INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 6 | 2026 Art. 3

When Risk is Not Enough: Inter-Legality, Fundamental Rights and the Institutional Limits of European AI Governance

Adityasinh Ranjitsinh Ghatge
Law Student,
2nd Year, BBA.LL.B.,
Bharati Vidyapeeth New Law College, Pune

Recommended Citation
Adityasinh Ranjitsinh Ghatge, *When Risk Is Not Enough: Inter-Legality, Fundamental Rights and the Institutional Limits of European AI Governance,* 5 IJHRLR 24-32 (2026).
Available at www.ijhrlr.in/current-issues/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto & Co. administrator.
For more information,
please contact submission.ijhrlr@gmail.com

When Risk Is Not Enough: Inter-Legality, Fundamental Rights and the Institutional Limits of European AI Governance

Elif Biber, A Rights-Based Inter-Legal Approach to Artificial Intelligence, Hart Publishing, Oxford, 2026, 1st edn., 256 pp., ISBN 9781509979011, Price: £90.00 (Hardback).

INTRODUCTION

European AI regulation now operates within a dense and rapidly developing legal framework. The EU Artificial Intelligence Act establishes a risk-based structure for governing AI while the General Data Protection Regulation regulates much of the data environment on which these systems depend. The EU Charter and the European Convention on Human Rights provide overlapping guarantees and national public law continues to regulate the exercise of administrative authority.[1] This combination has intensified a broader scholarly debate over whether fundamental rights can be protected adequately within risk-based technological regulation or require a more explicitly rights-centred legal framework.

Elif Biber enters this debate from the field of European public law, drawing on her research on artificial intelligence, fundamental rights and inter-legality.[2] In *A Rights-Based Inter-Legal Approach to Artificial Intelligence*, she argues that AI cannot be governed adequately when the legal regimes surrounding it are treated as separate and self-contained systems. Rights may be affected at several stages of an AI system's lifecycle while legal responsibility may be divided among developers, vendors, public authorities and human decision-makers. For Biber, the resulting problem is therefore not simply technological risk but the fragmentation of legal authority itself.

The book proposes an inter-legal method for coordinating these overlapping regimes and placing fundamental rights at the centre of AI governance. Its strongest contribution lies in showing why AI regulation cannot be understood through the AI Act alone. Yet its argument also

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L 2024/1689, July 12, 2024; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119/1, May 4, 2016; Charter of Fundamental Rights of the European Union, 2012/C 326/02; Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

[2] *University of Luxembourg, "Sumeyye Elif Biber", available at: https://www.uni.lu/fdef-en/people/sumeyye-elif-biber/ (last visited on Sept. 14, 2026).*

invites a more difficult inquiry. Must risk-based and rights-based regulation be treated as competing models or can fundamental rights operate as binding limits within a risk-based structure? This review argues that Biber is most persuasive in diagnosing legal fragmentation, lifecycle effects and the hybrid distribution of public power while the institutional operation of inter-legality remains less fully resolved. The central issue is ultimately not only which rights apply but who must reconcile overlapping legal regimes, according to what principles and with what consequences for responsibility and effective remedies.[3]

FROM REGULATORY FRAGMENTATION TO INTER-LEGALITY

Biber treats AI as a socio-technical system rather than an isolated technological artefact.[4] The distinction controls much of the argument. If AI is understood chiefly as software, regulation naturally concentrates on technical characteristics, measurable risks and product compliance. If it is understood as an arrangement of data, models, institutional choices, economic incentives, human oversight and administrative authority, the legal inquiry changes. The relevant question is not only whether a system is technically safe but how power is distributed through it and which rights are affected at different stages of its operation.

This framing exposes the central difficulty of regulatory fragmentation. A single AI deployment may raise questions under the AI Act, data protection law, equality law, administrative law, the EU Charter and the ECHR. Private technical standards may shape a system later used by a public authority. An arbitrary or discriminatory administrative outcome may originate in training data, model design or procurement although the legally visible decision appears only at deployment. Conventional analysis tends to ask which legal regime applies. Biber instead asks how several applicable regimes should interact when none can explain the problem adequately on its own.

