ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance

Mehmet. Kaya[1*], Hamza. Shahid[2]

[1] Department of International Relations, Istanbul University, Istanbul, Turkiye
[2] Department of Law, University of the Punjab, Lahore, Pakistan

*** Corresponding author email address**: mehmet.kaya@istanbul.edu.tr

Received: 2025-01-29 **Revised:** 2025-03-22 **Accepted:** 2025-03-28 **Published:** 2025-04-01

ABSTRACT

This article aims to explore the legal dilemmas arising from the intersection of cross-border data flows and digital sovereignty within the evolving landscape of transnational governance. Using a narrative review approach and a descriptive analysis method, this study synthesizes recent academic literature, international legal instruments, regional regulations, and national policies published between 2020 and 2024. The sources include peer-reviewed legal scholarship, policy documents from international organizations, and national legislative texts. The analysis focuses on the conceptual foundations of cross-border data movement and digital sovereignty, the legal frameworks governing data governance, and the challenges of harmonizing national interests with global connectivity. The study draws upon legal theory and comparative regulatory analysis to critically examine multilateral initiatives and national responses. The study finds that cross-border data flows are essential to digital trade, innovation, and global interconnectivity, yet they increasingly face legal constraints due to states' pursuit of digital sovereignty. This pursuit manifests in data localization laws, extraterritorial enforcement of domestic regulations, and strategic decoupling efforts, particularly among major geopolitical actors. International and regional efforts at harmonization—such as those by the OECD and G20—offer frameworks for trust-based data governance but remain hindered by divergent regulatory philosophies. Fragmentation of legal norms has resulted in significant compliance challenges and enforcement dilemmas, while human rights protections in data governance vary widely across jurisdictions, affecting privacy and freedom of expression. Effective governance of cross-border data flows requires a balance between national sovereignty and transnational cooperation. Moving forward, interoperability and mutual legal recognition offer viable alternatives to legal uniformity or isolation.

Keywords: *cross-border data flows, digital sovereignty, data localization, legal fragmentation, transnational governance, interoperability, data protection.*

How to cite this article:

Kaya, M., & Shahid, H. (2025). Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. *Interdisciplinary Studies in Society, Law, and Politics, 4*(2), 219-233. https://doi.org/10.61838/kman.isslp.4.2.20

1. Introduction

In the contemporary digital era, the global exchange of data across borders has become a defining feature of international connectivity, economic growth, and technological innovation. Cross-border data flows underpin everything from e-commerce and cloud computing to international financial transactions and online communication platforms. These flows facilitate the seamless operation of multinational corporations, enable scientific and academic collaboration, and serve as critical infrastructure for digital economies. The increasing volume, velocity, and value of transnational data movement have rendered data a core strategic asset in the twenty-first century. However, as states, corporations, and individuals become more reliant on

digital data, concerns over data access, control, and protection have intensified, giving rise to contentious debates about sovereignty, jurisdiction, and regulation in cyberspace.

The concept of digital sovereignty has emerged in response to these tensions, encapsulating a state's desire to exert control over digital infrastructure, data governance, and technological standards within its territory. Unlike traditional notions of sovereignty, which focus on physical borders and territorial authority, digital sovereignty involves the assertion of legal, political, and normative power in cyberspace, a domain inherently transnational and diffuse. States pursuing digital sovereignty often do so through legislative instruments that mandate data localization, restrict cross-border data transfers, or assert extraterritorial reach over digital service providers. The European Union, for example, has advanced digital sovereignty through its regulatory framework under the General Data Protection Regulation (GDPR), which imposes strict conditions on data flows beyond EU borders and exemplifies a rights-based approach to data governance (Feng, 2023). Similarly, countries like China and Russia have implemented data localization laws to secure data within national borders, citing reasons of national security, cultural integrity, and economic independence (Du, 2022).

Yet, the pursuit of digital sovereignty often collides with the principles of transnational digital integration and the free flow of information that underpin the global internet. Legal scholars have noted that digital sovereignty can exacerbate regulatory fragmentation, create conflict-of-law scenarios, and hinder multilateral cooperation on data governance (Goode, 2023). Moreover, there is a growing concern that the weaponization of data and the politicization of digital infrastructure could lead to a balkanized internet, undermining its openness and universality (Crowley et al., 2020). These issues have drawn attention from scholars, policymakers, and international institutions seeking to balance the legitimate aspirations of states to control data with the need to preserve global digital interdependence.

