Please quote as: Currie, W. L., Schlagwein, D., Leimeister, J. M. & Willcocks, L. (2025). Rethinking technology regulation in the age of AI risks. Journal of Information Technology (JIT), , 10. doi: 10.1177/02683962251378815

JIT

Editorial

Rethinking technology regulation in the age of AI risks

Journal of Information Technology
2025, Vol. 0(0) 1–10

DOI: 10.1177/02683962251378815
Journals.sagepub.com/jinf
Sage

Wendy L Currie[1], Daniel Schlagwein[3], Jan Marco Leimeister[2] and Leslie Willcocks[4]

Abstract

This paper argues that artificial intelligence exposes the shortcomings of traditional regulatory paradigms, challenging Easterbrook's 'Law of the Horse' view that general legal principles suffice. AI's opacity, autonomy, and systemic risks demand risk-informed, technology-specific governance. We identify the pacing problem, where innovation outstrips regulatory capacity, and propose a tripartite framework distinguishing functional, structural, and relational risks. Comparative analysis of EU, US, UK, and Chinese approaches highlights divergent logics of precaution, market oversight, hybrid flexibility, and state control. Effective governance requires embedding risk into policy design through adaptive, proportionate, and harmonised mechanisms, balancing innovation with accountability. The paper underscores the urgency of global coordination and calls for interdisciplinary IS research to inform anticipatory, participatory, and ethically grounded regulation.

Keywords

Artificial Intelligence, Regulation, Governance, Innovation, Risk

Introduction

The rapid evolution of artificial intelligence (AI) has reignited foundational debates in legal theory, policy, and governance, exposing the limitations of traditional regulatory frameworks in addressing the unique challenges posed by intelligent systems. As editors of the Journal of Information Technology, we are committed to advancing critical, interdisciplinary, and socio-technical perspectives on emerging technologies. We encourage research that theorizes digital innovation and engages with its institutional, ethical, and policy implications. This editorial affirms our wider position: that information systems (IS) scholarship is integral to critically examining how societies govern, negotiate, and respond to transformative technological change.

This editorial on AI risk and technology regulation re-examines Easterbrook's (1996) 'Law of the Horse' metaphor, which argued against technology-specific legislation in favour of general legal principles; an approach grounded in a time when digital systems were comparatively rudimentary and their societal repercussions limited. In contrast, today's AI technologies, characterised by emergent behaviours, recursive learning, and systemic risks, challenge this analogy and necessitate fundamentally rethinking regulatory paradigms (Judge et al., 2025).

Unlike earlier technologies, AI operates as a dual force: it drives unprecedented innovation while simultaneously introducing novel risks, from algorithmic bias in autonomous decision-making to the commodification of personal data and threats to democratic institutions (Arora et al., 2023; Grote et al., 2024). In IS terms, this duality reflects the generative

[1]Audencia Business School, France
[2]St Gallen University, Switzerland
[3]University of Sydney, Australia
[4]London School of Economics, UK

Corresponding author:
Wendy L Currie, Audencia Business School, 8 Rte de la Jonelière 44300 Nantes, France.
Email: wcurrie@audencia.com

tension between infrastructural 'openness' that fuels innovation and governance 'closure' that safeguards societal interests (Henfridsson and Bygstad, 2013; Markus, 2007).

The opacity of deep learning models for humans, their ability to evolve post-deployment, and their integration into critical sectors such as healthcare, finance, and criminal justice render conventional ex ante regulation increasingly ineffective (Berente et al., 2021; Haenlein and Kaplan, 2019). The stakes are high. Without strong oversight, AI risks deepening inequality, undermining human autonomy, and disrupting national and global governance structures (Manheim and Kaplan, 2019; McKinley, 2022).

We argue AI regulation requires different regulatory approaches compared to traditional frameworks, and calls for embracing a nuanced, ethical, and risk-informed approach. That is, adaptive to technological change, proportionate in its application of oversight, harmonised across jurisdictions to reduce fragmentation, and grounded in ethical principles that prioritise transparency, accountability, and public engagement (Kashefi et al., 2024; Marchant, 2011). These pillars are not mutually exclusive but interdependent, forming the foundation of a regulatory architecture capable of managing AI's complexity and pace of development. The unprecedented speed of technological progress requires ex ante governance and requires high-risk providers to run documented risk management before market entry. AI's autonomous behaviour, flawed or biased training data, lack of oversight, and overreliance on automation have created many high-risk use cases. Examples such as McDonald's AI tool, unable to interpret orders, or allegations of AI-generated articles in the magazine Sports Illustrated (Analytics Insight, 2024) underline far-reaching societal consequences.

As AI systems edge closer to artificial general intelligence (AGI), the window for proactive governance is narrowing. Anchoring risk as a central regulatory construct and fostering coherence across institutional domains becomes imperative. Policymakers must act to ensure that the trajectory of AI development reinforces, rather than undermines, ethical norms, and societal values (OECD, 2023, 2024). The urgency of this approach is underscored by recent controversies, from deep-fake-based disinformation to biased hiring algorithms (Vaccari and Chadwick, 2020). These cases suggest the potential consequences of delayed or insufficient regulatory responses (Hacker et al., 2023; Maslej et al., 2024). Such controversy not only highlights the ethical and societal stakes of AI but also exposes a deeper structural issue: the inability of regulatory systems to keep pace with technological innovation. This phenomenon, known as the pacing problem, is the focus of the next section.

