European Journal of Risk Regulation (2026), **17**, 357–373
doi:10.1017/err.2025.10079

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

The Transformation of European Risk Regulation: Managing Uncertainty and Powers in the Digital Age

Mª Verónica Vargas[1] and Giovanni De Gregorio[2]

[1]PhD candidate at the CEU International Doctoral School (CEINDO), Universitat Abat Oliba CEU, CEU Universities, Calle Bellesguard 30, 08022 Barcelona, Spain and [2]PLMJ Chair in Law and Technology, Católica Global School of Law, Universidade Católica Portuguesa, Lisbon, Portugal
*Corresponding author. E-mail: mvargasc@uao.es

Abstract

Risk regulation has increasingly expanded in European digital policy, yet it is diverging from its roots, especially the precautionary principle. Rather than traditionally focusing on scientific evidence and knowledge, the European approach to risk regulation has been increasingly based on constitutional values such as the protection of fundamental rights and democracy. This article seeks to unravel the logic that has led the Union to move from an approach to risk more based on science to a model which considers constitutional values as parameters to assess and mitigate risks. By focusing on European digital regulation, primarily the GDPR, the DSA and the AI Act, this work underlines how the constitutional rationale of this transformation comes as a response to the intangibility of risks resulting from digital technologies and to imbalances of information and knowledge coming from the concentration of private power in the digital ecosystem. The primary argument is that risk regulation in European digital policy does not seek to rationalise uncertainty through science but to govern epistemological uncertainty through the instruments of constitutionalism, with the goal of addressing the impact of digital technologies on fundamental rights and imbalances of power.

Keywords: accountability; constitutionalism; European Union; governance; powers; risk regulation

I. Introduction

Risk regulation has been expanding in European digital policy.[1] From the regulatory framework of personal data to content and artificial intelligence (AI), the European approach has primarily relied on risk assessment obligations and procedures focusing on mitigating risks to fundamental rights. Particularly, the framework of data protection, platform regulation, and artificial intelligence underlines this focus on constitutional rights, as seen in the Recitals of the General Data Protection Regulation (GDPR),[2] the Digital

[1] Vagelis Papakonstantinou and Paul de Hert, *The Regulation of Digital Technologies in the EU: Actification, GDPR Mimesis and EU Law Brutality at Play* (Routledge 2024).

[2] 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.

Services Act (DSA),[3] and the Artificial Intelligence Act (AI Act).[4] The main characteristic bringing together these regulations is the focus on European constitutional values anchored in democracy and the rule of law, as in Article 2 TUE, which serve as the core parameter for assessing and mitigating risks.

However, the approach oriented to constitutional values has not always characterised European risk regulation. Instead, risk regulation in Europe has been more intricately connected to science and precaution as a principle.[5] Ever since the last century, the rationalisation of risk has been the answer for the unknown landscape that transnational and technological threats pose to social goods. This process was grounded in the quantitative cost-benefit analysis and reinforced by the precautionary principle.[6] This principle has indeed played a foundational role in modulating European policies within many different fields, from environmental law to food safety.[7] Rooted in risk assessments of potential harm based on a mix of scientific and statistical data, this principle has been serving as a guiding framework for policy-makers, limiting the uncertainty by trying to rationalise risk.

European digital policy instead seems to follow another path. Rather than being directly connected to ex-ante parameters or scientific risk assessment and knowledge, the European approach to risk regulation in digital policy considers risk not in terms of scientific uncertainty, but rather in terms of the impact on constitutional values, particularly fundamental rights, coming from digital technologies and the imbalance of powers between public and private actors. The lack of a clear precautionary framework in digital regulation is particularly evident when examining landmark legislative instruments in different areas. While elements of the precautionary principle can be identified in the AI Act, as in the case of the prohibited practises,[8] and the technical threshold for generative AI models with systemic risk,[9] the overall regulatory approach to risk regulation in European digital policy remains distinct from other fields, particularly where the precautionary principle served as a guide.

This shift of view highlights a fundamental divergence in how risk is conceptualised and regulated across different domains. Digital policy operates in an environment of uncertainty, where risks are often speculative and difficult to quantify,[10] as well as left to the assessment made by the regulatees such as private actors. The difference indeed can be attributed to the inherent challenges in quantifying and measuring digital risks, particularly in areas such as personal data processing and the dissemination of illegal content. Issues such as algorithmic bias, misinformation, privacy violations, and

[3] 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.

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[5] Maria Weimer, *Risk Regulation in the Internal Market: Lessons from Agricultural Biotechnology* (Oxford University Press 2019).

[6] Maria Weimer and Luisa Marin, "The Role of Law in Managing the Tension between Risk and Innovation: Introduction to the Special Issue on Regulating New and Emerging Technologies" (2016) 7 *European Journal of Risk Regulation* 469–74 <http://doi.org/10.1017/S1867299X00006012>.

[7] Kristel De Smedt and Ellen Vos, "The Application of the Precautionary Principle in the EU" in Simone Arnaldi and others (eds), *The Responsibility of Science* (Springer 2022) p 163.

[8] AI Act, Art. 5.

[9] Ibid, Arts. 28b(2) and Annex VIII.

[10] Ljupcho Grozdanovski and Jasper De Cooman, "Forget the Facts, Apply the Law: Artificial Intelligence, Fact-Finding and the European Union" (2023) *49* Rutgers Computer and Technology Law Journal 296.

cybersecurity threats are difficult to measure using traditional scientific methods.[11] Unlike environmental hazards or food safety risks, which can be assessed through empirical testing and scientific methodologies, the impact of digital risks is often diffuse, context-dependent, and difficult to predict.[12] In this case, digital policy addresses risks that are often not yet fully understood, leading to regulatory frameworks that prioritise governance mechanisms over science. Likewise, the concept of risk in digital policy is often linked to broader societal and ethical considerations rather than direct scientific evaluation. In the case of AI regulation, for example, concerns about bias, discrimination, and autonomy are central to regulatory discussions,[13] but they do not lend themselves to the same types of analysis used in science-based knowledge. Instead, they require normative judgements about fairness, accountability and fundamental rights. This has led to the development of regulatory mechanisms, including impact assessments and ethical guidelines,[14] which aim to manage risks through governance rather than through the scientific identification and mitigation of hazards.

