

AI in European Law: A Deep View

Herwig C. H. Hofmann, Elif Biber, and Zahra Yusufli

The Purpose of the Book

This book invites to explore the legal challenges posed by the growing use of technology across various sectors of EU law and policy. It addresses the legal challenges posed by AI technologies by looking at the intersections of policy-specific questions and regulation with general AI regulatory questions in fields such as competition law enforcement, fraud detection and criminal liability, labour law and working conditions, autonomous decision-making systems, and financial market regulation. These chapters are set against a discussion of questions of digital rights, open data policies and challenges of access to justice and judicial review of data-related matters.

By bringing together scholars from diverse legal backgrounds, spanning public, private, and criminal law, the book offers a multidimensional understanding of how latest technology is reshaping legal systems. Each chapter analyses both specific regulatory challenges and their implications for the EU's wider digital agenda. The case studies and legal analyses are grounded in real-world examples, linking legal theory to practical concerns.

The primary aim of this volume is to assess whether the current EU legal framework is equipped to address the profound transformations AI brings. It does so by analysing how AI affects decision-making by both private and public actors, and how legal systems respond to issues such as algorithmic opacity, autonomy, and the continuous learning capacity of AI systems. These features challenge conventional legal categories and demand new approaches to accountability, transparency, and risk management.

A key theme of the book is the need for interdisciplinary approaches in AI governance. Legal expertise alone is insufficient to evaluate high-risk AI systems, which also require input from computer science, ethics, and sector-specific knowledge. This is reflected in the volume's structure, with each chapter combining doctrinal analysis with technical and contextual insights. For example, the regulation of algorithmic management systems in labour law, or the review of smart contracts in private law, are discussed not

only in terms of legal compliance but also practical feasibility and societal impact.

The book also addresses the cross-border dimensions of AI regulation, considering how EU law interacts with national and international legal frameworks. Topics such as social scoring, fraud detection, and AI in supply chains illustrate the cross-border nature of these challenges.

In sum, this volume argues that AI regulation is not just a technical exercise, but a normative project concerned with balancing innovation, democratic control, and the protection of fundamental rights. The EU's evolving regulatory approach represents a significant attempt to govern AI in line with these values. By offering a combination of theoretical reflection and policy-relevant analysis, this book contributes to the ongoing re-evaluation of how law can and should respond to the digital transformation of society.

Structure of the Volume and Key Themes

A recurring theme of this volume is the issue of accountability in the public sector use of AI: who can be held responsible, and through which legal safeguards, when automated systems produce harmful or unjust outcomes? Chapter 2 by Arthur Bianco illustrates this challenge through the example of AI-driven tax administration in the European Union. Tax authorities increasingly rely on AI tools for fraud detection, audit selection and taxpayer services, yet these systems may produce opaque, biased, or erroneous outputs with severe consequences for individuals. Bianco shows that these risks are not matched by an adequate EU-level regulatory response. Although the AI Act frames certain public-sector AI as 'high-risk,' it expressly excludes tax administration from this category, leaving such systems subject only to minimal transparency obligations. The safeguards central to the AI Act therefore do not apply, despite the significant coercive powers tax authorities wield over citizens. Bianco argues that this gap reflects political sensitivities surrounding fiscal sovereignty and a narrow, market-focused legislative design. His contribution demonstrates that accountability in AI-supported public administration cannot be achieved through technical regulation alone: safeguards for fundamental rights must be embedded even in domains that lie at the heart of state authority.

Where Bianco exposes accountability gaps in public-sector AI, in Chapter 3, Zahra Yusifli turns to the workplace to show how similar gaps arise

under the EU AI Act in employment relations. Although Annex III classifies workplace AI systems as high-risk, the Act's derogation clause in article 6(3) opens a path for employers to argue that their tools merely support, rather than shape, decision-making. Yusifli shows how these derogations, combined with ambiguous thresholds for 'material influence' and narrow conceptions of harm, risk allowing high-impact employment systems to escape the obligations designed to ensure transparency, human oversight and accountability. This is particularly problematic in contexts of algorithmic management, where power imbalances already discourage human intervention and facilitate automation bias. Even when transparency duties exist, workers often lack the procedural tools, bargaining power and information needed to challenge AI-supported decisions. Her analysis demonstrates that meaningful worker protection cannot rest solely on risk classification and supply-chain obligations. Instead, robust safeguards rooted in labour law, collective rights, and enforceable oversight are required to prevent AI from entrenching managerial prerogatives and eroding workplace autonomy.

In Chapter 4, Isabella Lorenzoni explores how data's dual role, as both a competitive advantage for firms and a crucial input for public enforcement, reshapes EU competition law. She examines business-to-business data sharing, where dominant firms' control over proprietary datasets may exclude rivals and distort markets. Traditional mechanisms such as the Essential Facilities Doctrine provide limited ex post remedies. In contrast, emerging EU regulations like the Digital Markets Act and the Data Act introduce ex ante data-sharing obligations to address market failures in data access. Crucially, the chapter extends this analysis to the public sector, showing how business-to-government and government-to-government data sharing can equip competition authorities with the datasets necessary to deploy AI-based enforcement tools. In an era of 'computational antitrust,' authorities need high-quality, machine-readable data to detect collusive practices, assess mergers, and monitor digital markets. Lorenzoni identifies legal gaps in the Data Act's provisions and argues for tailored sectoral frameworks that enable proactive data sharing while safeguarding privacy and commercial confidentiality. The chapter calls for integrated legal approaches that not only regulate dominant firms' data power but also empower regulators to uphold fair competition in AI-driven markets.

