



Cyber Law and Digital Transformation: Addressing Emerging Legal Issues in the Global Information Era

Ardiana¹, Gilang Rizki Aji Putra²

¹ Pancasila University, Indonesia. E-mail: ardiana@gmail.com

² Syarif Hidayatullah State Islamic University Jakarta, Indonesia. E-mail: gilangrizkiajiputa0@gmail.com

ABSTRACT

The rapid proliferation of digital technologies has outpaced the capacity of traditional legal frameworks to govern cyberspace, creating a global governance deficit with profound implications for cybersecurity, data protection, and cross-border cooperation. This study examines the emerging legal issues arising from digital transformation and evaluates the adequacy of contemporary cyber law responses at national, regional, and international levels. Drawing on a normative juridical methodology with a descriptive-analytical approach, the research synthesizes regulatory developments across multiple jurisdictions, including the European Union's Artificial Intelligence Act and Digital Services Act, the United Nations Convention against Cybercrime (Hanoi Convention), the Budapest Convention and its Protocols, and emerging digital trade agreements such as the ASEAN Digital Economy Framework Agreement and the Digital Economy Partnership Agreement. The analysis reveals a persistent tension between regulatory fragmentation and the inherently borderless nature of digital technologies, compounded by asymmetries in enforcement capacity between developed and developing nations. Findings indicate that while significant normative advances have been achieved—particularly in AI risk classification, cross-border data transfer mechanisms, and international cybercrime cooperation—critical gaps remain in liability attribution for autonomous systems, quantum-era cryptographic governance, and the operationalization of legal pluralism in cyberspace. The study contributes a conceptual framework for understanding cyber law as a dynamic, multi-level governance system that must balance innovation, sovereignty, and fundamental rights. Practical implications for policymakers, regulators, and international organizations are discussed, alongside recommendations for harmonizing legal standards without undermining legitimate regulatory diversity.

Keywords: Artificial Intelligence Regulation, Cross-Border Data Flows, Cybercrime Convention, Digital Sovereignty, Digital Transformation, International Cooperation, Legal Harmonization, Platform Liability

Citation: Ardiana and Putra, Rizki Aji Putra. 2024. "Cyber Law and Digital Transformation: Addressing Emerging Legal Issues in the Global Information Era". *JLCS: Journal of Law and Cultural Studies* 2 (1), 1-18. <https://doi.org/10.30872/jlcs.v1i2.1>.

1. INTRODUCTION

The global information era has fundamentally reconfigured the relationship between law and technology. Digital transformation—encompassing artificial intelligence, cloud computing, the Internet of Things, and blockchain technologies—has generated unprecedented economic and social value while simultaneously exposing the limitations of legal frameworks designed for a pre-digital world. The World Economic

Forum estimates annual global losses from cybercrime at approximately USD 10.5 trillion by 2025, with projections rising to USD 15.63 trillion by 2029. These figures underscore a fundamental governance deficit: the technological substrate of the global economy is evolving at a pace that legal institutions, which operate through deliberative and incremental processes, struggle to match.

The challenge is not merely one of regulatory speed. Digital technologies are inherently extraterritorial, operating across jurisdictional boundaries with minimal regard for national legal demarcations. This creates what scholars have characterized as a "law lag"—a structural mismatch between the spatial logic of digital networks and the territorial logic of legal systems (Reed, 2012; Murray, 2019). The problem is compounded by the emergence of autonomous systems capable of making decisions without direct human intervention, raising novel questions of liability, accountability, and legal personhood that existing doctrinal frameworks were never designed to address (Floridi, 2018; Hallevey, 2020). The European Union's Artificial Intelligence Act, which entered into force in August 2024 and has been phasing in its provisions since February 2025, represents the most ambitious attempt to date to construct a comprehensive regulatory architecture for AI, yet its extraterritorial reach and risk-based classification model have generated significant debate regarding their global impact and coherence with other national approaches.

Three interrelated developments frame the contemporary governance landscape. First, the negotiation and signing of the United Nations Convention against Cybercrime—the Hanoi Convention—in October 2025 marked the culmination of nearly three years of contentious multilateral negotiations involving over 150 nations. The Convention seeks to harmonize national laws, enhance cross-border investigations, and facilitate electronic evidence sharing, yet it was adopted amid concerns about human rights safeguards and potential misuse to curb free expression. Second, the proliferation of regional and bilateral digital trade agreements—including the ASEAN Digital Economy Framework Agreement (DEFA), which reached substantial conclusion in October 2025, and the Digital Economy Partnership Agreement (DEPA) initiated by Singapore, Chile, and New Zealand—has created a complex patchwork of data governance norms that is increasingly difficult for businesses and regulators to navigate. Third, the emergence of digital sovereignty as a guiding policy principle has driven a wave of data localization mandates and cloud sovereignty frameworks, particularly in the Asia-Pacific region, raising questions about the long-term viability of the open internet as a unified legal space.