The present article aims to review and critically analyze the legal dilemmas that arise at the intersection of cross-border data flows and digital sovereignty. It seeks to explore how different jurisdictions conceptualize and operationalize digital sovereignty and how these legal frameworks impact the governance of transnational data. The review highlights normative, institutional, and regulatory challenges posed by divergent approaches to data control, especially when national laws assert extraterritorial authority or conflict with international obligations. In doing so, the article contributes to the broader discourse on transnational governance by examining the legal tools, doctrines, and strategies employed by states and international actors to assert control over digital domains. It also interrogates the implications of such strategies for human rights, trade law, and global regulatory coherence.

To achieve these aims, the study adopts a narrative review methodology, which is particularly suited for synthesizing diverse legal sources, identifying patterns across jurisdictions, and interpreting the evolving normative landscape. The rationale for using a narrative review approach lies in its flexibility and depth, allowing for a comprehensive examination of doctrinal developments, policy documents, judicial decisions, and scholarly analyses. Rather than adhering to a narrow empirical scope or a systematic quantitative framework, this method facilitates an interpretive analysis of legal arguments, regulatory innovations, and conceptual debates. In legal scholarship, narrative reviews are invaluable for tracing the genealogy of legal concepts and for assessing how evolving political and institutional contexts reshape legal norms (Leonelli, 2021).

Moreover, the descriptive analysis method employed in this review allows for a thematic exploration of the legal and political claims embedded in digital sovereignty discourse. This includes examining how legal frameworks prioritize sovereignty over interoperability, how transnational actors respond to jurisdictional complexity, and how competing interests shape the contours of digital rights and state authority (Haagensen, 2023). Given the multidimensional nature of data governance—spanning trade, security, privacy, and human rights—this approach enables a nuanced account of the tensions and contradictions embedded in legal regimes.

The review's contribution lies in bridging theoretical insights with concrete legal developments, offering a critical lens through which to assess the evolving architecture of transnational data governance. It addresses how international legal principles such as

mutual recognition, extraterritoriality, and jurisdictional subsidiarity are being reinterpreted in light of digital transformations (Joerges, 2023). Furthermore, it highlights how the shift toward sovereign control of data is reshaping traditional understandings of globalization, legal integration, and transnational legal orders (Sourgens et al., 2024). By situating digital sovereignty within broader debates on law and globalization, the article adds value to contemporary legal literature that seeks to reconcile state-centric legal authority with the demands of a digitally interdependent world.

Ultimately, this article invites readers to consider whether the current trajectory of digital sovereignty promotes or impedes effective transnational governance. It asks whether legal systems are evolving in ways that enhance digital rights and institutional accountability or whether they are reinforcing unilateralism and regulatory disintegration. As states increasingly adopt strategies that prioritize national control over digital space, the stakes for global legal coherence and equitable access to digital infrastructure grow ever higher. This narrative review serves as both a conceptual exploration and a legal critique of the forces shaping our digital legal future.

2. Methodology

This study employed a narrative review approach grounded in a descriptive analysis method to investigate the legal dilemmas surrounding cross-border data flows and the concept of digital sovereignty within transnational governance frameworks. The narrative review design was chosen due to its capacity to synthesize and interpret a broad range of academic, legal, and policy-based literature without the rigid constraints of systematic review methodologies. The descriptive analysis method allowed for a thematic and interpretive exploration of emerging legal debates, jurisdictional conflicts, and evolving regulatory responses related to global data governance. This method is particularly well-suited to legal scholarship where the analysis often involves interpreting normative claims, identifying conceptual tensions, and evaluating legal coherence across jurisdictions. The aim was not to produce a statistical generalization but to provide a nuanced understanding of how different legal systems, institutions, and governments have responded to the challenges of governing digital data that routinely crosses borders.