Inter-legality supplies the conceptual answer. Biber draws on a theory developed to address overlapping legal orders and recasts it for AI governance. The framework emphasises the "publicness" and "inter-systemic" character of AI, follows rights across the lifecycle of the system and culminates in a three-step adjudicative model intended to translate the theory into legal practice. Fundamental rights are not treated as interests whose weight is determined by technical risk calculations. They

[3] Elif Biber, *A Rights-Based Inter-Legal Approach to Artificial Intelligence* (Hart Publishing, Oxford, 1st edn., 2026); University of Luxembourg, "Protecting our Rights: How Can Legal Systems Handle the AI Revolution?", Apr. 16, 2026, available at: https://www.uni.lu/fdef-en/news/protecting-our-rights-how-can-legal-systems-handle-ai-revolution/ (last visited on Sept. 14, 2026).

[4] University of Luxembourg, supra note 3.

function as normative constraints capable of shaping the interpretation of the regulatory systems that surround AI. The book therefore seeks to move European AI governance from parallel compliance with separate regimes toward legally coordinated rights protection.

METHOD, EVIDENCE AND THE STRENGTH OF THE DIAGNOSIS

The method is primarily doctrinal and conceptual, supported by European legislation, CJEU and ECtHR jurisprudence and examples of AI used by public authorities. That approach matches the research problem. Biber is not attempting to measure empirically how frequently algorithmic systems violate rights. She asks whether the legal structures governing them can recognise and respond coherently to rights problems that cross doctrinal boundaries.

The method is particularly effective when Biber reverses the usual perspective of AI regulation. Much analysis begins inside the AI Act, working outward from categories such as prohibited practices, high-risk systems, transparency duties and conformity assessment. Biber begins with the rights-bearing person and the institutional setting in which AI is used. This produces a more realistic account of public-sector AI, where public decisions may depend on private infrastructure, external vendors, technical standards and datasets that administrators neither created nor fully control. Formal attribution of a final decision to the State can therefore conceal a much more distributed structure of power.

Her lifecycle perspective is equally strong. Harm can be produced at one stage and become legally visible at another. Biased data, opaque design choices or defective procurement may constrain later administrative discretion long before an individual receives a decision capable of challenge. Following rights from design through deployment and review avoids the artificial assumption that accountability begins only at the point of final decision-making.

The weakness appears when diagnosis becomes institutional prescription. Inter-legality establishes why several legal orders must be considered together; it does not by that fact alone determine how conflicts among them are to be resolved. The broader literature on inter-legality has confronted the same difficulty.[5] Once hierarchy is displaced by interaction, a decision-maker needs criteria for deciding which norm controls, which institutional claim deserves priority and how conflicting rationales should be reconciled. Without such criteria, interpretive openness can become legal indeterminacy. Biber's framework is therefore more precise in identifying fragmentation than in specifying

[5] Neil Walker, "Legalising Inter-Legality", 1 *European Law Open* 216 (2022).

the authority through which fragmentation is finally settled.

THE RIGHTS–RISK DIVIDE

Biber's most provocative intervention concerns risk-based regulation. Her objection is strongest where risk language is allowed to redefine the content of fundamental rights. A rights violation is not always comparable to an undesirable outcome whose probability and severity can be calculated, mitigated and then accepted as residual risk. Rights structure the permissible exercise of public power. They may impose duties that do not disappear because aggregate benefits exceed individual costs.

The problem is sharpened by the AI Act's product-regulatory architecture. Risk classification, conformity assessment, technical standards and provider obligations are valuable tools for governing complex technology, yet they become normatively unstable when the protected object is a fundamental right rather than product safety. A conventional risk inquiry may ask whether a harmful outcome is sufficiently probable or severe to justify regulatory intervention. Rights law may ask whether a particular interference is lawful and justified in the first place.

Still, Biber's critique should not become an absolute opposition between risk and rights. Martin Ebers, while defending genuinely risk-based AI regulation, himself recognises that fundamental rights sit uneasily within a model built around probabilistic assessment and market regulation. Georgios Pavlidis pushes in a different direction, arguing that the final AI Act increasingly internalises rights as legal thresholds and procedural triggers across the AI lifecycle. Francesca Palmiotto's account of the legislative process likewise shows that the ultimate strength of rights protection will depend heavily on implementation, enforcement and judicial interpretation.[6] Taken together, this scholarship suggests that the conflict is not adequately captured by asking whether regulation should be risk-based or rights-based.