The theoretical foundation for examining these developments draws on several established traditions in cyber law scholarship. Lawrence Lessig's influential "code as law" thesis posits that the architecture of digital systems exercises a regulatory function that operates alongside and sometimes in tension with formal legal rules (Lessig, 1999/2006). This insight remains foundational for understanding how technical standards, algorithmic decision-making, and platform design choices shape behavior in ways that traditional legal instruments cannot fully capture. Complementing Lessig's framework, Andrew Murray's active matrix model emphasizes the dynamic interplay

between technological and social forces in shaping regulatory outcomes, rejecting both technological determinism and pure social constructivism (Murray, 2013). More recently, scholars have advanced the concept of "legal pluralism" in cyberspace, recognizing that multiple normative orders—state law, platform governance, technical protocols, and transnational private standards—coexist and compete within the digital domain (Schulz, 2020; Gikay, 2020). The work of the European Commission's High-Level Expert Group on AI further articulated a human-centric approach that positions fundamental rights at the center of digital governance, an approach that has influenced the design of the EU AI Act and the Council of Europe's Framework Convention on AI (European Commission, 2019).

The literature on cyber law and digital transformation reveals several critical research gaps. First, while a substantial body of scholarship examines individual regulatory domains—data protection, cybersecurity, AI governance, and platform liability—there is insufficient integration across these domains. Regulatory developments in one area frequently create unintended consequences in others, yet few studies systematically analyze these cross-domain interactions. Second, the overwhelming focus on EU and US regulatory frameworks has left the experiences of developing countries and emerging economies underexamined, despite the fact that these jurisdictions are home to a majority of the world's internet users and are often the primary targets of cybercrime and digital exploitation (Gikay, 2020). Third, the relationship between legal harmonization efforts and legitimate regulatory diversity remains poorly theorized. The tension between the push for global standards and the legitimate desire of nations to shape digital governance according to their own constitutional traditions, cultural values, and developmental priorities requires more nuanced analysis than the simple binary of "fragmentation versus harmonization" that dominates much policy discourse.

This study addresses these gaps by developing an integrated analytical framework for understanding cyber law as a multi-level governance system. The central research questions are: (1) What are the most significant emerging legal issues arising from digital transformation in the global information era? (2) How adequate are contemporary legal frameworks at national, regional, and international levels in addressing these issues? (3) What are the principal tensions and trade-offs that characterize efforts to harmonize cyber law across jurisdictions? (4) How can legal frameworks be designed to balance the imperatives of innovation, security, and fundamental rights?

The significance of this study lies in its integration of regulatory developments across multiple domains and jurisdictions into a coherent analytical framework. By examining cybersecurity, AI governance, data protection, platform liability, and international cooperation as interconnected elements of a single governance system, the research provides a more holistic understanding than domain-specific analyses can offer. The findings have implications for policymakers, regulators, and international organizations engaged in designing and implementing cyber law frameworks, as well as

for scholars seeking to understand the evolving relationship between law and digital technology.

2. LITERATURE REVIEW

2.1 Theoretical Foundations of Cyber Law

The scholarly foundations of cyber law were laid in the late 1990s through debates about whether cyberspace constituted a distinct jurisdictional space requiring its own legal regime or whether existing legal principles could be extended to the digital domain. John Perry Barlow's "Declaration of the Independence of Cyberspace" (1996) famously asserted that cyberspace was a sovereign realm beyond the reach of territorial governments, a position that subsequent scholarship has largely rejected as empirically untenable and normatively problematic (Lessig, 1999; Goldsmith & Wu, 2006). Lessig's counterargument—that cyberspace is not inherently unregulable but rather is regulated by its architectural code in ways that may be less visible than traditional law—established the intellectual framework for subsequent scholarship on internet governance (Lessig, 2006).

Lessig's model identifies four modalities of regulation: law, social norms, markets, and architecture (or "code"). In the digital context, architecture refers to the technical standards, protocols, and software configurations that determine what users can and cannot do. The regulatory power of architecture is exercised through design choices—what data is collected, how systems are configured, what default settings are applied—that are often made by private actors with limited public accountability. This insight has been extended by scholars examining platform governance (Gillespie, 2018), algorithmic regulation (Yeung, 2018), and the political economy of digital infrastructure (Plantin et al., 2018).

Murray's active matrix model offers a more dynamic account of the relationship between law and technology, emphasizing the recursive interactions between legal rules, technological affordances, and user practices (Murray, 2013). Murray argues that neither technology nor law can be understood as determining the other; rather, they co-evolve through ongoing processes of adaptation and mutual adjustment. This perspective is particularly relevant for understanding contemporary regulatory challenges, where the rapid pace of technological change requires legal frameworks that are themselves adaptive and iterative.

2.2 Cybersecurity Regulation and Critical Infrastructure Protection

The regulatory response to cybersecurity threats has evolved significantly over the past two decades. Early approaches focused primarily on criminalizing unauthorized access to computer systems and establishing basic security requirements for critical infrastructure. More recent frameworks have adopted proactive, risk-based approaches that emphasize resilience, incident reporting, and supply chain security. The EU's Network and Information Systems Directive (NIS2), the Digital Operational Resilience Act (DORA), and the Cyber Resilience Act represent this evolution toward comprehensive, cross-sectoral cybersecurity regulation (European Commission, 2020;

2022). In the United States, the Strengthening American Cybersecurity Act and the Cyber Incident Reporting for Critical Infrastructure Act similarly reflect a shift toward mandatory incident reporting and proactive risk management (Ramli et al., 2026).

