas Maaser and Stephanie Verlaan, *Big tech goes to war. Uncovering the growing role of us and European technology firms in the military–industrial complex* (Rosa Luxemburg Stiftung 2022); Martin Ebers and Marta Cantero Gamito (eds), *Algorithmic Governance and Governance of Algorithms: Legal and Ethical* Challenges (Springer 2021).

Article 1, that activities carried out throughout the lifecycle of artificial intelligence systems remain fully consistent with the protection of human rights, the preservation of democracy, and the safeguarding of the rule of law.[21] Were the provisions of this instrument to be broadly implemented, particularly by the private corporations that own and develop artificial intelligence systems, the future of the rights-protection framework would appear not merely less uncertain but indeed promising.

By aligning generative AI and other advanced technologies with established constitutional values, these actors can not only safeguard the resilience of existing rights-protection regimes but also actively contribute to their extension and deepening. In this sense, the technological mediation of decision-making need not undermine constitutional norms but can instead serve as a vehicle for reinforcing accountability, embedding human-centred values into automated processes, and promoting a rights-respecting governance framework for the digital age.

This thesis is expected to be confirmed by the convergence of the different actors on the global stage. The premises on which it is founded are fully traceable at European level. Europe, unlike the USA, the Russian Federation, or China, does not represent a single political system and does not have a single digital market. However, it is based on a common value-system, and it has looked to it in its attempt to harmonise the use of AI-systems. That is why this contribution now intends to refer to the first regulation on artificial intelligence in Europe, the so-called European AI Act.[22]

III. The European AI Act, lessons learned from a regulatory system still in the making

As previously noted, the use of AI in public administration is not merely a matter of technological innovation but one of constitutional transformation. The challenge for EU Member States is to ensure that the pursuit of algorithmic efficiency does not come at the expense of the constitutional order but rather enhances the capacity of public administration to serve the public interest within the boundaries of law, rights, and democracy.

The 180 'Whereas' introducing the Act clearly demonstrate this orientation. Summarising the scope of the Act in general terms, the use of AI in public administration must be situated within the principle of legality and the right to good administration under Article 41 of the Charter of Fundamental Rights. Any automated administrative process must comply with the requirements of transparency, reasoned decision-making, and effective remedy.

Moreover, the principle of accountability, central to both Article 2 TEU and the Charter, demands that public authorities remain institutionally responsible for the outputs of AI systems. As already emphasised, delegating *de facto* decision-making power to AI risks creating an opaque administration in which the chain of legal responsibility becomes

[21] As of 1 October 2025, the most recent update records forty-three signatories, including the European Union, Canada, the United States, Israel, Ukraine, and the United Kingdom.

[22] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 2024/1689. The contribution does not provide a comprehensive analysis of the legislative act. Rather, it draws attention to specific aspects that, by their very nature, have the most direct impact on human rights and the constitutional values established to protect them. For a summary of the provisions and the state of the art of its implementation, see Irina Orssich, 'The AI Act-brief introduction' in Benjamin Raue and others (eds), *Artificial Intelligence and Fundamental Rights. The AI Act of the European Union and its implications for global technology regulation* (volume 4, Institute for Digital Law Trier 2025).

diffuse or even invisible, thereby compromising judicial review and weakening democratic control.[23]

Data protection and privacy, enshrined in Articles 7 and 8 of the Charter and operationalised through the General Data Protection Regulation (GDPR), further constrain AI use in public administration. Profiling, automated decision-making, and predictive analytics, central to many AI systems, must be subject to strict safeguards, particularly where sensitive personal data or vulnerable populations are concerned.

The EU's Artificial Intelligence Act, currently under implementation, attempts to codify a risk-based regulatory framework, classifying AI systems by their potential impact on rights and safety.[24] The European Union's Artificial Intelligence Act represents a milestone in global technology regulation, introducing an architecture grounded in a risk-based approach that seeks to reconcile innovation with the protection of fundamental rights. Within this framework, AI systems are classified according to their potential to harm individuals or society. The Act distinguishes between four levels of risk, unacceptable, high, limited, and minimal. corresponding to the degree of regulatory scrutiny required. The most intrusive systems, those considered 'unacceptable', are prohibited outright because their use is deemed incompatible with European values of human dignity, equality, and democratic accountability.

'High-risk' systems, such as those deployed in law enforcement, critical infrastructure, or education, are subject to stringent obligations, including conformity assessments, documentation duties, and post-market monitoring. By contrast, 'limited-risk' applications, typically involving interaction with users or information provision, are regulated primarily through transparency obligations, while 'minimal-risk' systems are left largely unregulated. In theory, this stratified structure aims to ensure proportionality by tailoring obligations to the magnitude of potential harm, thereby avoiding both over-regulation and regulatory gaps.[25]

This model is inspired by the regulatory philosophy already tested in the field of data protection, particularly through the European General Data Protection Regulation (GDPR).[26] Like the GDPR, the AI Act entrusts much of the responsibility for compliance to the very actors who develop and deploy these systems. In the data protection context,

---

[23] The question of accountability in the GDPR (e.g., Articles 5 and 24) 'works as a meta-principle directed at data controllers so that they demonstrate, by virtue of their information background, compliance with GDRP requirements in the processing of personal data and as a remedy mechanism for failure to comply with them', Claudio Novelli, Mariarosaria Taddeo and Luciano Floridi, 'Accountability in artificial intelligence: what it is and how it works' (2024) 39 AI & Society 1871. For a comprehensive overview of the principal legal challenges in ensuring transparency and accountability in artificial intelligence systems, Ben Chester Cheong, 'Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making' (2024) 6 Frontiers in Human Dynamics 1.