The more precise question is whether risk governance is legally subordinated to rights. The final AI Act contains fundamental-rights impact assessment, human oversight, transparency obligations and

[6] Martin Ebers, "Truly Risk-based Regulation of Artificial Intelligence: How to Implement the EU's AI Act", 16 *European Journal of Risk Regulation* 684 (2025); Georgios Pavlidis, "The EU AI Act and the Rights-Based Approach to Technological Governance", 64(1) *Review of European and Comparative Law* 117 (2026); Francesca Palmiotto, "The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation", 16 *European Journal of Risk Regulation* 770 (2025).

special duties for high-risk uses.[7] These mechanisms do not establish that the Act protects rights adequately but they show that rights can operate from within a risk architecture. Biber is therefore most convincing when she argues that risk cannot determine the legal meaning of rights. She is less convincing if her argument is understood to require displacement of risk regulation itself. Inter-legality may be more valuable as a means of constitutionalising risk governance than as its replacement.

PUBLICNESS, RESPONSIBILITY AND REMEDIES

Biber's treatment of publicness is harder to resist. AI used by public authorities is frequently built outside the State. One actor may design the model, another may supply data, private or hybrid bodies may generate technical standards and the public authority may possess limited access to the system's internal operation. Yet the legal consequence is eventually experienced as an exercise of public power.

A narrow public/private distinction cannot explain this arrangement. Private design choices can acquire constitutional significance once embedded in administrative decision-making. This matters acutely in welfare, employment, migration, policing, taxation and access to public services. Rights protection cannot depend solely on identifying the person who makes the final administrative decision, it must examine how control, information and responsibility are distributed across the system.

Inter-legality nevertheless leaves an accountability problem. If several actors contribute to a harmful outcome, the law must still determine who owes which duty, what information must be disclosed, what standard of review applies and what remedy is available. Courts can interpret overlapping norms but usually after a dispute has matured. Regulators possess supervisory powers but divided mandates. Technical standard-setters hold expertise without necessarily possessing corresponding democratic legitimacy. Providers often control the information required to challenge a system. Inter-legality reveals these relationships but revelation is not allocation.

Remedies consequently provide the most demanding test of Biber's framework. A rights-based approach matters only if a rights-holder can obtain reasons, contest a decision, identify an accountable actor and secure effective redress. Biber's own subsequent work with Herwig Hofmann is revealing in this respect. Their 2026 analysis shifts the emphasis toward the "missing dialogues" among rights, risks and

[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), arts. 13, 14 and 27.

remedies arguing that abstract commitments to fundamental rights are insufficient unless translated into enforceable mechanisms and meaningful access to justice.[8] That later development does not displace the book's thesis; it clarifies where the thesis must ultimately lead. The move from rights to remedies is the point at which inter-legality must become institutional rather than merely jurisprudential.

A LEGAL ORDER MOVING AROUND THE BOOK

The European legal landscape shifted even as the book appeared. On 15 May 2026, shortly before publication, the European Union ratified the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. The Convention adds another rights-based layer to an environment already populated by the AI Act, GDPR, Charter, ECHR and national public law. The EU has indicated that obligations concerning private actors will be implemented through the AI Act and the broader Union acquis.[9] That development closely resembles Biber's descriptive account of inter-legality: the same technological activity is governed through norms originating in several legal orders that must operate together.

A clearer post-publication test arrived with Regulation (EU) 2026/1744, the Digital Omnibus on AI which entered into force on 27 July 2026. It postponed major high-risk requirements with rules for several Annex III high-risk uses moving to 2 December 2027 and product-embedded high-risk systems to 2 August 2028.[10] The postponement can be defended as a response to incomplete standards, implementation difficulties and the need for legal certainty. It can also be read through Biber's critique. If practical rights protection depends on technical standards and staged product compliance duties, delays in regulatory readiness can become

[8] Elif Biber and Herwig H.C. Hofmann, "A Human-Centric Approach Through Rights: The Missing Dialogues between Rights, Risks, and Remedies under the EU's Artificial Intelligence", available at: https://ssrn.com/abstract=7389400 (last visited on Sept. 14, 2026).