Developing countries have adopted diverse approaches to cybersecurity regulation, often shaped by their position in global digital supply chains and their institutional capacities. Indonesia's Cybersecurity and Cyber Resilience Bill (RUU KKS), included in the 2025 National Legislation Program, addresses a persistent gap in comprehensive legal frameworks and seeks to establish institutional coordination mechanisms, security standards for digital infrastructure, and mandatory incident reporting requirements. Zambia's Cyber Security Act and Cyber Crimes Act of 2025 establish frameworks for both cybersecurity governance and cybercrime prosecution, including provisions for data localization and online child protection. Vietnam's draft Cybersecurity Law 2025 includes provisions encouraging domestic cybersecurity products to enhance self-reliance. These national developments reflect broader patterns in cybersecurity regulation: the expansion of regulatory scope from critical infrastructure to digital products and services, the adoption of risk-based classification approaches, and the growing emphasis on public-private collaboration.

2.3 Artificial Intelligence Governance

The regulation of artificial intelligence has emerged as one of the most dynamic and contested areas of cyber law. The EU AI Act, the world's first comprehensive AI legislation, employs a risk-based classification system that distinguishes between unacceptable risk (prohibited practices), high risk (subject to extensive conformity assessment requirements), limited risk (subject to transparency obligations), and minimal risk (largely unregulated). The Act's first provisions entered into effect in February 2025, with rules for high-risk systems following in subsequent phases. The Act's extraterritorial reach—applying to providers and deployers of AI systems whose output is used within the EU, regardless of where the provider is established—has generated significant debate about its global impact and its interaction with other national regulatory approaches (Reinfeld & Gaon, 2025).

Comparative analysis of AI governance frameworks reveals both convergence and divergence across jurisdictions. The United States has adopted a predominantly sectoral and tort-based approach, relying on existing liability regimes and regulatory agencies to address AI-related harms rather than enacting comprehensive legislation (Stanford Law School, 2025). China has developed a layered regulatory architecture addressing specific AI applications—recommendation algorithms, deep synthesis, and generative AI—while also incorporating AI into its broader cybersecurity and data governance frameworks (China Cybersecurity Law, 2025). The United Kingdom has articulated a pro-innovation, principles-based approach that emphasizes regulatory flexibility. These divergent approaches reflect deeper differences in legal culture, political economy, and constitutional structure, raising fundamental questions about the feasibility and desirability of global AI governance harmonization (Reinfeld & Gaon, 2025).

A critical gap in current AI governance frameworks concerns liability attribution for harms caused by autonomous systems. Traditional tort law frameworks assume a human decision-maker whose conduct can be assessed against a standard of reasonable care. When AI systems make decisions with minimal human oversight, the chain of causation becomes attenuated and the allocation of responsibility among developers, deployers, and users becomes uncertain (Hallevy, 2020; Lior, 2025). The European Commission's proposed AI Liability Directive, which would have harmonized civil liability rules for AI-related damage, was withdrawn from the Commission's 2025 work programme, leaving a significant gap in the EU's regulatory architecture.

2.4 Cross-Border Data Governance

The regulation of cross-border data flows represents perhaps the most contested domain of contemporary cyber law. The EU's General Data Protection Regulation (GDPR) established a comprehensive framework for personal data protection that restricts transfers to third countries unless the receiving jurisdiction provides an "adequate level of protection" or the transfer is subject to appropriate safeguards such as Standard Contractual Clauses (SCCs). The adequacy decision regime has been applied to a limited number of jurisdictions, and the successive invalidation of the EU-US Privacy Shield by the Court of Justice of the European Union in the Schrems decisions has demonstrated the fragility of transatlantic data transfer mechanisms (Freshfields, 2025).

The Asia-Pacific region has witnessed a decisive shift toward data sovereignty and localization requirements. India's Digital Personal Data Protection Rules 2025 signal potential restrictions on outbound data flows, while Indonesia continues to strengthen data localization mandates. China, Russia, and Saudi Arabia have implemented some of the most restrictive data localization regimes globally, requiring domestic storage of certain categories of data and imposing strict conditions on cross-border transfers. These developments reflect a broader trend toward "digital sovereignty"—the assertion of state control over digital infrastructure, data, and technological standards as an element of national security and economic policy (Floridi, 2020).

The tension between data protection and data flow is particularly acute in the context of international trade. Digital trade agreements increasingly include provisions on cross-border data flows, data localization, and privacy protection, yet the relationship between trade law and data protection law remains unresolved. The OECD-WTO joint research on cross-border data flows suggests that the absence of data flow regulation would be associated with negative economic outcomes, while approaches that balance trade costs with trust benefits can deliver significant welfare gains. The challenge for policymakers is to design data governance frameworks that enable beneficial data flows while maintaining adequate protections for privacy, security, and other legitimate public interests.