The pacing problem and regulatory lag

The exponential advancement of AI has revealed a fundamental mismatch between the speed of technological innovation and the capacity of regulatory systems to respond, a phenomenon widely recognised as the pacing problem (Grote et al., 2024; Taeihagh, 2021). Unlike earlier technologies such as industrial machinery, contemporary AI systems, ranging from large language models like GPT to predictive policing tools, evolve dynamically, often in ways their creators cannot fully anticipate (Judge et al., 2025). This renders traditional regulatory models, which are designed for static, predictable technologies, increasingly obsolete. Even longstanding digital technologies have been critiqued as inadequately regulated, with their operational complexities eluding prevailing legal frameworks and categorical distinctions (Jacobides and Lianos, 2021). The regulatory gap has only widened with the advent of AI, whose emergent functionalities and epistemic opacity further challenge existing normative and institutional architectures.

An example of the pacing problem emerged following the public release of ChatGPT in late 2022. Within months, its widespread adoption in education, law, and healthcare triggered regulatory responses in many jurisdictions. Italy temporarily banned the tool over privacy concerns (GPDP, 2024), while later the EU more widely accelerated negotiations on the AI Act to address foundation models. This rapid AI integration outpaced institutional policies, illustrating how socio-technical systems can evolve quicker than governance framework adaptation. Policies are almost always post-hoc measures.

From an IS research perspective, this underscores the need for real-time regulatory feedback loops, mechanisms that allow institutions to sense, interpret, and respond to emergent behaviours in digital infrastructures. The ChatGPT case exemplifies how generative AI can reconfigure user practices, institutional norms, and risk perceptions in ways that challenge static regulatory models. Several structural barriers exacerbate this disconnect:

First, regulatory frameworks tend to be reactive, often emerging only after significant harm has occurred. For example, the public release of generative AI models spurred the EU's AI Act, just as high-profile data breaches have typically triggered General Data Protection Regulation (GDPR) enforcement actions (GDPR, 2020; Maslej et al., 2024). In the US, the absence of comprehensive federal AI legislation has left oversight fragmented across sectoral agencies such as the Food and Drug Administration and Federal Trade Commission, creating gaps in coverage for high-risk tools like emotion recognition systems (Manheim and Kaplan, 2019).

Second, persistent knowledge asymmetries between regulators and developers hamper effective oversight. Many regulatory bodies lack the technical expertise to audit black-box models or assess systemic risks. This asymmetry

is acute in domains like high-frequency trading or generative AI, where algorithmic opacity undermines accountability (Arora et al., 2023; Currie et al., 2019).

Third, AI systems often exhibit shifting risk profiles depending on their context of use (Novelli et al., 2024). A chatbot designed for customer service and general questions may pose limited risk, but if repurposed for mental health advice or legal counselling, it could become a high-risk application requiring stringent oversight. This fluidity complicates the application of static regulatory categories and challenges the effectiveness of one-size-fits-all approaches (Buiten, 2019; Hacker et al., 2023).

To bridge these gaps, policymakers must adopt more adaptive and anticipatory regulatory tools. The UK's Artificial Intelligence (Regulation) Bill, for example, proposes regulatory sandboxes, controlled environments where AI systems can be tested under supervision. This approach allows for real-time risk assessment without stifling innovation (UK, 2023b). Similarly, algorithmic audits and transparency mandates, such as those in the EU AI Act, require developers to document training data sources, decision logic, and failure modes. Independent audits, potentially conducted by agencies like the U.S National Institute of Standards and Technology (NIST), could further enhance compliance (Roberts et al., 2023).

Some jurisdictions are also experimenting with horizon-scanning mechanisms to identify emerging risks before they materialize (Zhang et al., 2025). Singapore's Infocomm Media Development Authority (IMDA), for instance, uses anticipatory governance to pre-emptively draft guidelines for technologies like deepfake detection. A similar model could be institutionalized in the US through a National AI Advisory Council (OECD, 2023; OECD, 2024).

The potential risks associated with regulatory inaction or substantial lag have become a growing concern among policymakers. Without adaptive regulation, innovation may continue to outpace safeguards, leading to public backlash and overcorrections that result in overly restrictive laws. This dynamic not only stifles beneficial innovation but also contributes to regulatory fragmentation, as jurisdictions adopt conflicting rules in response to local pressures (Tallberg et al., 2023). While regulatory lag is a pressing concern, it is only one dimension of the broader governance challenge. At the heart of AI regulation is the need to understand and manage risk, not just technical risk, but systemic, institutional, and relational risks. The next section introduces a framework to address this.

Risk as a central regulatory construct

AI ushers in a new category of risks that extend beyond technical errors. Potentially, AI risks are systemic, evolving, and deeply rooted in institutional dynamics. These risks arise from the complex interaction between algorithmic structures, economic incentives, and governance models, making them often resistant to conventional regulatory solutions and difficult to disentangle or control in isolation (Arora et al., 2023; Grote et al., 2024). A risk-informed regulatory framework must therefore move beyond static compliance checklists and instead address the logics that shape how AI is developed, deployed, and governed. To conceptualise these risks, a tripartite framework comprises functional, structural, and relational risks, with each category reflecting a distinct set of challenges that require tailored governance strategies.