The materials reviewed in this study included peer-reviewed journal articles, international legal instruments, regional regulations, national legislation, judicial decisions, and official policy documents published between 2020 and 2024. The academic sources were primarily drawn from legal, political science, and information policy journals indexed in major scholarly databases such as Scopus, Web of Science, and HeinOnline. Policy documents and legal texts were sourced from reputable institutional websites including the European Commission, World Trade Organization, Organisation for Economic Co-operation and Development (OECD), and national government portals. The search strategy involved keyword combinations such as “cross-border data flows,” “digital sovereignty,” “data localization,” “jurisdiction and data governance,” and “transnational digital regulation.” A critical inclusion criterion was the relevance of the document to legal analysis and regulatory implications, with priority given to texts that engaged explicitly with legal frameworks, rights-based concerns, and governance dilemmas. Duplicate and outdated sources, as well as those focusing solely on technical infrastructure without legal relevance, were excluded from the final synthesis.

The selected materials were analyzed using qualitative content analysis, with particular attention paid to identifying recurrent themes, conceptual debates, and legal inconsistencies across jurisdictions. Thematic coding was used to extract patterns related to how legal systems conceptualize digital sovereignty, respond to transnational data flows, and reconcile conflicts between domestic laws and international commitments. Emphasis was placed on examining the legal architecture of regulatory instruments such as the EU’s General Data Protection Regulation (GDPR), the U.S. CLOUD Act, and China's Personal Information Protection Law (PIPL), along with regional and multilateral initiatives such as OECD cross-border data flow frameworks and WTO e-commerce negotiations. Comparative legal analysis was employed to understand how divergent national laws shape the global data governance landscape and to assess the extent to which legal fragmentation or harmonization is occurring. The interpretive nature of the analysis also allowed for reflection on normative

dimensions, such as the implications of digital sovereignty claims for human rights protections and the global free flow of information.

3. Conceptual Foundations

3.1. Cross-Border Data Flows

Cross-border data flows refer to the movement of digital information across national borders through information and communication technologies. These flows encompass various categories of data, including commercial, personal, and strategic data. Commercial data generally includes digital information associated with business transactions, supply chains, financial records, and digital services. It plays a central role in e-commerce, digital marketing, and cross-border trade in services. Personal data includes any information relating to an identified or identifiable individual, such as names, addresses, biometric identifiers, and online behavior. This category has become increasingly significant with the proliferation of social media platforms, cloud storage, and health monitoring technologies. Strategic data refers to information that has relevance to national security, defense, infrastructure management, and diplomatic affairs. This type of data often triggers the most restrictive regulatory responses, as states seek to safeguard their sovereignty and critical systems from foreign access or interference (Du, 2022).

The movement of data across borders is vital for international trade and innovation. Global value chains depend heavily on real-time data exchanges to coordinate production, distribution, and logistics. For instance, multinational corporations rely on cross-border data flows to manage supply chain operations, human resource functions, customer analytics, and compliance reporting. Without such seamless data transfers, the efficiency and scalability of international business operations would be severely impaired. In the financial sector, cross-border data flows enable digital payment systems, fraud detection, credit scoring, and compliance with anti-money laundering regulations. Similarly, in sectors like health care and education, the international sharing of medical records, research findings, and educational content fosters collaboration and technological advancement (Canfield, 2023).

The digital economy has become increasingly dependent on uninterrupted and predictable data flows to ensure global connectivity. Emerging technologies such as artificial intelligence, machine learning, and the Internet of Things rely on large-scale, cross-border datasets to function effectively. These technologies not only drive productivity and innovation but also facilitate transnational cooperation in addressing global challenges such as climate change, pandemics, and disaster response. As noted by scholars, digital interdependence has redefined the traditional notions of economic integration, enabling countries to participate in global markets regardless of geographic distance (Feng, 2023). However, the ubiquity of cross-border data flows also raises critical concerns regarding data privacy, cyber-security, and legal accountability, especially when data is transferred to jurisdictions with different or weaker protections for individual rights (Leonelli, 2021). The reliance on digital infrastructure that transcends national borders has revealed regulatory and jurisdictional gaps in existing legal systems. These gaps are often exploited by corporations that engage in regulatory arbitrage or by states that assert extraterritorial jurisdiction over foreign-based data controllers. In such contexts, cross-border data flows have become both enablers of global digital commerce and sources of legal and political friction. Increasingly, countries are seeking to balance the benefits of open data flows with the need to assert control over data that originates within their borders or affects their populations. This balancing act is central to the emerging discourse on digital sovereignty.