2.5 Cybercrime and International Cooperation

The Budapest Convention on Cybercrime, adopted in 2001, remains the most widely ratified international treaty on cybercrime, with over 70 state parties. The

Convention establishes a common framework for criminalizing cyber-dependent and cyber-enabled offenses, and it provides mechanisms for international cooperation in investigations and electronic evidence sharing. However, the Convention has been criticized for its Eurocentric origins and its failure to address emerging threats such as ransomware-as-a-service, AI-enabled fraud, and the exploitation of virtual assets for money laundering (Council of Europe, 2025). The Convention Committee (T-CY) has adopted a Workplan for 2026–2027 that prioritizes tackling cyber scam centres, election interference, and challenges to freedom of expression under cybercrime laws.

The Hanoi Convention, adopted by the UN General Assembly in December 2024 and opened for signature in October 2025, represents the first global cybercrime treaty in nearly two decades. The Convention seeks to harmonize national laws, enhance cross-border investigations, facilitate electronic evidence sharing, and provide mutual legal and technical assistance, with particular attention to the needs of developing countries. The negotiation process was marked by deep-seated differences in legal and political systems, with Western nations raising concerns about potential misuse of the treaty to curb free speech and developing countries emphasizing the need for law enforcement capacity building. The final text represents a global compromise that complements rather than replaces the Budapest Convention.

Despite these normative advances, significant challenges remain in the operationalization of international cybercrime cooperation. Mutual Legal Assistance Treaties (MLATs), the traditional mechanism for cross-border evidence gathering, are widely acknowledged to be too slow and cumbersome for the pace of digital investigations. The EU's E-Evidence Regulation, entering into force in August 2026, represents an attempt to streamline cross-border access to electronic evidence through a European Production Order and a European Preservation Order. However, the effectiveness of such mechanisms depends on the willingness of service providers—many of which are headquartered in jurisdictions with different legal frameworks—to comply with foreign orders, and on the availability of adequate legal safeguards to protect privacy and other fundamental rights.

3. METHODOLOGY

This study employs a normative juridical methodology with a descriptive-analytical approach. Normative juridical research examines legal norms, principles, and doctrines through the analysis of primary legal sources—statutes, regulations, treaties, and judicial decisions—as well as secondary sources including scholarly commentary and policy documents. The descriptive-analytical approach serves two complementary functions: it systematically describes the content and structure of existing legal frameworks, and it critically analyzes their adequacy, coherence, and effectiveness in addressing the emerging challenges of digital transformation.

The research design is qualitative and comparative, drawing on legal materials from multiple jurisdictions and international organizations. Primary sources include the EU Artificial Intelligence Act (Regulation 2024/1689), the EU Digital Services Act (Regulation 2022/2065), the EU General Data Protection Regulation (Regulation

2016/679), the EU E-Evidence Regulation, the Budapest Convention on Cybercrime and its Additional Protocols, the United Nations Convention against Cybercrime (Hanoi Convention), the ASEAN Digital Economy Framework Agreement, the Digital Economy Partnership Agreement, and national legislation from Indonesia, Vietnam, Zambia, Nigeria, and other jurisdictions. Secondary sources include peer-reviewed journal articles, books, and reports from international organizations such as the Council of Europe, the United Nations Office on Drugs and Crime, the OECD, and the World Trade Organization.

The analytical framework integrates three dimensions of legal analysis. First, doctrinal analysis examines the content, structure, and internal coherence of legal norms. Second, comparative analysis identifies patterns of convergence and divergence across jurisdictions and legal traditions. Third, policy analysis assesses the practical implications of legal frameworks for stakeholders including governments, businesses, and individual rights-holders. The integration of these three dimensions enables a holistic assessment of cyber law as a multi-level governance system rather than a collection of isolated regulatory instruments.

The selection of jurisdictions and legal instruments for analysis was guided by three criteria: (1) regulatory significance, understood as the influence of a jurisdiction's approach on global normative development; (2) diversity of legal tradition and developmental context; and (3) availability of authoritative legal texts and scholarly commentary. The analysis prioritizes developments from 2020 to 2026, with reference to foundational instruments and scholarship where necessary for contextual understanding.

4. RESULTS AND DISCUSSION

4.1 The Regulatory Turn in Cybersecurity Governance: From Voluntarism to Mandatory Resilience

The analysis reveals a decisive global shift from voluntary, market-driven approaches to cybersecurity toward mandatory, risk-based regulatory frameworks. This regulatory turn is evident across jurisdictions and reflects a shared recognition that cyber threats have evolved beyond the capacity of individual organizations to manage through voluntary measures alone.

The EU has been at the forefront of this shift, implementing a layered regulatory architecture that includes NIS2 (replacing the original NIS Directive), DORA (applying to financial entities since January 2025), and the Cyber Resilience Act (addressing products with digital elements). DORA applies directly to insurers, intermediaries, and other financial entities with no transitional period, requiring demonstration of compliance across five pillars including ICT risk management, incident reporting, and third-party risk management. The European Commission has also tabled proposals for a strengthened Cybersecurity Act and a new Digital Networks Act (DNA), indicating an intention to further expand and deepen the regulatory framework.