[24] In light of the relative ease of access to information regarding the origin and implementation of the Act, see the recent '*Open Joint Letter against the Delaying and Reopening of the AI Act*'. The letter articulates collective concerns about the forthcoming proposal intended to simplify the digital regulatory framework, which reportedly may entail a reconsideration of the Artificial Intelligence Act, </www.beuc.eu/sites/default/files/publications/BEUC-X-2025-066_Open_Joint_Letter_against_the_Delaying_and_Reopening_of_the_AI_Act.pdf> accessed 10 November 2025.

[25] Valentina D'Antino, 'L'approccio basato sul rischio nell' AI Act: un nuovo paradigma di regolazione dell'intelligenza artificiale' (2025) 18 Federalismi.it 15.

[26] Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

this principle manifests in the notion of accountability, where data controllers are required not only to comply with the law but to demonstrate such compliance.

As observed by De Gregorio, the GDPR's reliance on a risk-based model effectively grants private entities a central role in determining how, rather than whether, they will comply with the law.[27] Controllers assess the risks associated with processing activities, decide what safeguards to adopt, and evaluate whether their measures align with the regulation's general principles. Although this flexibility allows for context-sensitive solutions, it simultaneously risks transforming compliance into a matter of procedural formalism rather than substantive protection.

A similar critique applies to the AI Act. The delegation of evaluative power to private operators may lead to a system in which the interpretation of 'risk' becomes contingent upon corporate assessments and technical self-reporting, rather than being anchored in robust external oversight. This introduces a potential paradox: the very subjects whose activities require regulation are often the same entities responsible for assessing and mitigating the risks they generate.

Scholars such as Yeung have described this as the 'regulatory turn to self-assessment', a process through which regulatory responsibility is outsourced to private actors under the guise of flexibility and innovation.[28] The result may be a regulatory landscape where compliance is framed as a technical exercise of risk management rather than a normative commitment to rights and accountability. Moreover, the risk-based approach, while pragmatic, has intrinsic limitations when applied to artificial intelligence. Risk assessment presupposes the capacity to foresee and quantify potential harms, yet AI systems, especially those based on machine learning and generative architectures, operate through dynamic, adaptive processes that evolve beyond initial programming. Their unpredictability undermines *ex ante* evaluation models and makes it difficult to determine at the design stage which risks may materialise during deployment. This uncertainty creates a structural tension within the AI Act because, although the Act seeks to pre-empt harm through categorisation, it relies on static criteria that are poorly suited to technologies that are inherently fluid and context dependent.

This problem becomes more pronounced when considering the broader implications for constitutional governance. If AI tools can adapt their behaviour to remain within the boundaries of legality without any substantive understanding of law's normative purpose, then legality risks being reduced to a computational process devoid of moral or constitutional content.

The law, traditionally conceived as an instrument of human judgment and ethical deliberation, may become a set of operational parameters enforced by the systems themselves. As scholars such as Hildebrandt argue, this operationalization of normativity challenges the anthropocentric foundations of law, demanding new conceptual tools to preserve human agency in environments increasingly governed by code.[29]

From a constitutional perspective, this shift marks a critical juncture. The more regulation depends on the self-governing capacities of AI systems, the less it reflects the deliberative essence of democratic decision-making. Legal norms risk being translated into algorithmic constraints rather than humanly interpreted principles. The emergence of

[27] Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022).
[28] The author focuses her analysis on the blockchain technology and the challenges to operate without the need for the state as a central authority. See Karen Yeung, 'Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law' (2019) 82(2) Modern Law Review 207.
[29] Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford University Press 2020).

what could be termed 'artificial legality' threatens to displace the constitutional balance between power and accountability, as authority migrates from human institutions to technological systems embedded within private infrastructures.

The principle of legality, which requires that power be exercised under the law and subject to review, is strained when decision-making processes become opaque, self-referential, and resistant to scrutiny. Furthermore, the concentration of technological power in the hands of a few multinational corporations complicates the exercise of sovereign control. Despite States' attempts to assert 'artificial sovereignty', their regulatory reach is often circumscribed by the global nature of digital infrastructures and the economic leverage of private actors. As Cohen notes, the governance of informational capitalism is shaped not by traditional hierarchies of authority but by networks of interdependence where private platforms perform quasi-regulatory functions.[30] In this environment, law risks becoming reactive rather than directive, following the trajectories of technological change rather than guiding them.

A possible way forward lies in reconfiguring the relationship between law, technology, and governance. The risk-based model should not be abandoned, but it must be supplemented with stronger institutional guarantees and substantive accountability mechanisms. Independent oversight bodies with technical expertise are essential to verify industry assessments and monitor compliance continuously. Moreover, transparency obligations must extend beyond formal documentation to include public access to information about system design, data sources, and performance metrics. Through such measures can risk-based regulation evolve from a procedural framework into a vehicle for democratic legitimacy.

Ultimately, the effectiveness of the AI Act will depend on whether it can move beyond the rhetoric of risk management toward a genuine constitutionalisation of AI governance. This means reasserting the primacy of human values and legal principles over technological optimisation. Regulation should not merely aim to prevent harm but to shape the moral and institutional ecosystem in which AI operates. As De Gregorio and others suggest, the challenge is to integrate constitutional reasoning into the design of digital regulation itself, ensuring that rights and accountability are not external constraints but intrinsic elements of technological development.[31]

By embracing this vision, European law can uphold its constitutional promise in an era where governance increasingly occurs through autonomous systems. Yet the Act's governance model, which relies on conformity assessment, technical standards, and national oversight bodies, may not fully address constitutional accountability gaps. While it represents a significant step toward harmonisation, the Act leaves unresolved the deeper question of how constitutional values, such as human dignity, non-discrimination, and legal certainty, are to be protected in algorithmic governance.