[9] Council Decision (EU) 2026/1080 of 21 April 2026 on the conclusion, on behalf of the European Union, of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, OJ L 2026/1080, May 13, 2026, art. 3 and Annex; Council of Europe, "European Union Ratifies the Council of Europe Framework Convention on Artificial Intelligence", May 15, 2026, available at: https://www.coe.int/en/web/artificial-intelligence/-/european-union-ratifies-the-council-of-europe-framework-convention-on-artificial-intelligence (last visited on Sept. 14, 2026).

[10] Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), OJ L 2026/1744, July 24, 2026, art. 1(40) and 4.

delays in the legal safeguards attached to high-risk systems.

Neither development proves that Biber's preferred model is correct. Together they demonstrate that the difficulty she identifies is real. European AI governance is becoming simultaneously more risk-regulatory and more saturated with rights commitments. The central problem is coordination, determining how rights derived from different regimes constrain technical regulation, who interprets those constraints, and what follows when compliance machinery and rights protection move at different speeds.

CONTRIBUTION, LIMITS AND OVERALL ASSESSMENT

A Rights-Based Inter-Legal Approach to Artificial Intelligence makes its most important contribution by changing the level at which the regulatory problem is perceived. It moves analysis away from the internal mechanics of one statute and toward interactions among legal regimes, institutional actors and stages of technological development. That shift is valuable because AI governance is fragmented by design. No single instrument governs data, discrimination, administrative legality, technical safety, human rights and remedies in equal measure.

The originality should be stated with some care. Biber is not the first scholar to argue that AI threatens fundamental rights nor is lifecycle governance itself wholly new.[11] Her distinctive move is methodological. She imports inter-legality into European AI public law and uses it to connect bodies of doctrine that are often analysed separately. The novelty therefore lies less in the subject matter than in the legal architecture through which the subject is organised. That makes the book particularly useful to public lawyers, human-rights scholars, regulators and judges who must work across doctrinal boundaries. It is less a manual for technical compliance than a challenge to the legal assumptions on which compliance systems are built.

The book also resists a subtler danger of allowing technical concepts to determine normative outcomes. Risk, explainability, human oversight and conformity assessment are not self-interpreting categories. Their legal significance depends on the rights and institutional principles against which they are applied. Biber makes that dependency difficult to ignore.

The principal limitation follows from the ambition of the theory. The

[11] Alessandro Mantelero, "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment", 34(4) *Computer Law & Security Review* 754 (2018); David Restrepo Amariles and Pablo Marcello Baquero, "Promises and Limits of Law for a Human-Centric Artificial Intelligence", 48 *Computer Law & Security Review* 105795 (2023).

more legal orders inter-legality brings into conversation, the more pressing the question of authoritative resolution becomes. A framework intended to overcome fragmentation can move the same fragmentation into adjudication if it does not specify sufficiently determinate criteria for priority, responsibility and remedy. This is not an argument for returning to sealed doctrinal compartments. It is an argument that inter-legality requires a stronger institutional account if it is to generate predictable legal outcomes.

The European focus is similarly both a strength and a boundary. Europe offers an unusually dense environment for developing the theory because supranational regulation, regional human-rights law and domestic public law already overlap. The same density may limit institutional portability to jurisdictions with weaker regulatory capacity, different traditions of rights adjudication or no comparable supranational legal structure. Inter-legality may therefore possess broader explanatory force than the specifically European mechanisms through which Biber operationalises it.

CONCLUSION

The book ultimately succeeds for a reason somewhat different from the strongest version of its regulatory claim. It does not establish that rights-based regulation must displace risk-based regulation. It does establish that risk governance cannot determine the content of rights on its own. Its most durable insight is that AI regulation is already an inter-legal problem of distributed power, lifecycle effects and overlapping norms. Its unresolved question is how that insight becomes an authoritative and remedially effective institutional practice.

That unresolved question identifies the next stage of the scholarship rather than cancelling Biber's contribution. The task now is to explain how inter-legality can coordinate overlapping rights without sacrificing legal certainty, how responsibility can be assigned across hybrid public-private systems and how rights can be made actionable when technical and legal governance fail simultaneously. Biber's book deserves attention because it redefines the problem that any serious account of rights protection in European AI governance must confront.