

Editorial Call for Papers: Special Issue on AI Governance, Cybersecurity Law, and Digital Rights

Type of article: Editorial

Abdeldjalil Khelassi^{1,2}, S M Nazmuz Sakib³

1 Editor-in-Chief of Medical Technologies Journal, Knowledge Kingdom Publishing

2 Associate Professor, University of Tlemcen

3 Fellow, Scholars Academic and Scientific Society, H.No-204, Borhawor, P.S-Murajhar, Dist- Hojai, Assam-782439, India

Abstract

The rapid proliferation of artificial intelligence systems, large language models, and autonomous decision-making tools across critical societal domains has created an urgent and growing demand for coherent, evidence-based legal scholarship. Existing regulatory regimes across different jurisdictions respond to these challenges with markedly divergent approaches: the European Union has pioneered a risk-tiered horizontal framework through its AI Act, while jurisdictions such as the United States, India, Singapore, and the Gulf Cooperation Council states pursue sectoral, innovation-forward governance strategies. This Editorial introduces the *Medical Technologies Journal* (MTJ) Special Issue dedicated to *AI Governance, Cybersecurity Law, and Digital Rights: Comparative Regulatory Frameworks Across Jurisdictions*. Against the backdrop of a decade since the adoption of the General Data Protection Regulation (GDPR) and with the EU AI Act entering its phased implementation cycle, this issue aims to generate scholarship that moves beyond descriptive doctrine to quantifiable, empirically grounded assessments of regulatory efficacy, enforcement gaps, and cross-border digital rights outcomes.

Keywords: AI Governance, Cybersecurity Law, Digital Rights, Comparative Regulatory Frameworks, Data Protection, Smart Contracts, Intellectual Property.

Corresponding author: Abdeldjalil KHELASSI, Abou Bekr Belkaid University of Tlemcen, Algeria.
Email: khelassi.a@gmail.com.

© 2026 KNOWLEDGE KINGDOM PUBLISHING

1. Introduction

The rapid proliferation of artificial intelligence systems, large language models, and autonomous decision-making tools across critical societal domains has created an urgent and growing demand for coherent, evidence-based legal scholarship. Existing regulatory regimes across different jurisdictions respond to these challenges with markedly divergent approaches: the European Union has pioneered a risk-tiered horizontal framework through its AI Act, while jurisdictions such as the United States, India, Singapore, and the Gulf Cooperation Council states pursue sectoral, innovation-forward governance strategies. This Special Issue invites rigorous comparative legal analysis of these divergent trajectories and their policy implications.

Against the backdrop of a decade since the adoption of the General Data Protection Regulation (GDPR) and with the EU AI Act entering its phased implementation cycle, this issue aims to generate scholarship that moves beyond descriptive doctrine to quantifiable, empirically grounded assessments of regulatory efficacy, enforcement gaps, and cross-border digital rights outcomes.

2. Theoretical and Methodological Foundations

Submissions to this Special Issue are encouraged to adopt one or more of the following methodological orientations, reflecting the interdisciplinary demands of contemporary digital law scholarship:

- **Comparative Regulatory Analysis:** Systematic side-by-side evaluation of statutory texts, enforcement records, and judicial interpretations across at least two distinct legal systems or economic blocs.
- **Empirical Legal Studies:** Quantitative or mixed-methods research drawing on litigation data, regulatory filings, incident reports, or survey instruments to ground legal claims in measurable outcomes.
- **Doctrinal Reconstruction:** Close textual analysis of emerging statutes, court decisions, and soft-law instruments to identify internal coherence, interpretive gaps, and reform pathways.
- **Law and Technology Integration:** Studies that combine legal analysis with technical knowledge of AI, cryptography, distributed systems, or cybersecurity to evaluate the technical feasibility of proposed legal obligations.

3. Significance and Relevance

This issue responds directly to active calls for comparative legal scholarship on AI and digital governance identified in the Annual Privacy Forum (APF 2026), the New York Law School AI and Data Law Summit. This issue is positioned to capture and evaluate regulatory developments in the final quarter of 2027, including scheduled AI Act compliance deadlines, the anticipated G7 AI code of conduct review cycle, and national data protection reform processes underway in South and Southeast Asia.