Functional risks arise from the technical architecture of AI systems. These include algorithmic bias, where discriminatory patterns in training data lead to unequal outcomes, and the opacity of black-box models that resist human interpretation, including in high-stakes domains like healthcare (Berente et al., 2021; Buiten, 2019). Security vulnerabilities, such as adversarial attacks that manipulate inputs to deceive autonomous systems, also fall into this category. Addressing functional risks requires pre-market certification processes, including bias audits and adversarial testing, as well as explainability mandates that compel developers to disclose model logic (Hacker et al., 2023; Roberts et al., 2023). However, these interventions often encounter resistance from market actors who view transparency as a threat to proprietary advantage, highlighting the tension between commercial secrecy and public accountability (Manheim and Kaplan, 2019).

Structural risks operate at the societal level and include the erosion of democratic norms through AI-powered disinformation and surveillance, the displacement of workers by automation, and the monopolisation of AI infrastructure by dominant tech firms (Grote et al., 2024; Zuboff, 2020). These risks destabilise institutions and exacerbate inequality. Regulatory responses may involve sectoral bans on particularly harmful applications, such as the EU's prohibition of social scoring or the creation of public AI alternatives to counterbalance private dominance (European Parliament, 2024; OECD, 2023). However, the drive for rapid scaling may at times be in tension with the precautionary principles embedded in governance frameworks (Currie and Seddon, 2021; Taeihagh, 2021).

Relational risks stem from asymmetries in power and knowledge between stakeholders. When tech firms withhold training data, as in the case of OpenAI's GPT-4, or when users are denied explanations for algorithmic decisions, it undermines public trust in AI systems (Arora et al., 2023; Curchod et al., 2020). These risks are further amplified by global inequities, where AI development is concentrated in the Global North, leaving other regions vulnerable to technological dependency. Mitigating relational risks requires participatory governance mechanisms, such as involving civil society in standard-setting or

establishing transparency escrows that allow regulators to review proprietary data (Kashefi et al., 2024; OECD, 2024). Thus, the market logic prioritises control over intellectual property, while the governance logic demands openness and inclusivity (Markus, 2007; Henfridsson and Bygstad, 2013; Avital & Te'eni, 2009).

The three categories of risk shape regulatory responses. The EU's governance-oriented approach emphasises ex ante classification and public safety, while the US favours sectoral oversight that preserves innovation. China's model, meanwhile, aligns AI development with state ideology, prioritising control over transparency (McMorrow and Hu, 2024; Zhang, 2024). The UK's 'pro-innovation' framework attempts to bridge these logics by combining regulatory flexibility with statutory safeguards, such as sandboxes and accountability mandates (UK, 2023b).

Ultimately, a risk-informed regime must also clarify responsibility, with developers potentially held accountable for technical flaws, deployers for misuse, and regulators for systemic oversight failures. The UK's 'chain of accountability' model exemplifies this approach, requiring designated risk officers at each stage of deployment (Roberts et al., 2023). By aligning liability with institutional roles, this model aims to balance the demands of innovation with the imperatives of public trust and ethical governance (Schlagwein and Willcocks, 2023). Having outlined the types of risks posed and how they shape regulatory responses, we now turn to the question of how governance itself is structured. This next section contrasts two dominant paradigms, self-regulation and rules-based regulation, exploring their implications for AI oversight.

From self-regulation to sanctions: The governance dilemma

The governance of AI is increasingly defined by a fundamental tension between two competing regulatory paradigms: self-regulation and sanctions-based enforcement. This dilemma reflects market autonomy versus state oversight in how societies manage technological risk and innovation (Black, 2002).

Self-regulation has long been the preferred model in the tech industry, grounded in the belief that innovation thrives best under minimal interference. This approach empowers firms to develop voluntary codes of conduct, ethics boards, and internal compliance mechanisms. Organizations like the Partnership on AI and ISO (2024) standards exemplify this logic, promoting best practices without legal compulsion. Nonetheless, self-regulatory approaches have shown limitations, particularly in high-stakes or rapidly evolving domains. AI systems, particularly large language models (LLMs), routinely generate hallucinations and plausible but false outputs, due to biased training data or flawed reasoning (Roberts et al., 2024). These errors, while technically (somewhat) explainable, can have serious real-world consequences, especially in domains like healthcare, finance, or criminal justice (Hacker et al., 2023).

Moreover, professional associations that promote ethical AI often lack enforcement power. When members violate guidelines, the most severe penalty is reputational damage or expulsion, sanctions that rarely deter misconduct in high-stakes commercial environments (Sanchez and Middlemass, 2022). As a result, critics argue that self-regulation is insufficient for managing the systemic risks posed by AI, particularly when dominant firms have both the incentive and the capacity to shape regulatory discourse to their advantage (Grote et al., 2024; Zuboff, 2020).