This regulatory expansion reflects a fundamental reorientation in cybersecurity governance: from a model that relies on voluntary standards and market incentives to one that mandates minimum security requirements, imposes accountability mechanisms, and treats cybersecurity as a public good rather than a private responsibility. The rationale for this shift is grounded in the recognition that cyber incidents generate significant negative externalities—affecting not only the directly targeted organization but also its customers, suppliers, and the broader digital ecosystem. In economic terms, the social cost of cyber insecurity exceeds the private cost, creating a systematic underinvestment in security that voluntary approaches are ill-equipped to correct.

However, the regulatory turn raises significant concerns about compliance costs, particularly for small and medium-sized enterprises (SMEs) and organizations in developing countries. The expansion of regulatory scope to digital products and services across the supply chain, as contemplated in the Cyber Resilience Act and Indonesia's Cybersecurity and Cyber Resilience Bill, may impose substantial burdens on manufacturers and developers who lack the resources to conduct comprehensive conformity assessments. These concerns are particularly acute in developing countries, where institutional capacities for regulatory enforcement are often limited and where the digital economy is dominated by imported technologies and services.

4.2 Artificial Intelligence Regulation: Between Innovation and Risk

The global landscape of AI regulation exhibits significant divergence, with different jurisdictions adopting fundamentally different approaches to balancing innovation and risk. The EU AI Act represents the most comprehensive and prescriptive framework, employing a risk-based classification that imposes stringent requirements on high-risk applications while leaving minimal-risk applications largely unregulated. The Act's first provisions took effect in February 2025, covering AI system definitions, AI literacy requirements, and prohibitions on unacceptable practices such as social scoring.

The global impact of the EU AI Act is already visible. The Act's extraterritorial reach—applying to providers and deployers whose AI system output is used within the EU—has prompted multinational companies to align their AI governance practices with EU requirements even in jurisdictions where no comparable regulations exist. This "Brussels Effect" is a familiar pattern in EU regulatory policy, observed previously in data protection (GDPR) and chemicals regulation (REACH). However, the AI Act's impact may be more limited than the GDPR's because AI development and deployment are characterized by greater heterogeneity across sectors and use cases, making uniform compliance strategies more difficult to design and implement (Reinfeld & Gaon, 2025).

The United States has adopted a fundamentally different approach, eschewing comprehensive federal AI legislation in favor of sectoral regulation and reliance on existing liability regimes. This tort-based approach emphasizes ex post liability for harms rather than ex ante regulatory approval, reflecting a broader preference for market-driven innovation and skepticism of centralized regulatory authority (Stanford Law School, 2025). The withdrawal of the proposed EU AI Liability Directive in 2025 leaves

the EU without a harmonized civil liability framework for AI-related damage, creating a regulatory gap that may undermine the effectiveness of the AI Act's *ex ante* requirements.

The divergence between the EU's precautionary approach and the US's innovation-oriented approach creates significant challenges for global AI governance. Companies operating across jurisdictions must navigate conflicting requirements, while the absence of mutual recognition mechanisms means that compliance with one jurisdiction's regulations does not automatically satisfy another's. The development of international standards—through the OECD, ISO, and IEEE—may provide a partial solution, but the experience of previous standard-setting efforts suggests that convergence at the level of general principles often coexists with persistent divergence at the level of specific requirements.

A critical issue that remains inadequately addressed in all jurisdictions is the liability of AI systems for autonomous harms. When an AI system makes a decision that causes harm—whether to an individual's rights, property, or physical safety—the allocation of responsibility among developers, deployers, and users is often unclear. Traditional doctrinal categories such as negligence, product liability, and vicarious liability were designed for human decision-makers and may not map cleanly onto AI systems that learn from data, adapt their behavior over time, and operate with varying degrees of human oversight. The scholarly literature has proposed several approaches—including strict liability for high-risk AI, proportionate liability based on contribution to risk, and no-fault compensation schemes—but no consensus has emerged, and legislative action has been limited (Lior, 2025; Hallevy, 2020).

4.3 Cross-Border Data Governance: Fragmentation and its Consequences

The analysis reveals a global landscape of cross-border data governance characterized by increasing fragmentation and competing normative frameworks. The EU GDPR's adequacy decision regime, which permits data transfers to jurisdictions deemed to provide "essentially equivalent" protection, has been applied to a limited number of countries and remains vulnerable to legal challenge. The Court of Justice's *Schrems II* decision invalidated the EU-US Privacy Shield on the grounds that US surveillance laws did not provide adequate protection for EU citizens' data, and the subsequent negotiation of the EU-US Data Privacy Framework has not resolved fundamental concerns about the scope of US intelligence collection (Freshfields, 2025).

The Asia-Pacific region has experienced a decisive shift toward data sovereignty, with India, Indonesia, China, and other countries implementing or strengthening data localization requirements. These developments reflect a broader geopolitical trend in which data is increasingly viewed as a strategic asset subject to national control, rather than a resource that should flow freely across borders. The European Union itself has contributed to this trend through its European Cloud Sovereignty Framework, announced in October 2025, which emphasizes data sovereignty as a component of strategic autonomy.