This mechanism, which has acquired central relevance in European digital policy, reflects a broader shift in risk regulation driven by the growing imbalance of power between public and private actors as shaped by the consolidation of information capitalism.[15] The transfer of regulatory responsibility directly to private actors leads to increase areas of private governance on the effective protection of fundamental rights and democratic values, as underlined by the GDPR, where the scope of obligations is primarily shaped by the data controllers based on the principle of accountability. As public authorities increasingly depend on market actors to implement and enforce regulatory goals, a significant share of regulatory responsibility is transferred to these private actors, who are thereby tasked with ensuring the effective protection of fundamental rights and democratic values through practices of risk assessment and mitigation.

Within this framework, this paper examines how risk regulation in European digital policy follows a different logic compared to the approaches characterising the precautionary principle. What has changed is not the reliance on risk regulation, but the approach to risk whose focus is on constitutional values such as the protection of fundamental rights and democratic values. Unlike the precautionary principle, which tends to be more centred on empirical risk assessment and scientific evidence to rationalise the imminent or possible material hazards and ultimately drive regulation, here, the parameter of risk assessment shifts from hard science to social science, and particularly to constitutionalism. The risk-based approach implemented in European digital policy looks at constitutionalism as science, so making principles such as proportionality and accountability the core of the system, replacing empirical data as the basis for risk assessment. This process has resulted in a regulatory framework where the

[11] Claudia Quelle, "Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach" (2018) 9 European Journal of Risk Regulation 502.

[12] Gianclaudio Malgieri and Cristiana Santos, "Assessing the (Severity of) Impacts on Fundamental Rights" (2025) 56 Computer Law & Security Review 106113.

[13] Claudio Novelli and others, "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity" (2024) *Computer Law & Security Review*, https://arxiv.org/pdf/2401.07348 (accessed 12 March 2025); Janneke Gerards and Raphaële Xenidis, *Algorithmic Discrimination in Europe: Challenges and Opportunities for Gender Equality and Non-Discrimination Law* (European Commission, Directorate-General for Justice and Consumers, Publications Office 2021); Matthew U Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" (2016) 29 Harvard Journal of Law & Technology 353.

[14] AI Act, Arts. 9 and 29.

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

assessment and mitigation of risks are mediated by legal and institutional considerations rather than scientific principles.

Furthermore, the paper argues that this transformation is part of the European constitutional reactions to the challenges posed by digital technologies to fundamental rights and democratic values and a way to address the imbalance of power between public and private actors in the digital age. This shift has been deeply influenced by the predominance of private actors, particularly large technology firms that dominate the digital ecosystem. The significant control over data, algorithms and digital infrastructures makes them both sources of potential risk and key entities and collaborators for risk mitigation. Rather than adopting a purely science-driven approach, the European approach to risk regulation in digital policy considers constitutional values as the parameter, thus leading risk regulation to become a way for public actors to limit the power imbalance between public and private actors while balancing fundamental rights, democracy and market dynamics shaping digital ecosystems.

This paper first explores the evolution of European risk regulation, particularly looking at the precautionary principle. Second, it analyses the characteristics of risk regulation in European digital policy, examining legislative frameworks such as the GDPR and the DSA, and the AI Act. Third, the paper examines how the evolving regulatory landscape of risk regulation oriented towards constitutional values reflects the broader imbalance between public and private actors in the digital age.

II. The evolution of European risk regulation and precaution

The rising threats of modern societies brought a new focus on understanding and rationalising risks. Risk rationalisation rests on the premise that probability, and, by extension, quantification make hazards amenable to comparable calculation and thereby to "objectively" defensible decision-making.[16] On this foundation, quantitative risk assessment and cost–benefit analysis have been constructed as tools that transpose the multiplicity of technological impacts into comparable metrics, allegedly providing technical support for regulatory choices.[17]

Yet, by homogenising environmental, health, economic and ethical dimensions, quantitative risk assessment excludes salient qualitative effects and proves inadequate under conditions of uncertainty, where outcomes are known but their probabilities are not, or ignorance, where even the universe of outcomes cannot be delimited.[18] In such contexts, regulatory science forfeits its supposed neutrality. Its judgments become entwined with political considerations and social values, blurring the traditional divide between risk assessment (facts) and risk management (values).[19]

Precisely because a stable epistemic foundation is unattainable in these circumstances, the precautionary principle emerges as a normative counterweight. Its logic is not to quantify the unquantifiable, but to acknowledge that where causal relations are unknown or incalculable and scope for surprise is wide, public decisions cannot rely solely on quantitative risk assessment techniques. Far from repudiating science, precaution demands a more pluralistic and candid approach to its use. Still grounded in empirical inquiry into the relevant observable reality, yet conscious of its limits and

[16] Jonathan B Wiener et al., *Reality of Precaution. Comparing Risk Regulation in the United States and Europe* (Taylor & Francis 2010). See also Bernstein, *Against the Gods* (n 9); Ian Hacking, *The Emergence of Probability* (Cambridge University Press 1975).

[17] Brian Wynne, "Uncertainty and Environmental Learning" (1992) 2 *Global Environmental Change* 111, 113.

[18] Ibid, 113.

[19] Jenny Steele, *Risks and Legal Theory* (Hart Publishing 2004) 6.

open to extra-scientific forms of knowledge.[20] Thus, whereas risk rationalisation seeks legitimacy through probabilistic calculation and the promise of objectivity, the precautionary approach shifts the centre of gravity to the governance of uncertainty, privileging prudence, the allocation of the burden of proof, and open political deliberation as means to safeguard the public interest when the "facts" are unstable or incomplete.

Historically, the precautionary principle has served as a tool for policymakers to manage risks predominantly in health, environmental and safety-related domains.[21] Its implementation has typically involved public policies aimed at limiting economic activities, such as restricting or banning products from circulation.[22]Risk takes shape through the interplay of diverse realities in a context of uncertainty.[23]Any account of risk is inseparable from how one conceives the state–society nexus, particularly as that nexus adapts within technology-driven knowledge societies.[24] At the same time, risk plays several distinct roles in the regulatory sphere: it can be the very focus of regulation, supply the rationale for introducing rules, shape the architecture and processes of regulatory bodies, and underpin the mechanisms through which regulators are held accountable.[25]

An example of this is financial market regulation, where risk is understood as the probability or possibility of events negatively affecting the strategic or economic objectives of financial institutions, particularly through losses, solvency deterioration, or reputational damage. As financial markets grew more complex and globally interconnected during the second half of the twentieth century, risk management became increasingly sophisticated, leading to a segmentation of risks into distinct categories such as credit risk, market risk, operational risk and liquidity risk,[26] as underlined by recent examples of the purported adoption of the precautionary principle in financial spheres as well as energy transition.[27]

[20] Andrew Stirling, *On Science and Precaution in the Management of Technological Risk: Volume I—A Synthesis Report of Case Studies* (Institute for Prospective Technological Studies 1999) p 16.