Sanctions-based regulation relies on formal legal authority to enforce compliance. This model is exemplified by the EU's GDPR, which imposes fines of up to 4% of global revenue for violations by companies (GDPR, 2020). The EU AI Act extends this logic, introducing tiered penalties for non-compliance with risk-based AI classifications. Sanctions-based governance offers clear accountability and deterrence, but it also faces challenges. Regulatory agencies often lack the technical expertise to audit complex AI systems, and enforcement can be slow, reactive, and jurisdictionally fragmented (Currie et al., 2019; Manheim and Kaplan, 2019).

The two approaches to governance and regulation are further challenged by the widening gap between rapid technological change and the slower, more deliberate evolution of the regulatory system (Taeihagh, 2021). The autonomy and opacity of AI systems inhibit regulators' ability to anticipate harms or intervene proactively. This suggests that hybrid models that combine the agility of self-regulation with the authority of state oversight are likely to be more effective in regulating AI. To illustrate how governments position their operational strategies, Table 1 compares regulatory requirements at key stages of the AI lifecycle.

In the UK, this dilemma is demonstrated by the differences between the Government's ex-post pro-innovation approach (2023a) and the ex-ante private members' AI Bill, presented to the House of Lords (2023b). The Government favours flexibility over rigid rules. Rather than imposing blanket legislation, it focuses on existing regulators to adapt oversight within their sectors, guided by broad principles like safety, transparency, and fairness. The focus is on encouraging voluntary measures, international cooperation, and iterative adjustments before considering stricter future laws. These measures aim to embed ethical governance into corporate structures while preserving innovation flexibility (Roberts et al., 2023).

In contrast to the government's lighter-touch model, the AI Bill reflects growing pressure from Parliament and civil society to adopt a more formal statutory AI approach. It stipulates a new AI Authority, mandatory AI compliance

Table 1. AI lifecycle requirements across jurisdictions.

	EU (new regulation)	US (executive order)	UK govt (proposed regulation)	House of lords (AI bill)	China (strategic policy)
Pre-deployment	Conformity assessments for high-risk AI; CE marking; notified bodies	Mandatory red-teaming for dual-use models; compute thresholds; sectoral pilots (e.g., FDA)	Pro-innovation principles; sector-led risk assessments	Regulatory sandboxes; mandatory risk audits; AI officers	State approval for 'sensitive' domains; national security vetting
Transparency	Article 13: Explainability; user notification; logging requirements	Labelling of synthetic content; provenance standards; NIST AI RMF	Transparency encouraged via guidance; no statutory duty	Algorithmic passports; model documentation; public registers	Black-box models permitted if aligned with state goals; limited explainability required
Accountability	Fines up to 6% of global turnover; provider liability; post-market monitoring	Ex-post enforcement; civil rights investigations; agency-specific penalties	No central liability regime; relies on existing laws	Statutory presumption of causality; third-party audits; enforcement powers	Developer liability for 'harmful content'; state-enforced compliance
Participation	Multi-stakeholder AI board; public consultation on codes of conduct	Industry-led ethics boards; public-private partnerships	Sectoral regulators coordinate; limited public role	Public consultations required; AI authority oversight	State-directed public feedback mechanisms; limited civil society involvement

roles in businesses, and legally binding requirements around transparency, intellectual property, and public accountability. This approach is more cautious, centralised, and proactive, looking to define regulation from the start, rather than allowing it to evolve in a piecemeal fashion. The UK Government is not obligated to support or adopt bills presented to the House of Lords. Its purpose is to shape legislation, influence policy, and raise awareness. The US Executive Order on AI (2023) also reflects a precautionary, ex-ante approach, emphasising safety, security, and risk mitigation. Although both share features such as controlled environments for testing AI systems before full deployment, they differ significantly in scope, enforcement mechanisms, and regulatory philosophy.

The governance dilemma is not a binary choice but a spectrum. Effective AI regulation must balance innovation with accountability, recognising that neither self-regulation nor sanctions alone can address the full range of risks. A layered approach, combining internal governance, third-party audits, and statutory enforcement, offers the most promising path forward. This requires not only institutional coordination but also a shared understanding of risk, responsibility, and the public interest. While governance models vary in their reliance on market or

Table 2. AI risk levels identified by the EU.

AI level	Regulatory approach	Example
Unacceptable risk	Such practices are banned outright due to threats to rights or safety	Scraping of facial images to create recognition databases
High risk	If deemed a significant risk to health, safety, or fundamental rights system must comply with strict requirements	CV screening tools, medical diagnostics, border control AI
Limited risk	Transparency obligation requires users to be informed that they are interacting with AI	Chatbots must expose their AI nature unless obvious
Minimal or No risk	No regulatory constraints, but voluntary guidelines apply	AI in video games, spam filters, and photo editing tools

state mechanisms, a more fundamental shift is needed as risk is directly embedded into the design of regulatory policy. The following section explores how this can be achieved through anticipatory, adaptive, and participatory approaches.

Embedding risk in policy design

As AI systems become more complex, autonomous, and embedded in critical infrastructures, the need to integrate risk directly into policy design has become paramount. Traditional regulatory models, often reactive and sector-specific, are ill-equipped to manage the emergent, cross-sectoral risks posed by AI technologies (Grote et al., 2024; Taeihagh, 2021). Embedding risk into policy design requires a shift from static compliance frameworks to dynamic, anticipatory governance mechanisms that can evolve in tandem with technological innovation.