The volume continues with a contribution examining how AI is reshaping access to legal services. In Chapter 5, Kalliopi Terzidou critically examines AI-powered legal chatbots, asking whether large language models such as ChatGPT and Gemini can support self-represented litigants in

navigating legal processes, with a focus on landlord-tenant disputes under Greek law. Drawing on the EU's commitment to trustworthy AI, Terzidou develops a normative framework grounded in fairness, human autonomy, explicability, and prevention of harm. Her evaluation reveals that while LLM-based tools score well on accessibility and readability, they often provide inaccurate, outdated, or incomplete legal information and lack proper citation of sources. Most troublingly, these systems can generate misleading outputs without safeguards such as consistent disclaimers or verifiable references. Rather than bridging justice gaps, such tools risk entrenching new inequalities when users rely on outputs that appear authoritative but cannot be trusted. Terzidou distinguishes sharply between AI augmentation, where professionals are supported by AI tools, and AI substitution, where users rely on these tools in place of professional advice. Her findings warn against uncritical optimism and call for rigorous design standards, public oversight, and institutional safeguards.

Chapter 6, authored by Anna Moraiti, addresses whether autonomous AI systems should be treated as bearers of legal rights and obligations, particularly under criminal law. This inquiry stems from real-world challenges in attributing liability when complex AI systems cause harm in ways that defy clear human attribution. Drawing on analogies with corporate criminal liability, proponents have suggested that recognising 'electronic personhood' could fill accountability gaps. However, Moraiti's analysis reveals significant doctrinal pitfalls in this analogy. While corporations embody human collectives and serve as proxies for their members' intentions, AI systems lack the capacity for reflection, moral agency, or relational grounding that personhood presupposes in criminal law. Extending criminal liability to AI risks creating an 'empty imputation,' allowing responsible human actors to evade scrutiny. Instead, Moraiti advocates for a more restrained approach rooted in civil law, where limited legal personhood could serve pragmatic goals such as fair risk allocation without overstepping conceptual boundaries. The chapter urges caution against anthropomorphising AI or diluting fundamental principles of criminal justice, while recognising the need for adaptive legal mechanisms in an age of emergent machine agency.

Chapter 7 by Grazia Bruzzese explores AI's deployment in digital fraud detection within the financial sector. Digital payment fraud has proliferated alongside the digitisation of banking, prompting institutions to turn to machine learning tools capable of detecting anomalous transactions in real time. Yet the adoption of such tools is not merely a technical upgrade but a legally intricate process. Banks must navigate overlapping obligations under

the AI Act, PSD2, the GDPR, and sector-specific supervisory standards. This layered regulatory context generates compliance complexity, particularly concerning the use, quality, and sharing of personal and transactional data. While AI can help mitigate fraud risk, its effectiveness hinges on access to large, high-quality datasets, a condition often hampered by inter-bank competition and privacy constraints. Bruzzese identifies this data bottleneck as a critical obstacle and proposes a coordinated EU approach that might include a centralised fraud data platform, analogous to existing anti-money laundering databases. The chapter demonstrates that technical tools alone cannot resolve fraud's persistence; effective AI deployment requires legal frameworks that facilitate data cooperation, uphold fundamental rights, and promote systemic resilience.

Chapter 8 by Théo Antunes focuses on smart contracts, automated, self-executing digital agreements, and their integration into legal frameworks governing contractual securities. Through a detailed analysis under Luxembourg law, one of Europe's most fintech-forward jurisdictions, the chapter probes how the immutable, automatic nature of smart contracts intersects with the flexible, interpretive requirements of private law. While Luxembourg has adopted several 'Blockchain Laws' to support innovation, Antunes shows that the legal regime remains primarily focused on blockchain as an object of investment rather than as a means of forming and executing obligations. This creates significant legal uncertainty when applying smart contracts to securities, which often demand human discretion and responsiveness to unforeseen events. The chapter identifies key challenges, from coding accuracy and oracle reliability to questions of enforceability, consent, and contractual form, and proposes practical safeguards including hybrid smart contracts that blend automation with human oversight. These recommendations aim to preserve the normative foundations of private law while enabling legal innovation. Antunes' contribution underscores that as automation technologies shape legal and economic life, their interaction with existing doctrines requires not only regulatory updates but conceptual clarity about what law demands when human judgment is outsourced to machines.

The final contribution by Elif Biber and Herwig C. H. Hofmann addresses a structural tension at the heart of the EU's Artificial Intelligence Act: the *missing dialogues* between its stated commitment to fundamental rights and the technocratic, risk-based framework through which those rights are meant to be protected. The chapter shows that, despite repeated references to fundamental and human rights and the rule of law, the AI Act insuffi-

ciently translates these commitments into enforceable legal mechanisms. The authors develop this argument in three steps. Firstly, they situate the AI Act within the EU's broader digital acquis, revealing how it conflates fundamental rights protection with technical risk management and product-safety compliance. Second, they examine human oversight obligations and the Fundamental Rights Impact Assessment (FRIA), arguing that both risk becoming symbolic, checklist-based exercises ill-suited to capturing the real-world impacts of AI. Thirdly, they analyse the Act's review and conformity-assessment procedures, showing how reliance on self-assessment and private actors weakens accountability and access to justice. Finally, the chapter outlines concrete steps to align fundamental rights with their legal enforcement, highlighting improved access to justice as key to realising the EU's human-centric approach to AI governance. This contribution serves as both a capstone and a call to action for the volume.