3.2. Digital Sovereignty

Digital sovereignty refers to the capacity of a state to regulate, control, and protect digital information, infrastructure, and technologies within its jurisdiction. While the term draws upon the classical notion of Westphalian sovereignty, it has evolved to encompass control over data, algorithms, platforms, and technological standards in cyberspace. At its core, digital sovereignty entails the authority of a government to set rules for how data is collected, processed, stored, and transmitted, including the power to impose restrictions on cross-border data transfers. Importantly, digital sovereignty is not synonymous with data protection or cybersecurity, although it often overlaps with both. Data protection primarily concerns the rights of individuals regarding their personal information, while

cybersecurity refers to the protection of systems, networks, and data from cyber threats. In contrast, digital sovereignty is a broader political and legal claim about the control over digital ecosystems and the ability to resist foreign influence or dependency (Sourgens et al., 2024).

The political dimensions of digital sovereignty are particularly pronounced in debates about technological self-sufficiency and resistance to digital colonialism. Some states argue that relying on foreign cloud providers, social media platforms, or search engines compromises their political autonomy and exposes their populations to foreign surveillance or cultural manipulation (Liu, 2024). For example, concerns about the extraterritorial reach of U.S. surveillance laws, such as the CLOUD Act, have prompted several countries to pursue strategies that ensure data remains physically stored within their borders (Haagensen, 2023). This has led to the proliferation of data localization mandates, national cloud initiatives, and the development of domestic alternatives to foreign-owned digital services. Such measures are often justified in the name of national security, economic sovereignty, or democratic control over information.

Legally, digital sovereignty is manifested in legislative and regulatory initiatives that define the territorial scope of data laws, assert jurisdiction over foreign digital service providers, and condition data transfers on compliance with domestic legal standards. The European Union's approach exemplifies a normative model that prioritizes fundamental rights, particularly privacy and data protection, in the governance of cross-border data flows. The GDPR sets strict requirements for international data transfers, permitting them only if adequate safeguards are in place, such as binding corporate rules or adequacy decisions. This regulatory model is increasingly being emulated by other jurisdictions seeking to align their data protection regimes with the EU standard or to assert equivalent sovereignty over their digital space (Perez, 2022).

At the strategic level, digital sovereignty is intertwined with broader questions of geopolitical competition and technological standard-setting. In recent years, the rise of digital nationalism has intensified rivalries over 5G networks, cloud infrastructure, and artificial intelligence governance. States are not only seeking to regulate data but also to shape the global norms and technical standards that govern the digital realm. As a result, multilateral cooperation on digital issues has become increasingly fragmented, with competing coalitions forming around divergent models of internet governance. The United States traditionally supports a multi-stakeholder approach involving private actors, civil society, and governments, while countries like China advocate for a state-centric model that emphasizes the primacy of national law and control (Mahardika, 2022).

The distinction between state-centric and multi-stakeholder interpretations of digital sovereignty reflects a fundamental tension in global data governance. The state-centric model, often associated with authoritarian or statist regimes, prioritizes central control, surveillance capabilities, and national resilience in the digital domain. It views sovereignty as the unilateral capacity of a government to impose rules on all digital activities within its borders, irrespective of the global implications. This model may involve censorship, restrictions on cross-border data flows, and the deployment of technical measures to monitor or filter internet traffic (Lilipaly et al., 2023). In contrast, the multi-stakeholder approach promotes a decentralized governance structure where private sector innovation, civil society participation, and international collaboration are seen as essential to preserving the openness, security, and inclusivity of the digital ecosystem (Sarcar, 2024).

Both models face challenges in practice. The state-centric approach risks creating digital silos that limit interoperability and suppress freedom of expression. It can also lead to duplicative or conflicting regulations that burden international businesses and undermine global standards. On the other hand, the multi-stakeholder model has been criticized for its limited accountability and uneven representation, particularly for actors from the Global South. Some scholars have argued that without mechanisms to ensure equitable participation and regulatory alignment, multi-stakeholderism may entrench existing power asymmetries rather than democratize global digital governance (An, 2022).