[21] Kristel De Smedt and Ellen Vos (n 7).

[22] Jale Tosun, "How the EU Handles Uncertain Risks: Understanding the Role of the Precautionary Principle" (2013) 20 Journal of European Public Policy.

[23] For the purpose of this paper, we consider scientific uncertainty a subset of epistemic uncertainty. Consistent with regulatory governance scholarship, risk is used here as a device to rationalise decision-making under uncertainty, distinct from hazard (source of harm) and from uncertainty itself. See Christopher Hood, Henry Rothstein and Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford University Press 2001); Michael Power, *The Risk Management of Everything: Rethinking the Politics of Uncertainty* (Demos 2004); Michael Power, *Organized Uncertainty: Designing a World of Risk Management* (Oxford University Press 2007); Andrew Stirling, "Risk, Precaution and Science: Towards a More Constructive Policy Debate" (2007) 8 EMBO Reports 309–315.

[24] Karl-Heinz Ladeur, *Das Umweltrecht der Wissensgesellschaft: Von der Gefahrenabwehr zum Risikomanagement* (Schriften zur Rechtstheorie 167, Duncker & Humblot 1995). In Maria Weimer, *Risk Regulation in the Internal Market.* (24).

[25] Julia Black, "The Role of Risk in Regulatory Processes" in Robert Baldwin, Martin Cave and Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford University Press 2010) p 302.

[26] Christopher Carrigan and Cary Coglianese, "*Capturing Regulatory Reality: Stigler's The Theory of Economic Regulation*" (University of Pennsylvania, Institute for Law & Economics Research Paper No 16-15, 4 July 2016) https://ssrn.com/abstract=2805153 (accessed 28 April 2025).

[27] Kukuh Komandoko, "The Role of the Precautionary Principle in Mitigating Financial and Banking Crisis" (2020) 5 International Journal of Innovative Science and Research Technology 2456. Hugues Chenet et al., *Developing a Precautionary Approach to Financial Policy – From Climate to Biodiversity: The INSPIRE Sustainable Central Banking Toolbox, Policy Briefing Paper 02* (University College London and New Economics Foundation April 2022). OECD, *Understanding and Applying the Precautionary Principle in the Energy Transition* (OECD Publishing 2023).

The conceptualisation of the precautionary principle has then been shared upon other spheres of regulation and policy making with the aim of coping with the evolving reality or at least having tools to decipher it. Therefore, this principle evolved into an intellectual and practical guide to respond to natural disasters and imminent environmental hazards in the twentieth century.[28] Prudence thus became a principle guiding decision-making when the contingent circumstances that surround a situation are uncertain, involving the evaluation of available knowledge to avoid potential harm to the environment, people integrity and other legally protected interests, even in the absence of complete information about the risks involved.

The first legal expression of the precautionary principle appeared in national legal systems,[29] such as those of Germany and Sweden.[30] German environmental policy known as *Vorsorge* (prudence and foresight), and Swedish antipollution legal standards already in 1981 established legitimacy to act before all certainty about a concrete situation was accomplished,[31] exemplify this evolution. Also, Mary Stevens explains that this approach gained prominence in the international arena, spreading to environmental law, particularly through the North Sea protection conferences. Germany introduced this already settled domestic approach to shed light on the discrepancy of whether to wait for proof of harmful effects before acting. Already in the second conference, the terminology of "precautionary approach" was adopted.[32]

By 1990, the principle was explicitly recognised in supranational fora such as the Bergen Declaration,[33] and the OSPAR Convention,[34] where its role in addressing scientific uncertainty was emphasised, allowing preventive actions even in the absence of conclusive evidence. In a broader international context, the principle was formally enshrined at the international level in the 1992 Rio Declaration, adopted at the United Nations Conference on Environment and Development. Its goal was to ensure that scientific uncertainty would no longer be an excuse for inaction when serious or irreversible threats of harm are at stake.[35] Therefore, this principle, which emerged from international environmental

[28] Although the precautionary principle was systematised in the last century, some traces can be found in the origin to the ancient Greece, when Aristotle referred to prudence as "practical wisdom" (*phronesis*), different than the theoretical wisdom (*sophia*). Therefore, prudence is understood in its classical sense as the "ability to discern the most appropriate course of action". Unlike philosophy, prudence addresses contingent matters, which cannot be systematically resolved in advance and require specific responses for each unique situation. See Roberto Andorno, "The Precautionary Principle, A New Legal Standard for a Technological Age" (2004) 1 Journal of International Biotechnology Law 11.

[29] See Sonja Boehmer-Christiansen, "The Precautionary Principle in Germany - Enabling Government" in Tim O'Riordan and James Cameron (eds), *Interpreting the Precautionary Principle* (Earthscan 1994) p 31.

[30] Ragnar Löfstedt, "The Swing of the Regulatory Pendulum in Europe: From Precautionary Principle to (Regulatory) Impact Analysis" (2004) 28 Journal of Risk and Uncertainty 237–60.

[31] Staffan Westerlund, "Legal Antipollution Standards in Sweden" (1981) 25 Scandinavian Studies in Law 223, 231.

[32] Mary Stevens, "The Precautionary Principle in the International Arena" (2002) *Sustainable Development Law and Policy* Spring/Summer, 13–15.

[33] Bergen Declaration, Fifth International Conference on the Protection of the North Sea (Bergen, 2002) https://www.ospar.org/site/assets/files/1239/5nsc-2002_bergen_declaration_english.pdf (accessed 28 April 2025).

[34] Convention for the Protection of the Marine Environment of the North-East Atlantic (OSPAR Convention) (1992). In relation to the protection of the marine environment. Art. 2 of the OSPAR Convention establishes the precautionary principle, allowing preventive measures to be taken in the face of reasonable concerns that substances or energy introduced into the marine environment may cause harm, even without conclusive evidence of a causal relationship.