A risk-based approach to AI regulation begins with classification. The EU's AI Act exemplifies this by categorising AI system risk into four tiers, based on the potential harm that they may cause to health, safety, rights, democracy, the rule of law, and the environment (European Parliament, 2024). This is summarised in Table 2 below.

This model allows regulators to tailor oversight based on the potential impact of an AI system, rather than its technical architecture alone. However, such classification schemes must be flexible enough to accommodate evolving use cases and hybrid applications, such as general-purpose AI models that can be repurposed for high-risk tasks (Seidel et al., 2025).

Policy instruments must also reflect the relational and systemic nature of AI consequences. These tools embed risk management into the development lifecycle, enabling iterative learning and adaptive regulation (Roberts et al., 2023). Similarly, the OECD's AI principles emphasise transparency, robustness, and accountability as foundational elements of risk-aware governance (OECD, 2024).

Institutional design plays a critical role in operationalising risk-based regulation. Centralised authorities, such as the proposed UK AI Authority, can coordinate cross-sectoral oversight, reduce fragmentation, and ensure consistency in enforcement. However, effective risk governance also requires distributed expertise. Sectoral regulators, for example, finance, healthcare, or transportation, interpret and apply AI-specific rules within their domains, leveraging their contextual and operational knowledge (Currie et al., 2019; Marchant, 2011).

Stakeholder engagement is another pillar of risk-embedded policy. Public consultations, citizen juries, and participatory audits can unpack diverse perspectives on what constitutes harm, fairness, or acceptable trade-offs. This is particularly important for marginalised communities, who may be disproportionately affected by algorithmic bias or surveillance (Arora et al., 2023; Manheim and Kaplan, 2019). Embedding risk in policy design thus requires not only technical tools but also democratic processes that legitimise regulatory decisions.

Finally, international coordination is essential. AI systems often operate across borders, and inconsistent risk definitions or enforcement standards can lead to regulatory arbitrage. Initiatives like the OECD AI Policy Observatory and the Global Partnership on AI aim to harmonise risk frameworks and promote interoperability, but significant gaps remain (Tallberg et al., 2023).

Embedding risk in AI policy design is not a one-time exercise but an ongoing process of negotiation, adaptation, and institutional learning. It demands a multi-level governance architecture that integrates technical, legal, and ethical dimensions of risk, while remaining responsive to the evolving capabilities and societal impacts of AI. However, these systems operate globally, while regulation remains fragmented. The next section examines the global divergence in AI governance and the urgent need for harmonisation.

Global divergence and the need for harmonization

The global landscape of AI regulation is marked by significant divergence, with jurisdictions adopting distinct approaches shaped by their institutional structures, political priorities, and economic strategies (see Table 1). This regulatory fragmentation poses a major challenge for multinational AI developers and policymakers alike, as inconsistent standards create compliance uncertainty, hinder innovation, and undermine efforts to manage cross-border risks (Manheim and Kaplan, 2019; Tallberg et al., 2023).

In the EU, a precautionary governance logic dominates (Novelli et al., 2024). The EU AI Act adopts a rights-based, risk-tiered framework that emphasises human oversight, transparency, and fundamental rights. It prohibits certain applications outright, such as social scoring, and imposes strict obligations on high-risk systems, including documentation, testing, and post-market monitoring (European Parliament, 2024). This model reflects the EU's broader commitment to digital sovereignty and ethical technology development.

By contrast, the US has embraced a market-driven, sectoral approach. Federal regulation remains fragmented across agencies like the Federal Trade Commission (FTC), Food and Drug Administration (FDA), and NIST, while states such as California and Illinois have introduced their own AI and data privacy laws. The Biden administration's 2023 Executive Order on AI signals a shift toward more centralised oversight, but the US continues to prioritise innovation and competitiveness, often relying on voluntary

Table 3. Case examples.

EU AI Act Article 6: Risk Tiering in Practice
Article 6 of the EU AI Act operationalizes risk-based regulation by classifying AI systems into four tiers: Unacceptable, high, limited, and minimal risk. This tiering determines a level of scrutiny, but this has sparked debate over scope creep and enforcement feasibility for general-purpose AI models (European Union, 2025)
UK AI Sandbox Clause (House of Lords Bill): Anticipatory Regulation
The AI bill was reintroduced to parliament on 4 March 2025 by Lord Holmes. This introduces regulatory sandboxes, controlled environments for testing high-risk AI systems under supervision. This anticipatory governance tool allows regulators to assess real-world impacts while enabling innovation. It reflects a shift from reactive to experimental policymaking (Osborne Clarke, 2025)
Industry CEO Letter (June 2025): Political Economy of Risk
In June 2025, 44 European tech CEOs signed an open letter urging a pause to the EU AI Act, citing concerns over innovation stifling and compliance burdens. The letter highlights structural tensions between regulatory ambition and industrial competitiveness (FT, 2025)

frameworks and industry self-regulation (Currie et al., 2019; US Federal Register, 2023).

To illustrate how regulatory philosophies are being operationalised, Table 3 presents case studies that illustrate the tensions and trade-offs in current AI governance. These three examples highlight the practical implications of regulatory design. Together, they underscore the political, institutional, and economic dynamics shaping AI oversight in Europe and beyond.