The EU AI Act, in fact, details cases, circumstances and flows that mainly concern transactions taking place within the European market. In relation to these, protections for the person are invoked. What, however, should receive greater attention is the very transformation of the concept of the person, today no longer only a legal subject but in itself an object of law.[32]

---

[30] Julie Elisabeth Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).

[31] De Gregorio (27).

[32] With reference to the early transformations brought about by the advancement of information technology, and in further elaboration of the argument proposed, see Julie Elisabeth Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012), and Stefano Rodotà, *Il*

The contemporary digital economy has normalised a deep shift in the legal status of the individual: from a bearer of rights to a commodity-like node in markets of data, attention, and predictively modelled behaviour.

What began as a subtle instrumentalisation of fundamental rights in the name of global efficiency has consolidated into an architecture in which persons are assessed, ranked, and traded as bundles of data points. In the earlier phases of economic globalisation, substantive rights were reinterpreted as accessories to market freedoms, rendering the rights-bearing subject simultaneously an economic factor—consumer, user, or prosumer, whose dignity was implicitly mediated by transactional logics.[33] In the digital era the subject is reframed as a product whose value fluctuates with algorithmic appraisals extracted from personal data and behavioural traces.[34] Thus, dependence on the use of technological platforms, which now pervade human action endemically, effectively renders meaningless the safeguards designed to protect individual rights. The increasingly pressing necessity to remain connected, to employ available tools, and to exist as persons even in virtual reality entails an equally pressing compulsion to grant consent to any request for access, disclosure, or use of personal data. This, in turn, undermines, or at least significantly weakens, the provisions of the European AI Act concerning informed consent (Art. 61), as well as those relating to harm arising from manipulation, for example (Art. 5).[35]

When automated decision-making becomes pervasive, the fundamental question shifts from consent formalities to the substance of power: who defines the purposes, shapes inferences, and sets the thresholds that distribute benefits and burdens across populations? In view of this, rights cannot be reduced to transactional waivers, they must retain their *status* as constraints that channel both public and private power. In this sense, the neologism coined by Luciano Floridi is particularly striking, as he speaks of the 'onlife' condition to describe the new experience of a hyperconnected reality in which it no longer makes sense to ask whether one is online or offline.[36]

Critically, commodification in the digital environment does not occur merely through the sale of raw personal data but rather through the monetisation of predictive inferences concerning future behaviours or conditions such as creditworthiness, consumer attrition, or susceptibility to persuasion. These predictions emerge from a complex data ecology composed of observed information, inferred characteristics, and proxy variables that

---

diritto di avere diritti (Laterza 2012), which builds upon his earlier reflections, explaining how 'Technologies challenge old rights and impetuously demand new ones. Around them, the very identity of the subject is redefined', Stefano Rodotà, *Tecnologie e diritti* (Il Mulino 1995) 15. Strictly on the evolution of rights related to the evolution of the personal identity within the digital transformation in the EU context, Valeria De Santis, 'Identità e persona all'epoca dell'intelligenza artificiale: riflessioni a partire dall'IA Act' (2024) 19 Federalismi.it 137.

[33] Aware of the impossibility of generalising across the peculiarities of individual legal systems to which reference should be made, this analysis focuses on the evolution of rights such as the right to personal identity and the right to privacy within the broader context of the ongoing technological transformation. For a more detailed examination of this issue in relation to the Italian legal framework, see Giorgio Pino, 'The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights' in Mark Van Hoecke and François Ost (eds) *The Harmonization of Private Law in Europe* (Hart Publishing 2000). A wider approach, in the light of article 8 of the ECHR in Lusine Vardanyan and Hovsep Kocharyan, 'The right to data protection in the light of personality rights: does it prevent the emergence of data ownership?' (2022) 4(1) Journal of Ethics and Legal Technologies 105.

[34] See Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

[35] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22(4) Computer Law Review International 97.

[36] Luciano Floridi (ed), *The Onlife Manifesto: Being Human in a Hyperconnected Era* (Springer 2015).

frequently reproduce existing social asymmetries. The resulting outputs are circulated in markets not as personal data but as so-called 'insights' or 'audiences', even though they directly shape how individuals are targeted, priced, and monitored within algorithmic systems.[37]

Contemporary debates on global data governance frequently present data as a new factor of production whose circulation must be optimised to stimulate innovation and economic growth. While such narratives highlight the potential gains from increased data access and sharing, they often overlook the normative dimension of informational power.

From a constitutional perspective, the question is not whether data should flow, but under what conditions such flows remain compatible with the protection of the person as the ultimate end of legal order. The challenge lies in embedding informational infrastructures within a hierarchy of norms that affirms dignity, autonomy, and accountability as foundational values.[38] Within this framework, on the EU AI Act the so-called right to explanation (art.86) emerges as a crucial constitutional safeguard. It expresses the individual's entitlement to understand, question, and influence the automated processes that increasingly mediate access to services, opportunities, and recognition.[39]

This right, however, cannot be reduced to a mere formal notification of algorithmic involvement; it must instead encompass substantive transparency, enabling individuals to reconstruct the logic, purposes, and consequences of automated decision-making. It requires that affected persons be equipped not only to understand how decisions are reached but also to contest them effectively and to obtain meaningful remedies. In this sense, the right to explanation should operate as a bridge between procedural fairness and substantive justice within the algorithmic environment.

Public-interest data intermediaries and fiduciary duties for digital platforms could serve as vehicles for operationalising this normative demand by mediating between informational asymmetries and constitutional accountability. The broader objective is to restore a person-centred informational order in which explanation, participation, and contestation are treated not as compliance burdens but as expressions of democratic legitimacy. A genuinely constitutional approach to artificial intelligence thus requires the translation of this insight into the architecture of data governance itself, reaffirming that explanation is not a procedural accessory but a condition of freedom in the digital age.