The consequences of data governance fragmentation are significant for both economic and normative reasons. Economically, restrictive data transfer policies can increase trade costs, reduce productivity, and limit the diffusion of innovation. OECD-WTO research suggests that while some regulation of data flows is associated with trust benefits that facilitate economic activity, excessive restrictions can impose substantial costs on digital trade and cross-border investment. For multinational enterprises, the complexity of navigating multiple, overlapping, and sometimes conflicting data governance regimes creates compliance costs that disproportionately affect smaller firms and organizations in developing countries.

Normatively, the fragmentation of data governance raises the question of whether the international legal order can accommodate legitimate regulatory diversity without descending into a regime of competing sovereignties in which the most powerful states impose their preferences on others through market power and extraterritorial enforcement. The EU's exercise of regulatory authority through the GDPR has been characterized by some scholars as a form of "digital colonialism" that imposes European values on non-European populations (Gikay, 2020), while others view it as a legitimate exercise of democratic sovereignty in the face of global platform power. Resolving this tension requires more than technical fixes; it requires a normative framework for evaluating the legitimacy of cross-border regulatory assertions—a framework that is currently lacking in international law.

4.4 Cybercrime Cooperation: The Hanoi Convention and Beyond

The adoption of the UN Convention against Cybercrime (Hanoi Convention) represents a landmark achievement in international legal cooperation, yet its significance must be assessed against persistent implementation challenges. The Convention's substantive provisions cover a broad range of cyber-dependent and cyber-enabled offenses, including illegal access, data interference, computer-related fraud, and offenses related to child sexual abuse material. It establishes mechanisms for international cooperation, including extradition, mutual legal assistance, and the sharing of electronic evidence, and it includes provisions for technical assistance and capacity building directed toward developing countries.

However, the Convention's negotiation was marked by fundamental disagreements about its scope and purpose. Western nations expressed concerns that the treaty could be used to legitimize restrictions on freedom of expression and to facilitate surveillance of political opponents, while developing countries emphasized the need for stronger law enforcement cooperation and capacity building. The final text incorporates human rights safeguards, but the effectiveness of these provisions will depend on their interpretation and application by state parties, which may have different understandings of the balance between security and liberty.

A more fundamental challenge concerns the relationship between the Hanoi Convention and the Budapest Convention. The two instruments overlap significantly in their substantive provisions but differ in their membership, governance structures, and institutional arrangements. The Council of Europe has emphasized that the Hanoi

Convention "complements" the Budapest Convention, but the practical implications of this complementarity remain unclear. For states that are parties to both instruments, the question arises of which mechanism to invoke in specific cases and how to resolve potential conflicts. For states that are parties to neither or to only one, the proliferation of overlapping instruments may create confusion rather than clarity.

The operationalization of international cybercrime cooperation faces additional challenges from the structure of the global internet economy. The vast majority of electronic evidence relevant to cybercrime investigations is held by a small number of private companies headquartered in the United States, including Microsoft, Google, Meta, and Amazon. These companies are subject to conflicting legal obligations: US law, particularly the Stored Communications Act, restricts the disclosure of user data to foreign governments, while the laws of other jurisdictions may require such disclosure. The EU's E-Evidence Regulation seeks to address this problem by establishing a European Production Order that can be served directly on service providers, but the effectiveness of this mechanism depends on reciprocal arrangements with third countries and on the willingness of service providers to comply.

4.5 Platform Liability and Content Governance

The regulation of online platforms has emerged as a central battleground in cyber law, with significant developments in both the EU and the United States. The EU Digital Services Act (DSA), fully applicable since February 2024, establishes a comprehensive framework for platform accountability that includes transparency obligations, risk assessment and mitigation requirements for very large online platforms, and a crisis response mechanism. The DSA represents a departure from the liability exemption model that has dominated internet governance since the US Communications Decency Act Section 230, moving toward a model of "regulated self-regulation" in which platforms are granted conditional immunity but are also subject to substantial regulatory oversight (Kohl, 2024).

A significant judicial development in this area was the Court of Justice of the European Union's *Russmedia* judgment (C-492/23), delivered in December 2025, which held that online platforms cannot rely on intermediary liability protections when data protection violations are involved. The Court's reasoning emphasized the distinct legal bases of data protection law and intermediary liability law, rejecting the argument that compliance with the latter automatically satisfies the former. This judgment has significant implications for platform operators, who must now navigate both content moderation obligations under the DSA and data protection obligations under the GDPR without the benefit of the liability safe harbour that previously shielded them from certain claims.

The systematic review of intermediary liability scholarship identifies several persistent challenges: the inconsistency of legal frameworks across jurisdictions, which complicates compliance for global platforms; the tension between content moderation and freedom of expression; the difficulties of applying traditional liability doctrines to algorithmic amplification and recommendation systems; and the need for harmonized

standards regarding anonymous defamation and e-commerce liability (Kohl, 2024). These challenges are unlikely to be resolved through incremental adjustments to existing frameworks; they may require more fundamental rethinking of the relationship between platform power, user rights, and public interest regulation.