[35] Rio Declaration on Environment and Development, Report of the United Nations Conference on Environment and Development (Rio de Janeiro, 3–14 June 1992) UN Doc A/CONF.151/26 (Vol I): "In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation."

protection legislation,[36] has since extended to various areas related to safety, such as human, animal and plant health.[37]

Likewise, the precautionary principle also entered the EU legal order around that time. Besides, every step in the evolution of EU regulation was supposed to be a step forward for environmental policy, making sustainable development a core standard for the conclusion of supranational and national agreements.[38] The precautionary principle has increasingly become a general principle of law,[39] and a guiding framework for situations where political actions were not based on fully known or "knowable" information,[40] particularly when decision-making involved scientific uncertainty about the potential risks of harmful events. To unify the criteria for its application, the European Commission approved the Communication on the Precautionary Principle in 2000.[41] This document outlined the conditions under which the principle could be invoked:

> In those specific circumstances where scientific evidence is insufficient, inconclusive or uncertain and there are indications through preliminary objective scientific evaluation that there are reasonable grounds for concern that the potentially dangerous effects on the environmental, human, animal or plant health may be inconsistent with the high level of protection chosen for the Community.[42]

Moreover, the Communication draws a distinction between the enabling situation (scientific uncertainty about a potential harm), the studies corroborating the intuition of potential harm, and the characteristics of the precautionary measures. With regard to the enabling situation, the Commission understands that policy decisions to act or not to act will be made on the basis of the triggers for recourse to the precautionary principles,[43] particularly the identification of potentially negative effects, the performance of a scientific assessment, and, finally, the existence of scientific uncertainty.[44] The principle cannot be invoked solely on intuition, but it requires a comprehensive analysis of the specific risk to determine scientific uncertainty.[45]

Furthermore, the Commission identified four components for risk evaluation: hazard identification, hazard characterisation, exposure appraisal, and risk characterisation. Each of these steps, when incomplete, contributes to the overall level of uncertainty and

[36] Ibid, 22

[37] Alberto Alemanno, "*The Shaping of the Precautionary Principle by European Courts: From Scientific Uncertainty to Legal Certainty*" (Bocconi Legal Studies Research Paper 2007); Johan Zander, *The Application of the Precautionary Principle in Practice: Comparative Dimensions* (Cambridge University Press 2010).

[38] Kristel De Smedt and Ellen Vos (7).

[39] Regarding debate on the nature of the principle as general principle or approach see Jacqueline Peel, "Precaution–A Matter of Principle, Approach or Process?" (2004) 5 Melbourne Journal of International Law 483–501; Johan Zander, *The Application of the Precautionary Principle in Practice: Comparative Dimensions* (Cambridge University Press 2010); Joanne Scott, *Legal Aspects of the Precautionary Principle: A British Academy Brexit Briefing* (British Academy 2019).

[40] Natalie Eckley and Henrik Selin, "All Talk, Little Action: Precaution and Its Effects on European Chemicals Regulation" (2004) 11 Journal of European Public Policy 78–105.

[41] Commission Communication on the Precautionary Principle [2000] OJ C200/1.

[42] Ibid, 2.

[43] Ibid, 13.

[44] For the purpose of this paper, scientific uncertainty is considered as the inability to reach a scientific consensus or the lack of full available information, as referred in the Communication from the Commission on the precautionary principle, 16.

[45] Terje Aven, "A Risk and Safety Science Perspective on the Precautionary Principle" (2023) 165 *Safety Science* 106211. A risk and safety science perspective on the precautionary principle. He explains that uncertainties must be scientific in order to properly talk about the performance of precautionary principle instead of pure risk analysis.

influences the foundation for protective actions. Once the scientific evaluation is as complete as possible,[46] and the decision is made by assessing the consequences of action, and also of inaction, the precautionary measure must meet the following requirements.[47] First of all, the measures taken by decision-makers should be proportional to the chosen level of protection in that matter. Secondly, the application of the principle cannot be discriminatory. In third place, despite the lack of information, measures should be consistent with the others already adopted in similar circumstances or using similar approaches. The fourth requirement presupposes examination of the benefits and costs of action and lack of action, acknowledging the economic evaluation but taking into account other methods, such as those concerning efficacy and the socio-economic impact. The fifth component is related to the provisional nature of the principle as it entails that measures should be subject to review in the light of new scientific data in order to maintain or adjust the previous actions. Finally, another characteristic of the precautionary principle applied to real policies is the shift in the burden of proof.

All the above depict the Commission's effort to systematise this principle and to require exhaustiveness in risk assessment, to the extent possible, in order to avoid justifying arbitrary decisions under the pretext of the precautionary principle. This principle has been a key component of European legal and regulatory frameworks, with courts and policymakers responsible for defining its scope and application for almost half a century. Recent examples of its application include the 2024 regulation on the environmental performance of flights,[48] and the 2025–2030 Sustainable Fisheries Partnership Agreement,[49] illustrating the principle's continued relevance in European policy. However, this approach has raised questions about its impact on innovation and legal certainty,[50] also leading to inconsistencies in the EU's judicial application of the principle,[51] particularly regarding the degree of uncertainty required, the justification for its invocation, and the measures taken. At the same time, one cannot forget that the precautionary principle serves as a performative tool, particularly in science-based situations that rely on context-specific actions by policymakers.[52]

Regulation based on the precautionary principle often exhibits a hybrid nature, combining command-and-control mechanisms with more flexible instruments. On the one

[46] Commission Communication on the Precautionary Principle (n 50), 15.

[47] Ibid, 17–21.

[48] Commission Implementing Regulation (EU) C/2024/8795 final establishing detailed provisions for the voluntary environmental labelling system for estimating the environmental performance of flights, in accordance with Article 14 of Regulation (EU) 2023/2405 of the European Parliament and of the Council (Flight Emissions Label) (European Commission, 18 December 2024).

[49] Implementation Protocol of the Sustainable Fisheries Partnership Agreement between the European Union, the Government of Greenland and the Government of Denmark (2025–2030) ST/14781/2024/INIT (12 December 2024).