This argument is situated within what can now be identified as the emerging strand of digital constitutionalism, a framework increasingly invoked to examine the normative constraints and rights-based imperatives of the digital environment.

---

[37] Cohen (30) and the still actual contribution of Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar 2015).

[38] Beyond the references already provided, see Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76.

[39] On the right to explanation in the EU AI Act, Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual explanations without opening the Black Box: automated decisions and the GDPR' (2018) 31(2) Harvard Journal of Law & Technology 841; Margot Kaminski and Gianclaudio Malgieri, 'The Right to Explanation in the AI Act' (2025) 25(9) University of Colorado Law Legal Studies Research Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5194301> accessed 03 November 2025; Lilian Edwards and Michael Veale, 'Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for' (2017) 16(1) Duke Law & Technology Review 18; Lilian Edwards and Michael Veale, 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?' (2018) 16(3) IEEE Security & Privacy 46. For a technical study see the business manual edited by The Research Institute – Digital Human Rights Center '*The right to explanation in the AI Act*' (2025).

Over the past decade, the term has been employed to conceptualise the constitutional dimensions of data governance, algorithmic decision-making, and platform regulation. Within this framework, however, multiple approaches coexist.

This contribution does not aim to engage with the line of research focused on identifying new or evolving rights in response to ongoing digital transformations, which often seeks to provide solutions to the evident issue that generative AI may produce content susceptible of legal protection, independently of the inputs provided by natural or legal persons who interact with it. By a process of exclusion, it likewise does not align with scholarship advocating the drafting of 'digital constitutions', that is, proposals aimed at revising constitutional frameworks to accommodate the emerging digital reality. Instead, the analysis offered here, informed by doctrinal debate and by the current regulatory landscape in Europe, points to the need to reinforce a theory of constitutionalism grounded in values in the digital age.

In the view investigated, this entails recognising the continued relevance of modern constitutionalism even in the context of ongoing technological transformations. It further implies harnessing available instruments to ensure that emerging technologies are guided by constitutional values capable, by their intrinsic force, of constraining power wherever it is exercised. In practical terms, this approach seeks to bridge the gap between normative ideals and technological practice, embedding fundamental principles such as human dignity, autonomy, accountability, and proportionality into the design, deployment, and oversight of digital infrastructures.

The critical review has also provoked crucial scrutiny, questioning the conceptual coherence, normative force, and practical significance of digital constitutionalism in light of established constitutional theory. Critics contend that applying the notion of constitutionalism risks overstating the normative weight of initiatives that are largely regulatory, self-regulatory, or technical in nature and that may not satisfy the core procedural and substantive guarantees traditionally associated with constitutional frameworks. From this perspective, digital constitutionalism is often depicted as a project shaped or co-opted by private actors, particularly major digital platforms, which raises concerns regarding accountability, the protection of fundamental rights, and the institutional capacity of public authorities to enforce constitutional norms in the data-driven economy.

Within the European context, these critiques underscore the need for a framework in which principles such as transparency, contestability, proportionality, and effective oversight are not merely aspirational but operationalised, ensuring that the development and deployment of AI and digital infrastructures respect the primacy of human dignity, personal autonomy, and the rule of law.

IV. European jurisprudential Insights on AI Governance

The arguments presented thus far already find substantial support in judicial precedent. This paragraph aims to provide a selected synthesis of both pending and concluded cases, which may enrich the body of knowledge underpinning the analysis of artificial constitutionalism as advanced herein.

The jurisprudential backbone of contemporary struggles to align automated governance with constitutional values is formed by the Court of Justice of the European Union's (ECJ) landmark rulings on data protection and consent, which have repeatedly reaffirmed the primacy of fundamental rights in the digital setting.

In *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems,*[40] the Court invalidated the EU–US Privacy Shield on the ground that United States surveillance law did not provide protections essentially equivalent to EU fundamental-rights standards, thereby demonstrating that commercial bargains and cross-border data flows cannot eclipse constitutional guarantees. [41]

The decision's insistence that adequacy of protection be assessed substantively rather than formally has a direct bearing on AI systems whose operation depends on transnational data pipelines: if the legal environment in the recipient jurisdiction cannot be shown to secure rights in practice, transfers are impermissible, with consequential implications for multinational AI services that rely on offshore processing and model training. The judgment thus operates as a constitutional constraint on the architecture of AI supply chains, reinforcing the proposition that regulatory design must attend to systemic, structural threats to rights rather than merely ex post remedies.[42] Complementing the ECJ data-protection line is a stream of jurisprudence from the European Court of Human Rights (ECtHR) that clarifies the scope of privacy and procedural safeguards in contexts of mass and automated surveillance.

The Grand Chamber's engagement with bulk interception and state surveillance in the cases collected under *Big Brother Watch and Others v The United Kingdom* emphasises the necessity for adequate procedural guarantees and independent oversight whenever technical systems permit large-scale collection and automated processing of personal communications. [43]

An additional precedent established by the ECtHR, *Wieder and Guarnieri v United Kingdom* deepens the European judicial engagement with algorithmic and data-driven governance. [44] The case was brought by two cybersecurity researchers, Joshua Wieder, an American citizen, and Claudio Guarnieri, an Italian citizen, who challenged the United Kingdom's system of bulk interception of communications and intelligence sharing under the Investigatory Powers Act 2016. They argued that these practices, especially in their automated and algorithmically-driven dimensions, infringed their rights under Articles 8 and 10 of the European Convention on Human Rights.