4. Scope and Taxonomy of Invited Submissions

This Special Issue is grounded in current and active scholarly debates identified across leading law journals, including *Computer Law and Security Review*, the *Journal of AI Law and Regulation* (AIRE), and *Columbia Journal of Environmental Law*. It targets the following intersecting areas of inquiry:

- **AI Governance and Regulatory Benchmarking:** Comparative mapping of the EU AI Act, the US AI Bill of Rights Blueprint, China AI governance directives, and ASEAN Guidance on AI Governance, with particular focus on enforcement architecture and liability allocation for foundation models and general-purpose AI systems.
- **Medical Technologies and Healthcare Law Regulation:** Legal, ethical, and regulatory frameworks governing medical devices, AI-driven diagnostic software (SaMD), algorithmic clinical decision-support tools, robotic surgery systems, and digital health interventions. Submissions may address post-market surveillance obligations, liability for AI-driven clinical errors, software-as-a-medical-device compliance, and cross-border regulatory alignment for health technologies.
- **Cybersecurity Law and Network Security Regulation:** Legal frameworks governing cybersecurity incident reporting, critical infrastructure protection, and the emerging intersection of AI-driven malware detection with national and transnational law. Submissions may address regulatory gaps in AI-specific vulnerability management, algorithmic bias liabilities, and model drift in critical network operations.
- **Data Protection and Digital Rights:** Post-GDPR developments in data sovereignty, cross-border data flows, and the regulation of biometric and health data under diverse legal traditions. Contributions may examine how privacy-preserving AI architectures interact with national data protection mandates.

- **Smart Contracts and Blockchain in Legal Systems:** Legal recognition, enforceability, and regulatory treatment of blockchain-based smart contracts across civil law and common law jurisdictions, with attention to supply chain transparency, automated compliance mechanisms, and decentralised finance regulation.
- **International Law and Emerging Technology:** The application of public international law principles to cyberspace, including sovereignty, attribution, non-intervention, and the extraterritorial reach of domestic digital regulations.
- **Patent Law and Intellectual Property in the AI Invention Cycle:** Legal questions arising from AI-assisted and AI-generated inventions, including inventorship doctrine, patentability thresholds, and cross-border IP enforcement in the context of machine learning patent filings.

5. Target Audience

- Legal scholars specialising in technology law, international law, and comparative constitutional law.
- Regulators and policy analysts at national data protection authorities and AI governance agencies.
- Practitioners in technology law firms, in-house legal teams at AI companies, and compliance officers in financial services and healthcare sectors.
- Interdisciplinary researchers at the intersection of computer science, economics, and law.

6. Operational Timeline and Review Process

Phase	Milestone	Target Date
Phase 1	Call for Papers Opens	1 August 2026
Phase 2	Full Manuscript Submission Deadline	30 April 2027
Phase 3	Double-Blind Peer Review	1 May–15 July 2027
Phase 4	First-Round Decisions	31 July 2027
Phase 5	Revised Manuscript Submission Deadline	15 September 2027
Phase 6	Final Editorial Decisions and Proofs	15 November 2027
Phase 7	Publication of the Special Issue	15 December 2027

7. Call to Action

The rapid evolution of digital governance, cybersecurity law, and AI frameworks demands rigorous, peer-reviewed legal scholarship that connects comparative jurisprudence with technological reality. By providing an open-access, *Medical Technologies Journal* seeks to advance cross-border regulatory

discourse and offer clear policy pathways for the future of digital rights. We invite legal scholars, technical researchers, and policy experts to contribute their work to this Special Issue.

8. Guest Editor Credentials

Engr. Dr. S M Nazmuz Sakib (CMSA, FPWMP, FTIP, BIDA, FMVA, CBCA) is a Professor of Science in Research and Development holding qualifications in law (Bachelor of Laws with Honours, Dhaka International University), engineering (BEng in Information Technology), and business administration (DBA, MBA). His published legal and interdisciplinary scholarship includes contributions on the 2003 US intervention in Iraq and global security dynamics (*Springer Nature Handbook of Migration, International Relations and Security in Asia*), blockchain technology for smart contracts (*CRC Press*), and the sociology and culture of South Asia (*Simulacra*). He holds active designations as a FinTech Industry Professional (FTIP) and Capital Markets and Securities Analyst (CMSA) from the Corporate Finance Institute, and serves on editorial boards spanning toxicology, environmental monitoring, and mathematics education. His patent portfolio includes registered designs in Germany, India, the United Kingdom, and Australia in domains from network security to medical devices, underscoring a direct engagement with the practical intersection of intellectual property law and technological invention.