[50] Cass R Sunstein, *Laws of Fear: Beyond the Precautionary Principle* (Cambridge University Press 2009); Johan Zander, *The Application of the Precautionary Principle in Practice: Comparative Dimensions* (Cambridge University Press 2010); David Gee, "More or Less Precaution" in European Environment Agency (ed), *Late Lessons from Early Warnings II: Science, Precaution, Innovation* (EEA Report No 1/2013, 2013) 643; Ragnar Löfstedt, "The Precautionary Principle in the EU: Why a Formal Review Is Long Overdue" (2014) 16 *Risk Management* 143–5; Daniel Castro and Michael McLaughlin, *Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence* (Information Technology and Innovation Foundation 2019) https://itif.org/publications/2019/02/04/dont-put-artificial-barriers-artificial-intelligence-out-fear-new-report/ (accessed 28 April 2025).

[51] Kimberly Garnett and David KJ Parsons, "Multi-Case Review of the Application of the Precautionary Principle in European Union Law and Case Law" (2017) 37 *Risk Analysis* 502; Alemanno (n 46).

[52] Mark Geistfeld, "Implementing the Precautionary Principle" (New York University School of Law, NYU Law and Economics Research Paper No 00-004, 2000) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=289146 (accessed 28 April 2025).

hand, some environmental regulations impose clear obligations of result that reflect a strict regulatory approach. For example, Directive 2008/50/EC on ambient air quality and cleaner air for Europe sets binding limit values for pollutants such as nitrogen dioxide (NO_2) and particulate matter,[53] leaving no room for discretion to Member States in certain cases.[54] This represents a paradigmatic case of a mandatory outcome obligation. On the other hand, the precautionary principle is also operationalised through procedural tools such as Environmental Impact Assessments (EIAs), which embody a more open-ended, risk-assessment logic. Directive 2011/92/EU (as amended by Directive 2014/52/EU) requires the identification, description and evaluation of potential environmental effects of certain public and private projects prior to approval.[55] However, it only refers to lists of broad environmental factors to be considered, such as biodiversity, soil, water and human health, but does not prescribe specific outcomes.[56] Instead, it facilitates informed decision-making under uncertainty, aligning with the core logic of precaution.

This orientation to precaution has not found space in digital policy. Although the risks associated with digital technologies are acknowledged and have been at the basis of the adoption of new legal instruments, the precautionary principle is not formally invoked in digital policies implemented by the European Union in the last decade. The GDPR or the DSA refers to risk regulation and assessment, but they do not follow the same approach characterising policies and legislation based on the precautionary principle. Just as the precautionary principle offered answers for a long list of subjects such as health, food safety, industrial management, chemicals, pharmaceuticals, nuclear power plants and medical devices,[57] it does not offer the same guidance for countering the risks brought about by the digital age, even though it raises concerns about significant damage.

As underlined in the next section, risk regulation in European digital policy does not follow the same logic as the precautionary principle. The approach oriented to fundamental rights and democratic values in digital policy primarily leads to looking at risk assessment with a different focus, moving from scientific evidence to a constitutional-based approach.

III. The emancipation of European digital regulation

Risk regulation has been an instrument to address the challenges of a risk society.[58] However, the approach to risk has undergone an evolution within the framework of European digital policy. The risk regulatory approach analysed before diverges substantially from the approach applied to digital policies and regulation which not only consider risks but also are "risk-based," thus reflecting the transformation of normative paradigms in response to the challenges of the digital age.

Risk regulation and a risk-based approach to regulation do not necessarily overlap as concepts. The former looks at risk as the direct object of regulation, with acceptability thresholds and control measures defined in the instrument itself, while the latter considers risk as an assessment and prioritisation criterion that guides compliance and enforcement within an existing framework. In Black's[59] account, risk-based approaches

[53] Directive 2008/50/EC of the European Parliament and of the Council of 21 May 2008 on ambient air quality and cleaner air for Europe.

[54] Ibid, Art. 13.

[55] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment.

[56] Ibid, Art 3.

[57] Tosun (n 31).

[58] Ulrich Beck, *Risk Society: Towards a New Modernity* (Sage 1992).

[59] Julia Black, "The Emergence of Risk-Based Regulation and the New Public Risk Management in the UK" [2005] Public Law 512, 513.

structure decision processes (e.g., tailoring obligations to operator risk profiles, managing agency and compliance risks), but they do not, by themselves, settle what counts as an acceptable risk. Put differently, risk regulation is substantive, determining the substantive content of what is to be controlled, while risk-based regulation is methodological and organisational, shaping not the content but the way to address risks.

In the context of digital regulation, the European regulatory approach defines a mix between an attempt to regulate risk and a risk-based approach which acquires not only a political but also an eminently constitutional dimension, since the measures adopted are aimed at preventing negative effects for fundamental rights and democracy. As Grozdanovski points out, referring to the AI Act,[60] but equally applicable to the GDPR and the DSA, the definition of risk in this sphere is oriented not only towards physical integrity but, above all, towards safeguarding essential liberties. A new model therefore emerges, characterised by three intertwined shifts: who decides, how risk is calculated, and what regulatory outcomes follow.

1. The regulators: from public regulators to private regulatees

In the traditional approach to risk regulation, public authorities, assisted by scientific experts, were responsible for both the evaluation and the management of risk. Two important milestones were risk evaluation (facts) and risk management (values).[61] Scientists would be responsible for evaluating the piece of reality they had to decipher and ideally submit their neutral findings to decision makers to cautiously manage that information and provide an outcome or policy to the benefit of society.[62] Hesselink affirmed that this model resulted in two agents: the epistemic authority and the governance authority. While there is controversy over whether they are perfectly separated and the output of the first one is delivered totally neutral,[63] Hesselink explains that they obtained legitimation from different resources. Scientific findings earn credibility through rigorous methods and peer review, whereas political authority relies on democratic oversight and legal accountability for its legitimacy.[64] Therefore, the genuine answer to the question posed before regarding milestones or elements added to make digital risk regulation so different relies not on the steps to process risk but on the agents that have the power to do so.

Yet, in the digital sphere, the locus of decision-making migrates decisively toward private actors. When looking directly into European digital regulations, there can be found subjective obligations of protection depending on the risk posed to fundamental rights. For example, the GDPR generally introduces the principle of accountability, *de facto* delegating data controllers the responsibility to conduct a risk assessment.[65] One example is the obligation to conduct a data protection impact assessment to measure risks in relation to the processing of personal data. Indeed, when the processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.[66]

[60] Grozdanovski and De Cooman (n 11), 296.

[61] Steele, *Risks and Legal Theory*, 6.

[62] Sheila Jasanoff, "The Songlines of Risk" (1999) 8 *Environmental Values* 135, 141.