The Court acknowledged that the applicants, though residing outside the United Kingdom, fell within the jurisdiction of the respondent State for the purposes of Article 1 of the Convention, as their communications were capable of being intercepted and analysed by UK authorities. This interpretation expanded the extraterritorial reach of the Convention in the context of global digital networks, reaffirming that human-rights protection cannot be constrained by geographical borders when surveillance

---

[40] Case C-311/18 [2020] ECLI:EU:C:2020:559.

[41] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L 207/1. On the case and its implications for the new framework governing transatlantic data flows between Europe and the United States, see Sergi Batlle and Arnaud van Waeyenberge, 'EU–US Data Privacy Framework: A First Legal Assessment' (2024) 15(1) European Journal of Risk Regulation 191.

[42] Ibid 40. See Cinzia Peraro, 'Protezione extraterritoriale dei diritti: il trasferimento dei dati personali dall'Unione europea verso Paesi terzi' (2021) 3 Ordine internazionale e diritti umani 666.

[43] App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021). See Monika Zalnieriute, 'Big Brother Watch and Others v. the United Kingdom' (2022) 116(3) American Journal of International Law 585.

[44] App nos 64371/16 and 64407/16 (ECtHR, 12 Sep 2023). See Yuval Shany, 'Catching Up: The European Court of Human Rights approximates its approach to extraterritorial jurisdiction over Digital Surveillance to that of the Human Rights Committee' (2024) 5 European Convention on Human Rights Law Review 182.

technologies operate transnationally.

On the merits, the Court found a violation of Article 8 ECHR, emphasising that the legal framework governing bulk interception lacked sufficient safeguards against arbitrary interference. In particular, the Court noted that the interception and selection of data involved large-scale automated filtering processes based on selectors, keywords, and analytical algorithms, yet the safeguards controlling those automated stages were insufficiently precise or subject to independent oversight.

The legislation did not adequately define the parameters for automated processing or specify how machine-learning or pattern-recognition systems could be used to derive inferences about individuals. This opacity meant that the interference was not 'in accordance with the law' within the meaning of Article 8(2) ECHR.

The Court also stressed that effective safeguards require not only prior authorisation but continuous and independent supervision throughout the surveillance cycle, especially where algorithms autonomously prioritise or flag data for human review. Such systems, if left unchecked, risk producing forms of *de facto* automated decision-making about individuals' communications and activities without accountability. In this sense, *Wieder and Guarnieri* is the first Strasbourg judgment to engage explicitly with the algorithmic dimension of state surveillance, recognising that the constitutional risks of automation go beyond mere data volume to include opacity, bias, and the absence of human oversight.

With respect to Article 10 ECHR, the Court reiterated that journalists, researchers, and activists enjoy enhanced protection due to their role in democratic discourse. Because both applicants were engaged in investigative cybersecurity and digital-rights research, the interception regime's chilling effects on their professional activities were constitutionally relevant. The Court held that the system's lack of precision and the absence of procedural guarantees against the misuse of intercepted material violated the essence of freedom of expression.

Doctrinally, the case offers the Court an opportunity to refine its jurisprudence following *Big Brother Watch and others v The United Kingdom*,[45] and *Zakharov v Russia*,[46] which will be discussed in more detail below), by examining whether existing safeguards judicial warrants, post-factum review, and ministerial authorisation are sufficient when surveillance systems are powered by artificial intelligence capable of self-optimisation. It also invites reconsideration of how the necessity in a democratic society test should operate when predictive analytics can anticipate and act upon human behaviour without direct human intervention.

If the Court recognises the qualitative difference between human and algorithmic surveillance, *Wieder and Guarnieri* could mark a new stage in European human rights law, one that extends constitutional reasoning from the control of State discretion to the governance of automated decision systems themselves.

At a deeper level, the case underscores a broader institutional concern. As digital infrastructures increasingly blur the boundary between public and private intelligence operations, effective constitutional oversight depends not only on formal legal authorisation but on technical auditability and algorithmic transparency. The applicants' claim, framed within the vocabulary of informational self-determination, thus contributes to the ongoing European debate about whether current legal instruments, designed for the analogue era, can meaningfully constrain machine-

[45] Ibid 43.
[46] App no 47143/06 (ECtHR, 4 Dec 2015).

intensive governance.

As mentioned, the Grand Chamber's judgment in *Zakharov v Russia* stands as a seminal articulation of the European Court of Human Rights' constitutional understanding of privacy and State surveillance in the digital age. [47]

The applicant, Roman Zakharov, a Russian journalist and editor-in-chief of a publishing company, challenged the Russian system of secret surveillance of mobile telephone communications, arguing that the legal framework governing interception lacked sufficient safeguards to prevent arbitrary or abusive interference by public authorities. The Court, in a 17-judge Grand Chamber formation, unanimously found a violation of Article 8 ECHR, holding that the mere existence of a legislative framework permitting secret interception of communications, without adequate procedural guarantees and independent oversight, amounted to an interference with private life.

The judgment is of particular constitutional relevance because it recognised *locus standi* for potential, rather than actual, victims of surveillance, thus departing from a strictly individualised notion of harm. The Court emphasised that surveillance measures must be necessary in a democratic society, a test that encompasses legality, foreseeability, and proportionality and it went further, by stressing that such measures must also be subject to effective, independent, and impartial oversight, both *ex ante* and *ex post*. This introduced a standard of accountability that resonates with the principle of 'algorithmic transparency' in AI regulation.

In the reasoning, the ECtHR explicitly criticised the Russian legal framework for granting the Federal Security Service (FSB) direct and unmonitored access to telecommunications networks, without requiring prior judicial authorisation.