China's model reflects a state-centric logic, combining rapid AI development with strong ideological control. While the Cyberspace Administration of China (CAC) mandates algorithmic transparency and content moderation, this transparency is tightly controlled and aligned with state ideology, particularly the enforcement of 'core socialist values'. As such, China's regulatory model prioritises control over open accountability, using transparency as a tool of governance rather than public empowerment (China State Council, 2017; McMorrow and Hu, 2024). While China leads in AI deployment, its regulatory approach is tightly integrated with national security and censorship objectives, raising concerns about surveillance and digital authoritarianism.

These divergent models create a compliance minefield for global AI firms (see Table 2). A system deemed compliant in one jurisdiction may be banned or heavily restricted in another. For example, facial recognition technologies are widely used in China, cautiously regulated in the US, and largely prohibited in the EU. This lack of harmonisation not only increases operational costs but also risks regulatory arbitrage, where firms exploit weaker regimes to deploy high-risk systems (Kashefi et al., 2024).

Efforts to bridge these divides are underway. Initiatives like the OECD AI Principles and the Global Partnership on AI (GPAI) advocate for common values such as transparency, accountability, and a human-centric approach to AI development (OECD, 2024). However, these initiatives remain non-binding, and geopolitical tensions often hinder

Table 4. Regulatory archetypes comparison.

	EU (new regulation)	US (executive order)	UK govt (proposed regulation)	House of lords (AI bill)	China (strategic policy)
Core priority	Fundamental rights, safety, and trust	Innovation, national security, and competitiveness	Innovation-first, sector-led regulation	Public safety, fairness, and accountability	National rejuvenation, ideological alignment
Risk approach	Ex-ante bans (e.g., social scoring); tiered risk classification	Ex-post oversight; red-teaming for dual-use models	Ex-post, contextual, non-statutory risk-based principles	Ex-ante, statutory duties for high-risk AI; mandatory audits	State-led approvals for 'sensitive' domains; strategic sectors prioritized
Transparency	Mandatory for high-risk AI; user notification; logging	Voluntary (except for dual-use and healthcare); provenance labelling	Encouraged via guidance; no legal obligation	Algorithmic passports; public registers; explainability duties	Required for private firms; state actors exempt
Enforcement	Fines up to 6% of global turnover; CE marking; post-market monitoring	FTC, DOJ, and agency-specific penalties; export controls	No central enforcement body; relies on existing regulators	AI authority with investigatory powers; statutory liability presumption	Political censure, license revocation, and national security enforcement

deeper cooperation. The UK's AI (Regulation) Bill (2023b) attempts to position the country as a regulatory intermediary, combining innovation-friendly oversight with ethical safeguards and interoperability with international frameworks.

To move toward harmonisation, policymakers must prioritise interoperability over uniformity. This means aligning core principles, such as risk classification, auditability, and redress mechanisms, while allowing flexibility in implementation. Mutual recognition agreements, joint regulatory sandboxes, and cross-border audit protocols could facilitate trust and reduce duplication. Moreover, global standards bodies like ISO and IEEE can play a critical role in codifying technical norms that transcend national boundaries (ISO, 2024).

Ultimately, harmonisation is not about erasing differences but about creating a coherent global governance architecture that enables responsible AI innovation while safeguarding fundamental rights. As AI systems increasingly operate across borders, the need for coordinated, risk-based, and inclusive regulation becomes not just desirable but essential. To further clarify how different jurisdictions operationalise their AI governance philosophies, Table 4 compares different regulatory frameworks (the EU, U.S, UK, and China) across four key dimensions: core priority, risk approach, transparency, and enforcement.

The Core Priority of the EU is to prioritise fundamental rights, safety, and trust, demonstrating its rights-based regulatory tradition. In contrast, the US focuses on innovation and national security, while China aligns AI development with ideological goals. The UK Government and House of Lords differ slightly, with the former emphasising innovation and the latter public accountability.

The Risk Approach adopted by the EU is a tiered, ex-ante risk classification system, banning certain applications outright. The US relies on ex-post oversight, while the UK Government uses non-statutory principles (contrary to the House of Lords), whilst China enforces state-led approvals for sensitive domains.

Transparency obligations vary widely. The EU mandates explainability and logging for high-risk AI, while the US and UK Government rely on voluntary guidance. The House of Lords proposes algorithmic passports and public registers, whereas China requires transparency only for private firms, exempting state actors.

Enforcement mechanisms range from the EU's strict fines and CE marking to the US's agency-specific penalties. The UK Government lacks a central enforcement body, while the House of Lords proposes an AI Authority. China enforces compliance through political and national security channels.

Areas for future research

This editorial reframes AI regulation as a socio-technical governance challenge, proposing a risk-informed framework that integrates institutional theory, digital infrastructure evolution, and participatory oversight. It demonstrates AI systems transcend their technical dimensions to become institutional forces that actively reshape governance structures, market dynamics, and technological paradigms (Friedland and Alford, 1991; Grote et al., 2024). These complex interactions create fundamental tensions between fostering innovation and ensuring accountability, between transparency requirements and proprietary interests, and between national regulatory sovereignty and the need for global interoperability, that existing legal frameworks struggle to reconcile (Easterbrook, 1996). Moving forward, IS research is well-positioned to engage with several critical dimensions of AI governance and policymaking.