[63] See for the counterargument of this traditional model: van Asselt and Vos, "The Precautionary Principle and the Uncertainty Paradox" (n 57) 313.

[64] Martijn W Hesselink, "A European Legal Method? On European Private Law and Scientific Method" (2009) 15 European Law Journal 20. In Maria Weimer, *Risk Regulation* (43).

[65] GDPR, Art. 5.

[66] Ibid, Art. 35.

Meanwhile, the DSA requires providers of intermediary services to act in a diligent, objective and proportionate manner, taking into account the fundamental rights of the recipients of the service, as enshrined in the Charter.[67] Likewise, VLOPs should diligently identify, analyse and assess systemic risks arising from the design, functioning, or use of their services. These assessments must be carried out at least once a year or prior to the deployment of functionalities likely to have a critical impact.[68] The DSA mandates that such assessments focus on risks such as the dissemination of illegal content, negative effects on fundamental rights, including privacy, data protection, freedom of expression, non-discrimination and the rights of the child, as well as on democratic processes, public security, public health and individuals' physical and mental well-being.

With regard to the AI Act, it establishes different risk assessments applying to the providers of high-risk AI systems and deployers. For instance, the obligation to conduct a Fundamental Rights Impact Assessment prior to deploying high-risk AI systems,[69] particularly when used in sensitive areas such as justice, migration, democratic processes, or in decisions that significantly affect individuals. This assessment aims to identify the specific risks that the use of the system may pose to individual rights and freedoms, and the measures envisaged to prevent or mitigate those risks.

The reallocation of responsibility is not merely administrative, but it entails a reconfiguration of the relationship between public and private actors in the governance and control of technology. While the delegation of regulatory functions to private actors is not unique to the digital domain, the structure of delegation and oversight in EU digital regulation presents distinctive features. In other areas of risk regulation such as food safety and pharmaceuticals, private actors generate essential data and conduct trials, yet centralised public agencies such as the European Food Safety Authority or the European Medicines Agency retain decisive authority through *ex ante* approval processes, mandatory data disclosure, and public monitoring. By contrast, digital regulation relies predominantly on accountability and compliance obligations, where risk assessments and transparency reports are largely defined by the regulated entities themselves.

This system represents a different model of risk regulation compared to other areas where regulators have maintained more control. For instance, to ensure safety in the pharmaceutical area, public actors have adopted a paternalistic posture, presuming serious health risks and therefore concentrating power on the market. Meanwhile, in the digital realm, public actors have relied on private actors' capacity for self-regulation, with public intervention typically occurring only when harm or non-compliance arises. The lack of a central authority combined with the opacity of algorithms, trade secrecy protections and the unprecedented scale of concentrated private power, generates a much sharper informational asymmetry between regulators and firms. Thus, unlike the pharmaceutical or food sectors, where public oversight can independently validate private inputs, digital regulation places regulators in a structurally reactive position, dependent on the cooperation and disclosures of dominant platforms.

Unlike the classical decision-making model, where regulators occupied centre stage, exercising authority buttressed by expert scientific assessments, in the digital-risk arena, technical authority now resides with private entities, as they alone command the underlying datasets and possess privileged knowledge of their systems' internal operation.

[67] Digital Services Act, Art. 12(2).
[68] Ibid, Arts. 34(1)–(2).
[69] AI Act, Art. 27.

2. The risk calculation: from quantifiable hazards to intangible harms

The European approach to risk regulation in digital policy is also based on a different risk calculation paradigm. While risk has been mostly treated as an empirical and quantifiable prospect of tangible harm, e.g., pollutants are measured in micrograms per cubic metre, nuclear failures in millisieverts, anchored to legal thresholds,[70] digital risk, by contrast, is intangible and weakly measurable. Data processing, algorithmic bias, and information disorders lack stable metrics comparable to parts-per-million or exposure doses. Measurability becomes the decisive fracture line, for instance, between environmental and digital risk regimes,[71] where assessments rely less on science and more on constitutional reasoning about rights and democracy. This epistemic indeterminacy legitimises a plural and qualitative appraisal in which legal, ethical and socio-technical perspectives weigh as heavily as statistical models.

Digital risks in European digital regulation are indeed primarily connected to interference with fundamental rights and democracy. While epistemic uncertainty is present across domains, the European approach is marked by high ambiguity such as reasonable disagreement about values and metrics, e.g., "harm" to fundamental rights, and indeterminacy of outcomes emerging from complex socio-technical interactions. More specifically, regulations based on the precautionary principle have historically centred uncertainty around hazard identification and exposure–dose–response relationships, with comparatively greater tractability once measurement regimes stabilise. By contrast, digital risk assessment faces uncertainty, which does not only come from technological opacity but from assessments based on concepts which are connected to social sciences, and, particularly, constitutionalism.

Risk regulation, as inspired by the precautionary principle, has considered risks that, although uncertain, are connected to a physical and quantifiable reality. In contrast, in European digital regulation, the system of governance focuses on the integration of public and private actors concerning a technology whose full beneficial or threatening potential is not only unknown but also based on constitutional parameters which are different than scientific concepts. Whereas in the former, scientific uncertainty is subjected first to processes of evaluation and quantification through empirical data, meaning an assessment conducted by scientists. In the latter, the risks derived from digital technologies, that is, from data processing, online services, or AI, are speculative and often result from social dynamics, without a thorough scientific assessment carried out, difficult to measure, and often left to the assessment of private actors. The sustained absence of a systematic method to quantitatively delimit digital risks contrasts with the methodology of traditional scientific evaluation,[72] thus forcing regulators to deal with epistemological uncertainty in digital policies, rather than basing regulation on neutral scientific assessment of uncertainty.

The evolution of risk regulation in digital policies reflects a paradigmatic transformation that departs from the scientific and measurable approach of classic European risk regulation to embrace risk management based on constitutional values, reflecting the handling of uncertainty and the adaptation to new power dynamics in digital society. In policies inspired by the precautionary principle, risk has been primarily conceived in terms of an empirical and quantifiable assessment of potential harms and

[70] Council Directive 2008/50/EC of 21 May 2008 on ambient air quality and cleaner air for Europe [2008] OJ L152/1.

[71] Grozdanovski and De Cooman (n 11), 296.