4.6 Digital Trade and the Governance of the Digital Economy

The proliferation of digital trade agreements has created a complex layer of governance that operates alongside, and sometimes in tension with, domestic regulatory frameworks. The Digital Economy Partnership Agreement (DEPA), initiated by Singapore, Chile, and New Zealand in 2020, was the first standalone digital trade agreement and has since been joined by South Korea, with Peru's accession under negotiation. The ASEAN Digital Economy Framework Agreement (DEFA) reached substantial conclusion in October 2025 and is set to be signed in 2026, with nine core pillars covering digital trade facilitation, cross-border data flows, cybersecurity, digital payments, and emerging technologies.

These agreements share several features that distinguish them from traditional trade agreements. They are more detailed and more binding with respect to core digital issues such as data transfers and data localization, and they incorporate provisions on emerging technologies—including AI governance—that are absent from earlier agreements. DEPA, for example, includes modules on AI governance, digital identities, and open government data that go beyond the narrow focus on trade barriers that characterizes most digital trade provisions.

However, the relationship between digital trade agreements and domestic regulatory autonomy remains contested. Provisions on cross-border data flows may constrain the ability of governments to implement data localization requirements for legitimate public policy purposes, including cybersecurity and privacy protection. The inclusion of AI governance provisions in trade agreements raises questions about the appropriate locus of AI regulation: should AI standards be set through trade negotiations, where the primary objective is market access, or through dedicated regulatory processes that prioritize safety, fundamental rights, and democratic accountability? The experience of the EU's AI Act, which was developed through a transparent legislative process with extensive stakeholder consultation, stands in contrast to the closed-door negotiations that characterize most trade agreements.

4.7 Legal Pluralism and the Quest for Coherence

The analysis reveals a fundamental tension at the heart of contemporary cyber law: the proliferation of regulatory instruments at national, regional, and international levels has not produced a coherent global governance framework but has instead created a complex and sometimes contradictory patchwork of norms. This condition has been described in the scholarly literature as "legal pluralism" in cyberspace—the coexistence of multiple normative orders that claim authority over the same domain without a clear hierarchy or coordination mechanism (Schulz, 2020; Gikay, 2020).

Legal pluralism in cyberspace is not necessarily pathological. In some contexts, overlapping and competing norms can be productive, enabling experimentation with different regulatory approaches and allowing jurisdictions to adapt global standards to local conditions. The "regulatory sandbox" model, which has been adopted in various forms across the Asia-Pacific region, exemplifies this experimental approach, enabling controlled testing of innovative technologies and business models under regulatory supervision. However, legal pluralism becomes problematic when it generates uncertainty, arbitrage opportunities, and enforcement gaps that undermine the effectiveness of all regulatory frameworks.

The quest for coherence in cyber law requires more than harmonization—the imposition of uniform rules across jurisdictions. It requires the development of mechanisms for mutual recognition, coordination, and conflict resolution that respect legitimate regulatory diversity while ensuring minimum standards of protection. The Council of Europe's Convention 108+ on data protection, which has been ratified by a diverse group of states including non-European countries, offers one model for such coordination: it establishes common principles while allowing states to implement them through different legal mechanisms and institutional arrangements. Similar models could be developed for AI governance, cybersecurity, and platform regulation, though the political obstacles to such coordination are substantial.

5. CONCLUSION

This study has examined the emerging legal issues arising from digital transformation in the global information era and assessed the adequacy of contemporary cyber law responses. The analysis reveals a global governance landscape characterized by rapid normative development, significant regulatory divergence, and persistent gaps between legal frameworks and technological realities.

The principal findings can be summarized as follows. First, cybersecurity governance has undergone a decisive regulatory turn, with jurisdictions increasingly adopting mandatory, risk-based frameworks that impose minimum security requirements and accountability mechanisms. This shift reflects the recognition that voluntary approaches have failed to address the negative externalities of cyber insecurity. However, the expansion of regulatory scope raises significant concerns about compliance costs for SMEs and organizations in developing countries.

Second, AI regulation exhibits fundamental divergence between the EU's precautionary, comprehensive approach and the US's sectoral, liability-based approach. The EU AI Act's extraterritorial reach has generated a partial "Brussels Effect," but the absence of a harmonized AI liability framework and the persistence of conflicting national approaches create significant uncertainties for global AI development and deployment.

Third, cross-border data governance is characterized by increasing fragmentation, with data sovereignty and localization requirements proliferating alongside adequacy decisions and trade agreement provisions. This fragmentation

imposes substantial costs on digital trade and raises fundamental questions about the legitimacy of extraterritorial regulatory assertions.

Fourth, the Hanoi Convention represents a significant achievement in international cybercrime cooperation but faces substantial implementation challenges, including the proliferation of overlapping instruments, the conflicting legal obligations of service providers, and the need for adequate human rights safeguards.

Fifth, platform liability and content governance are undergoing significant transformation, with the DSA and the Russmedia judgment creating new obligations and uncertainties for platform operators. The tension between content moderation and freedom of expression, and the challenge of applying traditional liability doctrines to algorithmic systems, remain unresolved.

The theoretical contribution of this study lies in its integrated framework for understanding cyber law as a multi-level governance system. By examining cybersecurity, AI governance, data protection, platform liability, and international cooperation as interconnected domains, the research demonstrates that regulatory developments in one area have significant implications for others—implications that are often overlooked in domain-specific analyses. The study also advances the theoretical understanding of legal pluralism in cyberspace by distinguishing between productive and pathological forms of normative multiplicity and by identifying the conditions under which coordination mechanisms can mitigate the risks of fragmentation.