First, the field requires robust frameworks for dynamic risk assessment that can account for AI systems' evolving capabilities post-deployment (Judge et al., 2025; Taeihagh, 2021). This includes developing sophisticated mechanisms for contextual risk calibration that recognise how risk profiles transform across different application domains, from healthcare diagnostics to entertainment platforms (Buiten, 2019; Hacker et al., 2023), while bridging technical assessment methods with institutional theories of regulatory adaptation (Marchant, 2011).

Equally important is understanding the enforcement gap in AI governance. Research should examine the conditions under which various sanctions, from financial penalties to litigation, effectively modify behaviour in the AI sector (GDPR, 2020; Roberts et al., 2023), while investigating how emerging compliance professions like AI auditors and ethics officers institutionalise accountability within organisational structures (Currie et al., 2019; UK, 2023b). Such studies could reveal new pathways for aligning policy intentions with practical implementation (Berente et al., 2021).

The democratization of AI governance demands urgent scholarly attention, particularly regarding which participatory models most effectively incorporate diverse societal values into regulatory processes (Kashefi et al., 2024; Manheim and Kaplan, 2019). Research must prioritize marginalised perspectives (Arora et al., 2023), challenging conventional assumptions about expertise and representation in technical governance systems (Zuboff, 2015).

At the transnational level, comparative research should identify interoperability mechanisms that facilitate coordination without imposing artificial homogeneity across jurisdictions (OECD, 2024). These investigations must account for geopolitical realities (Zhang, 2024), particularly how national security concerns and economic competition shape, and often constrain, harmonisation efforts (Tallberg

et al., 2023), while drawing lessons from existing transnational governance regimes (Seidel et al., 2025).

Addressing these multifaceted challenges requires breaking down disciplinary silos through innovative research approaches. Longitudinal studies tracking regulatory experiments like sandboxes (UK, 2023b), methodological hybrids combining computational analysis with institutional ethnography (Berente et al., 2021), and critical examinations of power dynamics in standard-setting bodies (Grote et al., 2024) all represent promising directions. Without such robust, interdisciplinary research to inform policy development (OECD, 2023), there is a possibility of oscillating between overly cautious regulation and insufficient governance structures in this critical domain.

This editorial sets the stage for the Journal of Information Technology's special issue on 'Policymaking for Emerging Technology: Governance, Risk and Ethics', which seeks work on a risk-informed, socio-technical approach to AI governance and policymaking, and aims to stimulate interdisciplinary dialogue on how institutions adapt to the challenges posed by emerging technology.

References

Analytics Insight (2024) *The Most Controversial AI Decisions in Recent Years*. https://www.analyticsinsight.net/artificial-intelligence/the-most-controversial-ai-decisions-in-recent-years

Arora A, Barrett AM, Lee E, et al. (2023) Risk and the future of AI: algorithmic bias, data colonialism, and marginalization. *Information and Organization* 33(3): 100478.

Avital M and Te'eni D (2009) From generative fit to generative capacity: exploring an emerging dimension of information systems design and task performance. *Information Systems Journal* 19(4): 345–367.

Berente N, Gu B, Recker J, et al. (2021) Managing AI. *MIS Quarterly* 45(3): 1433–1450.

Black J (2002) Regulatory conversations. *Journal of Law and Society* 29(1): 163–196.

Buiten MC (2019) Towards intelligent regulation of artificial intelligence. *European Journal of Risk Regulation* 10: 41–59.

China State Council (2017) *China's 'New Generation Artificial Intelligence Development Plan'*. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

Curchod C, Patriotta G, Cohen L, et al. (2020) Working for an algorithm: power asymmetries and agency in online work settings. *Administrative Science Quarterly* 65(3): 644–676.

Currie WL and Seddon JJM (2021) Exploring technological instantiation of regulatory practices in entangled financial markets. *Journal of Information Technology* 37(1): 31–50.

Currie WL, Gozman DP and Seddon JJM (2019) Dialectic tensions in the financial markets: a longitudinal study of pre- and post-crisis regulatory technology. *Journal of Information Technology* 33(4): 304–321.

Easterbrook FA (1996) *Cyberspace and the Law of the Horse*. University of Chicago Legal Forum, Vol. 207.

European Parliament (2024) *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*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

European Union (2025) *Article 6: Classification Rules for High-Risk AI Systems*. https://artificialintelligenceact.eu/article/6/

Friedland R and Alford RA (1991) Bringing society back in: symbols, practices, and institutional contradictions. In: Powell WW and DiMaggio P (eds) *The New Institutionalism in Organizational Analysis*. Chicago: University of Chicago Press, 232–263.

FT (2025) *European CEOs Urge Brussels to Halt Landmark AI Act*. https://www.ft.com/content/a825759e-aec8-4184-bc73-f604f169204c

GDPR (2020) *General Data Protection Regulation (GDPR)*. GDPR.EU. https://gdpr-info.eu/

GPDP (2024) *Artificial Intelligence: Stop to ChatGPT by the Italian SA Personal Data is Collected Unlawfully, No Age Verification System is in Place for Children*. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847#english

Grote G, Parker SK and Crowston K (2024) Taming artificial intelligence: a theory of control-accountability alignment among AI developers and users. In: *Academy of Management Review*. Academy of Management: 1–22. Advance online publication.