[72] Regarding efforts to quantify digital risks see Gemma Galdon Clavell, *AI Auditing – Proposal for Algo-scores* (European Data Protection Board, SPE Programme 2024); J Mökander, "Auditing of AI: Legal, Ethical and Technical Approaches" (2023) 2 *Digital Society* 49.

then damages.[73] Instead, in digital policy, the regulatory approach is not risk-based but constitutional-based, thus emerging not only as a response to the need to manage inherent uncertainties of digital technologies but also the power imbalance and the information asymmetry that characterise contemporary technological environments, particularly between public and private actors. This model does not rely on science and knowledge, but rather on the recognition by public actors that the rapid evolution of digital technologies demands mechanisms to accommodate the unpredictability and dispersion of risks with the predominance of market actors while protecting fundamental rights and democratic values.

3. *The regulatory outcome: from precautionary measures to accountability and mitigation*

A subtle yet profound difference lies in the very nature of the risk being evaluated in digital policies. Despite applying a similar *ex-post* evaluation, such as impact assessments or simulations, as in the precautionary principle sphere, the agents and the epistemology of risk have changed, so have the regulatory outputs. Risk regulation influenced by the precautionary principle typically couples command-and-control obligations (e.g., binding emission ceilings) with procedural duties such as environmental impact assessments. The operative logic is preventive. In cases of scientific uncertainty, regulators lean on the side of caution and adopt more stringent preventive measures.

Digital regulations, conversely, privilege accountability and ongoing risk-management. In this regard, the GDPR has set the first paradigmatic example of this transition. Unlike the Data Protection Directive,[74] the GDPR regulatory framework has approached risk regulation, articulating the notion of accountability as connected with the protection of personal data as a fundamental right.[75] The GDPR can indeed be considered the first example of how fundamental rights have become an essential normative basis in European digital policy, opening the doors to the spread of a risk-based approach in the DSA and the AI Act. DPIAs under the GDPR, systemic-risk audits under the DSA, and FRIAs under the AI Act are conducted in the phase of development and often shortly before (or even during) deployment. Their aim is dynamic mitigation rather than prior prohibition. Even where obligations are stringent, e.g., annual reassessments, the remedies tend to be adaptive corrections (content moderation tweaks, bias monitoring, transparency reports) rather than outright bans.

This evolution underscores a constitutional turn. Regulation is calibrated to protect fundamental rights amid profound uncertainty and private dominance, rather than enforcing a priori technical ceilings. The result is a governance architecture in which precaution remains one option among many, overshadowed by iterative, rights-oriented risk management that continuously negotiate the fluid power relations of the digital ecosystem. This shift in risk regulation is founded on the imbalanced relationships between public and private actors in the digital age.[76] While risk regulation founded on precautionary principle has traditionally been aimed at managing risks in areas where public actors could rely on certain knowledge expertise, digital regulation faces the challenge of regulating areas governed by private actors in the algorithmic society.[77]

[73] Weimer and Marin (n 6).

[74] 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 L281/31.

[75] GDPR, Arts 1(2) and 5(2), Recital 74; Charter of Fundamental Rights of the European Union, Art. 8.

[76] Giovanni De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022).

[77] Jack M. Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation" (2018) 51 University of California Davis Law Review 1151; O Pollicino, "The Quadrangular

The imbalance between public and private actors stemming from the structural transformation in how knowledge and control are distributed, has shifted the locus of power to private actors. These actors, often large technology companies, hold exclusive access to critical datasets, algorithmic systems, and the technical know-how that underpin digital infrastructures.[78] As a result, public regulators frequently find themselves at a disadvantage, lacking the informational and technical capacity to assess or respond to emerging digital risks independently.

This divergence not only evidences the limited scope of the traditional precautionary model to respond to the challenges of governance, but it also implies a reconfiguration of the exercise of power, fundamental rights, and public and economic interests.

IV. Risk regulation and European constitutionalism in the digital age

The transition from a scientific rationality toward a constitutional approach in risk regulation represents, ultimately, a recognition and focus on the political, and not merely technical, nature of the challenges posed by digital technologies. The protection of fundamental rights and the safeguarding of democratic values form the core of risk regulation in the digital age, employing constitutional principles such as proportionality and accountability as normative guides to address the uncertainty of the digital environment.

This transformation can be considered a constitutional reaction. In response to risks to fundamental rights and power asymmetry, the EU has increasingly turned to a risk-based approach grounded in constitutional values as a means of asserting regulatory authority. Rather than relying solely on technical expertise or risk models, they invoke fundamental rights, such as privacy, equality, and freedom of expression, as normative anchors for intervention. This shift reflects an attempt to reestablish public oversight and legitimacy in grounds dominated by private governance. However, because private actors continue to control the architecture and logic of digital services and AI systems, this approach remains constrained, often reactive, and subject to the interpretive boundaries set by the very actors it seeks to regulate.[79]

This situation has made private actors, such as online platforms, an essential tile of the mosaic to ensure the enforcement of public policy objectives. A paradigmatic example is the EU policy against disinformation, which is profoundly based on a process of collaboration and trust between the European Commission, platforms and other stakeholders as manifested by the adoption of the Strengthened Code of Practice on Disinformation.[80] The underlying logic of this new regulatory paradigm lies in the functional duality that characterises private actors in the digital ecosystem. They are simultaneously generators of digital risk and its main mitigators. This paradox constitutes one of the defining features of contemporary digital regulation. Private entities, by concentrating critical information and controlling technological infrastructure, generate a power asymmetry with respect to public institutions responsible for safeguarding fundamental rights. Simultaneously, however, these same private actors constitute the

Shape of the Geometry of Digital Power(s) and the Move Towards a Procedural Digital Constitutionalism" (2023) 29 European Law Journal 10.

[78] Marietje Schaake, *The Tech Coup: How to Save Democracy from Silicon Valley* (Princeton University Press 2024).

[79] This asymmetric distribution of information is not unique to the digital age; it is a widespread feature of the risk society described by Ulrich Beck. What is distinctive now are the political responses adopted by public authorities, which follow an ex-post logic, as discussed in this paper.

[80] European Commission, *Strengthened Code of Practice on Disinformation* (June 2022) https://digital-strategy.ec.europa.eu/en/library/strengthened-code-practice-disinformation (accessed 28 April 2025).

most effective resource, and, actually, the only one available, to effectively assess and mitigate such risks, given their privileged technical knowledge and operational capacity.