The practical and policy implications of these findings are several. Policymakers should prioritize the development of mechanisms for regulatory coordination and mutual recognition that respect legitimate diversity while ensuring minimum standards of protection. The experience of the Council of Europe's Convention 108+ suggests that such mechanisms are feasible even in politically challenging environments, though they require sustained diplomatic effort and institutional commitment. Regulators should invest in capacity building for enforcement, particularly in developing countries where institutional resources are limited. International organizations should facilitate the development of common standards and best practices while avoiding the imposition of uniform rules that may be inappropriate for diverse legal, cultural, and developmental contexts.

The limitations of this study should be acknowledged. The analysis relies primarily on documentary sources and legal analysis rather than empirical data on the implementation and impact of regulatory frameworks. Future research should examine the actual effects of the regulatory instruments analyzed here—their impact on security outcomes, innovation, fundamental rights, and economic development—through empirical methods including case studies, surveys, and quantitative analysis. Additionally, the study's focus on developments in 2020–2026 means that earlier regulatory frameworks, particularly those in developing countries, may be underrepresented. Future research should examine longer-term trajectories of cyber law development and the factors that facilitate or impede regulatory convergence across jurisdictions.

The global information era presents both unprecedented opportunities and profound challenges for legal governance. The emerging legal issues identified in this study—AI liability, data sovereignty, cross-border evidence, platform accountability, and the governance of emerging technologies—will continue to evolve as digital transformation proceeds. The task for legal scholars and policymakers is not to solve these problems once and for all, but to develop adaptive, reflexive, and institutionally robust frameworks that can respond to technological change while protecting fundamental rights and enabling beneficial innovation. This requires a commitment to legal pluralism as a governing principle, combined with sustained efforts to build the coordination mechanisms, institutional capacities, and normative consensus necessary to make pluralism productive rather than pathological.

REFERENCES

- Barlow, J. P. (1996). A declaration of the independence of cyberspace. Electronic Frontier Foundation.
- Council of Europe. (2025). 33rd T-CY Plenary adopts Workplan 2026–2027. Cybercrime Convention Committee. <https://www.coe.int/en/web/cybercrime>
- European Commission. (2019). Ethics guidelines for trustworthy AI. High-Level Expert Group on Artificial Intelligence. <https://doi.org/10.2759/346720>
- European Commission. (2020). Proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). COM(2020) 823 final.
- European Commission. (2022). Proposal for a Regulation on digital operational resilience for the financial sector (DORA). COM(2022) 491 final.
- Floridi, L. (2018). Soft ethics and the governance of the digital. *Philosophy & Technology*, 31(1), 1–8. <https://doi.org/10.1007/s13347-018-0303-9>
- Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33(3), 369–378. <https://doi.org/10.1007/s13347-020-00423-6>
- Gikay, A. A. (2020). Rethinking the jurisprudence of cyberspace. *International Journal of Law and Information Technology*, 28(3), 236–258. <https://doi.org/10.1093/ijlit/eaab015>
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Goldsmith, J., & Wu, T. (2006). *Who controls the internet? Illusions of a borderless world*. Oxford University Press.
- Hallevy, G. (2020). *Liability for crimes involving artificial intelligence*. Cambridge University Press.
- Kohl, U. (2024). Recommender algorithms and the amplification of toxicity: The case for regulated self-regulation. *Quality & Quantity*, 58(2), 1–22. <https://doi.org/10.1007/s11135-024-01867-0>
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books.
- Lior, A. (2025). *AI and tort liability: Rethinking, recalibrating, and reallocating risk*. Routledge.
- Murray, A. D. (2013). *The regulation of cyberspace: Control in the online environment*. Routledge-Cavendish.

- Murray, A. D. (2019). *Information technology law: The law and society* (4th ed.). Oxford University Press.
- Plantin, J. C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20(1), 293–310. <https://doi.org/10.1177/1461444816661553>
- Ramli, A. M., Suseno, S., Mayana, R. F., Rajamanickam, R., & Rohmana, R. D. (2026). The urgency of regulating artificial intelligence in relation to cybersecurity and cyber resilience. *Cogent Law & Criminology*, 7(1), 2632977. <https://doi.org/10.1080/23311886.2026.2632977>
- Reed, C. (2012). *Making laws for cyberspace*. Oxford University Press.
- Reinfeld, Y., & Gaon, A. (2025). The global impact of the EU artificial intelligence framework. In *The EU Artificial Intelligence Act: Global implications* (pp. 1–28). Taylor & Francis. <https://doi.org/10.4324/9781032722788-12>
- Schulz, W. (2020). The problem of platform law: Pluralistic legal ordering on social media. In P. S. Berman (Ed.), *The Oxford handbook of global legal pluralism* (pp. 1–24). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780197516744.013.33>
- Stanford Law School. (2025). On the distinction between tort-based and risk-based AI regulation: A transatlantic perspective. Stanford Law School. <https://law.stanford.edu>
- Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. <https://doi.org/10.1111/rego.12158>