Hacker P, Engel A and Mauer M (2023) Regulating ChatGPT and other large generative AI models. *FAccT* 23(June): 12–15.

Haenlein M and Kaplan A (2019) A brief history of artificial intelligence: on the past, present, and future of artificial intelligence. *California Management Review* 61: 14–15.

Henfridsson O and Bygstad B (2013) The generative mechanisms of digital infrastructure evolution. *MIS Quarterly* 37(3): 907–931.

ISO (2024) *'What is Artificial Intelligence (AI)?'*.

Jacobides MG and Lianos I (2021) Ecosystems and competition law in theory and practice. Available at SSRN: https://ssrn.com/abstract=3772366 or https://doi.org/10.2139/ssrn.3772366

Judge B, Nitzberg M and Russell S (2025) When code is not law: rethinking regulation for artificial intelligence. *Policy and Society* 44(1): 85–97.

Kashefi P, Kashefi Y and Mirsaraei A (2024) Shaping the future of AI: balancing innovation and ethics in global regulation. *Uniform Law Review* 29(3): 524–548.

Manheim K and Kaplan L (2019) Artificial intelligence: risks to privacy and democracy. *The Yale Journal of Law and Technology* 21: 106–188.

Marchant GE (2011) The growing gap between emerging technologies and the law. In: *The International Library of Ethics, Law, and Technology*. Springer, Vol. 7: 19–33.

Markus ML (2007) The governance of free/open-source software projects: monolithic, multidimensional, or configurational? *Journal of Management & Governance* 11: 151–163.

Maslej N, Fattorini L, Perrault R, et al. (2024) Artificial Intelligence Index Report. Available at: https://doi.org/10.48550/arXiv.2405.19522

McKinley W (2022) Doomsdays and new dawns: technological discontinuities and competence ecosystems. *Academy of Management Perspectives* 36(2): 729–743.

McMorrow R and Hu T (2024) China deploys censors to create socialist AI. Available at: https://www.ft.com/content/10975044-f194-4513-857b-e17491d2a9e9

Novelli C, Casolari F, Rotolo A, et al. (2024) AI risk assessment: a scenario-based, proportional methodology for the AI act. *Digital Society* 3(13): 13.

OECD (2023) *Initial Policy Considerations for Generative Artificial Intelligence*. OECD Report. September, No. 1.

OECD (2024) *Global Partnership on Artificial Intelligence*. https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html

Osborne Clarke (2025) *Artificial Intelligence|UK Regulatory Outlook March 2025*. https://www.osborneclarke.com/insights/Regulatory-Outlook-March-2025-Artificial-intelligence

Roberts H, Babuta A, Morley J, et al. (2023) Artificial intelligence regulation in the United Kingdom: a path to good governance and global leadership? *Internet Policy Review* 12(2). Available at: https://policyreview.info/articles/analysis/artificial-intelligence-regulation-united-kingdom-path-good-governance.

Roberts H, Babuta A, Morley J, et al. (2024) Artificial intelligence and qualitative research: the promise and perils of large language model (LLM) 'assistance'. *Critical Perspectives on Accounting* 99. https://doi.org/10.1016/j.cpa.2024.102722

Sanchez GR and Middlemass K (2022) Misinformation is eroding the public's confidence in democracy. Available at: https://www.brookings.edu/articles/misinformation-is-eroding-the-publics-confidence-in-democracy/

Schlagwein D, Willcocks L, ChatGPT, et al. (2023) The ethics of using (generative) artificial intelligence in research and science. *Journal of Information Technology* 38(3): 232–238.

Seidel S, Frick CJ and vom Brocke J (2025) Regulating emerging technologies: prospective sensemaking through abstraction and elaboration. *MIS Quarterly* 41(1): 179–204.

Taeihagh A (2021) Governance of artificial intelligence. *Policy and Society* 40(2): 137–157.

Tallberg J, Erman E, Furendal M, et al. (2023) Global governance of artificial intelligence: next steps for empirical and normative research. *International Studies Review* 25(3). Available at: https://doi.org/10.1093/isr/viad040

UK (2023a) *A Pro-Innovation Approach to AI Regulation*. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

UK (2023b) *Artificial Intelligence (Regulation) Bill [HL]*. https://bills.parliament.uk/publications/53068/documents/4030

US Federal Register (2023) Fact sheet: president Biden issues executive order on safe, secure, and trustworthy artificial intelligence. *Federal Register* 88(210): 75191–75226. https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

Vaccari C and Chadwick A (2020) Deepfakes and disinformation: exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society* 6: 1–13.

Zhang A (2024) *The Promise and Perils of China's Regulation of AI*. University of Hong Kong Faculty of Law.

Zhang H, Dao D, Bowden J, et al. (2025) *Large Language Model Application for Regulatory Horizon Scanning: Case Study on Anti-Greenwashing Regulations*. University of Strathclyde.

Zuboff S (2015) Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30(1): 75–89.