The Court held that this arrangement failed to ensure adequate and effective guarantees against abuse and violated the essence of the right to privacy, as enshrined in Article 8. In accordance with Eleni Kosta, this judgment may be regarded as one of the earliest judicial recognitions that technological infrastructures themselves can give rise to constitutional violations when they facilitate unaccountable data flows or entrench asymmetries of power.[48]

The implications of *Zakharov* extend well beyond the surveillance context. The judgment has been widely cited in debates about the constitutional limits of automated data processing, predictive policing, and AI-driven monitoring systems. Its reasoning implicitly anticipates the challenge of ensuring human oversight and accountability in environments where decisions are mediated by opaque algorithmic systems.

Ultimately, *Wieder and Guarnieri v United Kingdom* confirms the European Court's continuing struggle to articulate a constitutional grammar for the age of algorithmic power, even over any wiretapping conducted within their territory. [49]

Although these decisions were framed around State activity, their doctrinal principles are generative: private-sector infrastructures that operate at a surveillance scale and perform *de facto* public functions attract similar demands of transparency, proportionality and independent control when their operation implicates the rights protected by the Convention.

---

[47] Ibid 46. See Serge Gutwirth Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law* (Springer 2014); Michela Michetti, 'Surveillance and technological (r)evolution. Implications and repercussions on human rights' (2023) 5(2) Humanities and Rights Global Network Journal 274.
[48] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff 2013).
[49] Ibid 44.

The ECJ has also clarified core operational concepts that directly affect AI governance in two leading cases. In *Planet49* the Court insisted that consent must be a clear affirmative act and cannot be inferred through pre-ticked boxes or manipulative interface designs. This strict conception of consent limits the capacity of platform operators to rely on transactional or bundled consent as a legitimising device for opaque profiling practices.[50]

In *Peter Nowak v Data Protection Commissioner*,[51] the ECJ adopted a capacious understanding of 'personal data', ruling that seemingly mundane artefacts, such as examination scripts and examiner comments, can fall within the protective ambit when they relate to an identifiable natural person.

Together, these rulings expand the perimeter of legal protection in ways that undercut business models premised on anonymisation rhetoric or on the sale of derivative 'insights.

The law will treat many algorithmically generated or inferred outputs as falling within rights-protective regimes, thereby complicating attempts to treat predictive products as purely commercial, non-personal commodities. Beyond these supranational anchors, national courts across Europe and in common-law jurisdictions have begun to test the boundaries of algorithmic governance in concrete regulatory spaces.

Recently, the UK High Court delivered a highly anticipated judgment in *Getty Images v Stability AI*.[52] During the course of the proceedings, Getty Images withdrew its primary copyright claims, leaving the Court to address only the remaining secondary copyright infringement issues. The judgment also examined the trademark allegations, dismissing the claim under section 10(3) of the Trademarks Act 1994 and finding that any infringement under sections 10(1) and 10(2) in relation to early versions of the Stable Diffusion model was extremely limited. This case marks one of the first intellectual property disputes to reach trial against an AI developer, attracting considerable attention from both the legal community and the public. Getty initially filed a broad claim in January 2023, encompassing copyright, database rights, trademark infringement, and passing-off, directed at the Stable Diffusion model, its training data, and the images generated.

By the conclusion of the trial in June 2025, only two central issues remained. The first concerned whether the distribution of model weights for certain versions of Stable Diffusion via Hugging Face amounted to secondary copyright infringement. The second addressed whether certain outputs of Stable Diffusion, identified as bearing watermark-like features, infringed the Getty or 'iStock trademarks'.

The ruling thus clarifies the extent of liability for AI-generated content and provides a framework for assessing the responsibilities of AI developers regarding the reproduction and dissemination of protected material.

British jurisprudence has also engaged with the constitutional implications of automated decision-making through the landmark case *R (Bridges) v Chief Constable of South Wales Police*.[53] This case concerned the deployment of Live Facial Recognition (LFR) technology by the South Wales Police in public spaces, an

[50] Case C-673/17 [2019] ECLI:EU:C:2019:801. In a critical perspective, Klaus Wiedemann, 'The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing?' (2020) 51 International Review of Intellectual Property and Competition Law 543.
[51] Case C-434/16 [2017] ECLI:EU:C:2017:994.
[52] [2025] EWHC 2863 (Ch).
[53] [2020] EWCA Civ 1058.

innovation heralded as a means to enhance security and operational efficiency. The claimant, Edward Bridges, a civil liberties campaigner, challenged the lawfulness of this practice on the grounds that it violated his rights to privacy and data protection under Article 8 of the European Convention on Human Rights and the UK's Data Protection Act 2018, and that it was incompatible with the public sector equality duty established by section 149 of the Equality Act 2010.

The Court of Appeal overturned the initial High Court ruling that had found the use of LFR lawful, holding instead that the legal framework governing facial recognition lacked the 'clear and foreseeable' safeguards required under the European Convention. The Court reasoned that the deployment of LFR gave the police 'too broad a discretion' in deciding where to use the technology, whose images to include in the watchlist, and how to assess and mitigate potential bias in the system. The absence of detailed and transparent policies meant that the interference with privacy was not 'in accordance with the law' as demanded by Article 8 ECHR. The Court also recognised that the equality implications of facial recognition were inadequately assessed, particularly given the well-documented risk of algorithmic bias against ethnic minorities and women. Beyond its immediate outcome, *Bridges* represents a constitutional milestone in the governance of AI-based surveillance technologies.

The decision reaffirms that technological convenience cannot substitute for legal certainty and accountability. In the Court's view, the use of AI systems by public authorities must be subject to strict procedural and substantive safeguards that preserve the principles of proportionality, necessity, and non-discrimination. By requiring clear statutory and administrative guidance, the Court effectively placed constitutional boundaries around the deployment of machine intelligence in law enforcement, insisting that any such system must be embedded within a rights-compliant regulatory architecture.