This imbalance has led to the development of a different regulatory approach that aims to manage the interaction and cooperation between public and private actors, and the expansion of risk regulation in digital policy is an example. By adopting a more performance-based approach,[81] in which responsibility rests with the regulated party, the risk-based approach focuses on the fulfilment of regulatory objectives through discretion and adaptability in their implementation. Digital regulation thus transforms into a fundamentally political process, characterised by constant negotiation between private and public interests. Even the AI Act, which introduces prohibited practices following a top-down approach, combines performance elements with technical standards for high-risk systems,[82] reflecting the hybrid proposal suggested by Coglianese for contexts in which pure measurement proves complex.[83]

Consequently, instead of demanding concrete results or imposing obligations following a more straightforward command-and-control approach, the European risk-based approach to digital technologies is based on performance criteria and accountability standards based on constitutional values such as fundamental rights and democracy. Although the precautionary approach, in some aspects, also incorporates properties of a performance-based model, the approach to risk regulation in digital policy aims not only to provide greater flexibility in responding to risk scenarios, but also to address the imbalance between public and private actors. As a result, the obligation to assess risks shifts to the bottom, particularly to those actors controlling information and technological infrastructures, which are responsible for assessing and mitigating risks.

At the same time, this process leads public actors to shift from evaluation and management to evaluation and control of a pre-determined set of risks. The DSA, for instance, identifies certain types of risks for VLOPs involving interests such as electoral processes and gender based-violence.[84] Likewise, the AI Act defines specific areas of risks, also prohibiting certain AI systems.[85] The differentiation between the actors completing the assessment of digital risk and the institutions in charge of controlling that assessment is at the foundation of the whole digital risk regulation model, which emancipates from the traditional forms of risk regulation. Private and public actors are therefore the two sides of the rope that, obviously with tension, tend to collaborate to strike a balance between public interest and market objectives.

Then, accountability becomes one of the cornerstones of this system. It, therefore, transcends its conception as a mere technical instrument to become a central principle that transforms the regulatory model, establishing a functional bridge between private power and the public safeguarding of constitutional rights. This principle, crystallised in the proactive accountability defined by the GDPR,[86] radically transforms the relationship between regulators and regulated entities, establishing a continuum of responsibility. Regulatory instruments such as the DSA require VLOPs to provide periodic and detailed reports on content moderation activities and risk management.[87] Also the AI Act requires impact assessments that allow for anticipating and mitigating potential impacts on

[81] Cary Coglianese, "Performance-Based Regulation: Concepts and Challenges" in Francesca Bignami and David Zaring (eds), *Comparative Law and Regulation: Understanding the Global Regulatory Process* (Edward Elgar Publishing 2016) p 403.

[82] AI Act, Art. 5 (prohibited practices); Arts. 9–15 (performance elements in high-risk systems).

[83] Coglianese (n 403).

[84] DSA, Art. 34.4.

[85] AI Act, Art. 5.

[86] Raphael Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020).

[87] DSA, Arts. 33–4.

fundamental rights.[88] This change moves the focus from predominantly preventive models toward approaches which are inherently speculative and uncertain nature of digital risks, whose anticipatory identification and quantification is frequently unfeasible, even for private actors.[89]

This approach leads to a principle-based system, where the content of compliance is not shaped by a rigid top-down approach but by the articulation of nuanced and contextual regulatory responses, avoiding both paralysing over-regulation and ineffective under-regulation. In this case, alongside accountability, proportionality becomes central in European digital policy, constituting a transversal gear to establish differentiated obligations and paths of collaboration that could respond to the various levels of risk presented by different actors and technologies in the digital age.

This model of risk regulation presents significant advantages, particularly in terms of adaptability to technological threats and regulatory flexibility, but also raises constitutional challenges. First, this approach entails considerable disadvantages, especially related to the potential impact on fundamental rights that may suffer significant interference before regulatory mechanisms can be effectively enforced. Second, the degree of discretion granted to private actors in compliance and governance may be considered as a threat, particularly considering the dependence of public actors on the risk assessment performed by private actors. Third, if risk regulation based on constitutional values is uncertain, this not only affects the internal market but also the legal certainty in enforcement. However, these challenges have not been addressed by regulators who should carefully reflect on the safeguards and procedures in the relationships between public and private actors, and focus on enforcement in order to avoid arbitrariness and ensure accountability.

This transformation of European risk regulation underlines that the main objective of this approach is not only addressing technological risks but also managing the imbalance of power in the relationship between public and private actors. Rather than managing the risk itself, this approach is the result of a broader constitutional situation of imbalance that requires public actors to collaborate more with private actors in order to achieve public policy objectives.

V. Conclusions

The epistemological uncertainty inherent to digital technologies, derived from both their accelerated evolution and the role of private governance, has revealed the limitations of traditional scientific criteria for addressing technological risk that transcend the merely quantifiable. In Europe, this challenge has led to a paradigmatic shift in the underlying rationality of regulation, leading to a risk-based approach whose aim is to govern epistemological uncertainty through the instruments of constitutionalism, with the goal of protecting fundamental rights and addressing imbalances of power.

These constitutional values have acquired indisputable centrality in the conceptualisation and contemporary regulation of digital risk, transforming fundamental rights into an authentic regulatory paradigm, as a new scientific criterion. In this case, European digital risk regulation has indeed anchored itself in essential constitutional principles such as accountability and proportionality, and, in general terms, a regulatory narrative centred on fundamental rights.

The transformation of the European risk-based approach is a phenomenon that requires a profound rethinking of traditional relationships between regulators and regulatees.

[88] AI Act, Art. 27.

[89] Giovanni De Gregorio, "The Normative Power of Artificial Intelligence" (2023) 30 Indiana Journal of Global Legal Studies 55.

In this case, European digital regulation has not focused on establishing prohibitions or static mandates, but on articulating a dynamic process of responsibility to protect fundamental rights and democratic values. Nonetheless, assessing the margin of manoeuvre introduced by the European approach to risk regulation and the collaboration between public and private actors in the definition and mitigation of risks remains a constitutional challenge, and, particularly, it requires not only procedural safeguards but also an effective enforcement of digital regulation.

Competing interests. The authors declare none.

Cite this article: MV Vargas and G De Gregorio (2026). "The Transformation of European Risk Regulation: Managing Uncertainty and Powers in the Digital Age". *European Journal of Risk Regulation* **17**, 357–373. https://doi.org/10.1017/err.2025.10079