Another example stand from the Italy's constitutional pushback against unrestrained automation is found in the judgment of the Consiglio di Stato, Section VI, dated 8 April 2019, No. 2270. This landmark case concerned the Ministry of Education's deployment of an algorithm to allocate teaching staff to positions nationwide. The automated system relied exclusively on digital criteria, producing assignments that were opaque, unpredictable, and effectively non-contestable by the teachers affected. Individuals had no meaningful opportunity to understand the logic underpinning their placement or to challenge the outcomes.

In response, the Consiglio di Stato annulled the administrative act, reasoning that the algorithmic opacity of the system infringed core constitutional protections, notably the principles enshrined in the Italian Constitution (Articles 3, equality; 24 right to defence and 97 efficiency, fairness, and impartiality of public administration). The decision underscores the Court's insistence that automated administrative processes remain subordinate to constitutional norms and that human oversight cannot be entirely supplanted by algorithmic determinations.

Similarly, the recently filed challenge against France's welfare-scoring regime provides a compelling illustration of how public-administration uses of AI are subject to rights-based scrutiny. In October 2024 a coalition of civil-society organisations, including 'La Quadrature du Net' and 'Amnesty International', lodged a complaint with the Conseil d'État, the highest administrative court in France, seeking to halt the use of a risk-scoring algorithm employed by the Caisse nationale des allocations familiales (CNAF). The system assigns scores to benefit recipients using socio-economic variables (including disability *status*, residency in disadvantaged neighbourhoods,

duration of rent and household composition) and flags individuals for investigation if their score crosses a predetermined threshold.

Critics argue, and the complaint asserts, that the system targets marginalised groups and thereby violates the rights to equality and non-discrimination under domestic and EU law, as well as the right to privacy guaranteed under Article 8 of the European Convention on Human Rights. Rather than a purely academic critique of technological architecture, the case confronts the reality of algorithmic decision-making within welfare distribution and deploys the language of rights and constitutional norms. It thereby helps to anchor the broader concept of 'artificial constitutionalism' in concrete administrative practice: if the State or its agencies outsource decision-making to algorithmic processes, the same constitutional values, transparency, contestability, non-discrimination, due process, that apply to human decision-makers must apply to their algorithmic equivalents.

In this respect the French case exemplifies several key dimensions of digital constitutionalism: first, the insistence that standard regulatory forms (data-protection rules, internal audits) may not be enough where automation produces structural risks to vulnerable populations; second, the recognition that claims for fairness and accountability must be embedded across the lifecycle of automated systems, from design and deployment to audit and redress; third, the emerging strategy of using courts to press for institutional responses to algorithmic governance rather than merely seeking technology-specific rules or soft-law guidelines.

Nevertheless, the case also exposes the limits of litigation as a transformative tool. The outcome remains pending, meaning its effect on future welfare-automation systems is speculative. Moreover, courts operating within administrative frameworks may lack the technical capacity or the institutional independence to fully scrutinise complex machine-learning systems, raising the risk that accountability claims become formal rather than substantive.

Consistent with the constitutional reasoning developed in Italy and France, the judgment of the District Court of The Hague in *NCJM and Others v State of the Netherlands* (SyRI) represents a landmark confrontation with automated welfare surveillance.[54] The SyRI system, developed by Dutch authorities, aggregated data from multiple public-sector databases to identify individuals deemed at risk of social benefit fraud. Plaintiffs, including civil-society organisations and affected individuals, challenged the system on grounds that it violated the right to privacy, equality, and due process.

The Court held that the system's opacity and the lack of meaningful avenues for individuals to contest algorithmic determinations rendered it incompatible with fundamental rights protections.

Key concerns included the automated profiling of vulnerable populations, the disproportionate burden imposed on those flagged by the system, and the absence of adequate safeguards or independent oversight. The ruling effectively suspended the use of SyRI, emphasizing that automated risk-assessment mechanisms in public administration cannot circumvent constitutional norms, even when designed to enhance efficiency or detect fraud.

Based on the foregoing analysis, whether the courts will seize the opportunity to operationalise artificial constitutionalism by reasserting the primacy of human rights

[54] C-09-550982-HA ZA 18-388 (2020)

over machine-enabled state functions remains an open question. This uncertainty, however, carries profound implications for the evolution of democratic governance in the AI era, as it underscores the delicate balance between technological innovation and constitutional accountability.

The trajectory of European jurisprudence suggests that courts are increasingly attentive to the risks posed by algorithmic opacity, automated decision-making, and the shifting *locus* of sovereignty.

The extent to which European courts embrace this responsibility will shape not only the legal contours of AI governance but also the broader normative landscape in which democratic principles are protected and reaffirmed amidst rapid technological change.

V. Final remarks

The technological transformation brought about by the advent of Artificial Intelligence has reshaped the entire world system as we knew it. This technological revolution therefore entails the need to redefine the fundamental categories through which reality itself is understood. In the midst of this Copernican shift, one fixed point remains the defence of the system of values upon which constitutional science is founded. Any transformation, even a revolutionary one, must not come at the expense of the ethical, moral, and legal achievements that humanity has secured. The defence of constitutional values remains a non-negotiable constant amid the technological upheaval of our time.

At a historical juncture in which even the idea of peace, once thought to be perpetual, at least in Europe, is being called into question, this reminder is far from superfluous. On the contrary, for the progress of humanity, just as it would make no sense to restrict technological development, which is by definition unstoppable, it is equally necessary to safeguard, reaffirm, and strengthen the fundamental principles without which progress would remain an end in itself.

This point acquires even greater relevance if we acknowledge that we are no longer dealing with an authority, namely, the State, capable of unilaterally regulating (and, by extension, controlling) the uses and effects of a given technology. The technology in question itself possesses the capacity to exercise its own form of authority over the States that depend on it for the performance of their functions.[55]

From this underlying logical standpoint, this contribution seeks to address the question of redesigning 'artificial constitutionalism' as a necessary step to rebalance the relationship between rights and individuals through the reaffirmation of values over authority.[56]

This assumption holds true regardless of the form authority takes, whether the traditional State authority as we once knew it, or a hybrid form composed of interconnections between public and private systems, in which the latter has come to own functions traditionally reserved for the former.[57]

Faced with this shifting of authority, without a shared sense of responsibility for the

[55] Sebastian Rosengrün, 'Why AI is a Threat to the Rule of Law' (2022) 1(10) Digital Society 1.
[56] As for the meaning assigned to individuals, the reference concerns the notion of "people" understood as legal subjects. In this respect, 'This concept evolved into law to describe the various roles that humans undertake in legal contexts – as debtors, creditors, property owners, plaintiffs, or defendants – ultimately representing the abstract ability to participate in any legal interaction', Claudio Novelli and others (3).
[57] On 'rights and powers in the digital age' considering that 'Non-state actors, private corporations and supranational governance institutions contribute to defining their rules and codes of conduct whose global reach overlaps with the traditional expression of national sovereign power', De Gregorio (27) 311.

axiological direction of AI development, regulation alone is destined to fail.

Further, the 'electronic body' of individuals deserves the same guarantees historically associated with corporeal integrity. Building on the trajectory from *habeas corpus* to *habeas data*, using the metaphor explored by Stefano Rodotà, the claim is not merely rhetorical and constitutes a substantive precondition for personal freedom in a data field society.

Further reflecting on the constitutional stakes, it is evident that the reduction of the person to an object of trade extends far beyond advertising. Credit scoring, fraud detection, and predictive policing operate through mechanisms that translate group-level correlations into determinations of individual fate.

When proxies are used in place of protected attributes, discrimination can be obscured behind technical categories that appear neutral while functioning as power multipliers. In this regard, the EU response, encompassing data protection, platform regulation, competition law, and AI governance, can be interpreted as a unified constitutional project aimed at re-embedding markets within the primacy of fundamental rights, yet it remains a project that is undeniably still largely unrealized.

Building upon the preceding discussion, it becomes apparent that, at least at a theoretical level, the foundations for anchoring technological development to the respect of constitutional values repeatedly invoked throughout this analysis are already established. These values, rooted in human dignity, equality, liberty, and democratic participation, form the normative compass that must guide the evolution of artificial intelligence and digital infrastructures.

Yet, the endurance of these principles cannot depend merely on rhetorical affirmation or declaratory commitments. It demands the formation of a critical mass of public institutions, regulatory bodies, civil society actors, and private entities capable of transforming constitutional ideals into concrete and enforceable norms within the technological sphere. From this vantage point, algorithmic decision-making must not simply coexist with constitutional law but must remain structurally subordinated to it in both design and application.

Preserving this normative hierarchy entails more than procedural compliance: it requires the creation of epistemically transparent systems whose operations can be understood, traced, and contested.

Mechanisms such as meaningful human oversight, systematic documentation of algorithmic reasoning, and the preservation of effective judicial review are indispensable elements of a constitutional architecture that aspires to embed human agency and accountability within the digital ecosystem. These safeguards ensure that technological efficiency serves democratic legitimacy rather than replacing it.

The state of the art is still far from this scenario. The AI Act, despite its ambitious scope, continues to rely on a regulatory logic that privileges procedural compliance over substantive guarantees. States, by embracing the rhetoric of technological sovereignty, claim to assert their authority over AI regulation and use, but this assertion risks becoming symbolic.

As AI systems gain the capacity for autonomous optimisation and self-regulation, modifying their own parameters to remain within formal legal constraints, the human oversight envisioned by the Act could become increasingly nominal. In effect, regulation may evolve into a meta-procedural framework in which systems appear compliant because they can simulate conformity with legal rules in real time.

In this broader constitutional landscape, the respect for fundamental values calls for a dynamic process of institutional adaptation. Such transformation presupposes a renewed constitutional imagination capable of integrating technological innovation into a rights-based order.

This task requires coordinated engagement among States, supranational organisations, and private corporations, each assuming responsibility for aligning technological development with the normative imperatives of constitutional democracy. The goal is not to arrest innovation, but to ensure that the transformative potential of artificial intelligence reinforces, rather than undermines, the moral and legal architecture that sustains human autonomy, dignity, and the rule of law.

Against this background, the persistent normative tension lies in reconciling the efficiencies promised by AI, such as enhanced service delivery, predictive analytics, and resource optimisation, with the constitutional duty to preserve human-centred, rights-compliant governance. This challenge becomes especially acute in contexts marked by algorithmic opacity, where decision pathways remain inaccessible even to those public authorities that deploy them. In such settings, reliance on risk-based approaches alone proves inadequate.

The legitimacy of AI-empowered decision-making requires not only robust *ex ante* safeguards but also comprehensive *ex post* remedies, including effective appeal mechanisms, independent oversight, and institutional capacities designed to guarantee transparency, accountability, and the continuing primacy of fundamental rights.

Through such an integrated framework can the constitutional order evolve in tandem with technological progress, ensuring that the human person remains at the centre of governance in the algorithmic age.

In summary, what this work has sought to argue is that it is necessary to reaffirm value-based constitutionalism as a means of constraining power, including the artificial one.