The contestation over digital sovereignty also reveals deeper anxieties about the legitimacy and effectiveness of transnational legal orders. In a world where digital interactions routinely traverse multiple jurisdictions, the conventional tools of international law—such as treaties, mutual legal assistance, and state-to-state cooperation—

often prove inadequate. This has prompted a turn toward transnational legal norms that cut across domestic and international boundaries, involving both public and private actors in the governance of digital ecosystems (Joerges, 2023). For example, private corporations like Google, Meta, and Microsoft increasingly participate in norm-setting processes, lobby for regulatory frameworks, and shape the de facto rules of data governance through their technical architectures and terms of service (Canfield, 2021). These developments challenge the traditional view of sovereignty as a purely state-based attribute and suggest the need for new legal theories that accommodate the complexity of digital interdependence.

In sum, digital sovereignty is a multidimensional and evolving concept that reflects the shifting boundaries of legal authority in the age of globalization. It encompasses political ambitions for control, legal assertions of jurisdiction, and strategic efforts to shape the global digital order. As states navigate the interplay between openness and control, and as transnational actors push for interoperable and inclusive governance models, the debate over digital sovereignty will remain a central issue in both legal theory and policy practice. Understanding its foundations and implications is essential for assessing the future of cross-border data flows and for crafting a more coherent and equitable global framework for digital governance.

4. Legal Frameworks and Governance Models

4.1. International and Regional Approaches

The global legal landscape governing cross-border data flows is shaped by a complex array of international, regional, and bilateral instruments, with differing objectives and degrees of enforceability. At the international level, the General Agreement on Trade in Services (GATS), administered by the World Trade Organization (WTO), provides a foundational framework for regulating digital trade, including data flows. Although GATS was drafted in the early 1990s, prior to the explosion of the digital economy, its provisions on market access and national treatment have been interpreted to apply to digital services as well. GATS encourages liberalization of trade in services but also includes exceptions for public policy concerns, such as privacy and national security, which countries have increasingly invoked to justify restrictions on data transfers (Minas, 2021). This has led to tensions between the principles of free data movement and sovereign rights to regulate information flows, particularly in sectors considered sensitive by national governments.

The European Union's General Data Protection Regulation (GDPR) represents the most comprehensive and influential regional framework for data protection and cross-border data governance. Enacted in 2018, the GDPR imposes strict rules on the collection, storage, processing, and transfer of personal data, both within the EU and internationally. One of its hallmark features is its extraterritorial reach: it applies not only to EU-based entities but also to non-EU organizations that process the personal data of EU residents. The GDPR sets out specific mechanisms for cross-border data transfers, including adequacy decisions, standard contractual clauses, and binding corporate rules. These tools ensure that personal data leaving the EU remains subject to a level of protection essentially equivalent to that guaranteed by EU law (Leonelli, 2021). The regulation has become a global benchmark, influencing legislative developments in countries seeking to align their data protection regimes with European standards.

In contrast to the GDPR's rights-based approach, the United States has developed a more sectoral and security-oriented legal framework. A key example is the Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in 2018. The CLOUD Act allows U.S. law enforcement agencies to compel domestic companies to produce data stored overseas, provided the data is under the company's "possession, custody, or control." This has raised concerns among privacy advocates and foreign governments, who view the Act as a unilateral assertion of jurisdiction that undermines data protection standards in other countries (Haagensen, 2023). The Act also provides for executive agreements with foreign governments, enabling mutual access to data under specified conditions. However, these agreements often lack transparency and do not always guarantee procedural safeguards equivalent to those required under frameworks like the GDPR.

Multilateral initiatives, particularly those led by the Organisation for Economic Co-operation and Development (OECD) and the WTO, have sought to promote coherence in cross-border data governance. The OECD has developed guidelines on the protection of

privacy and transborder flows of personal data, emphasizing the need for interoperability and accountability across jurisdictions (Feng, 2023). These guidelines encourage trust-based data sharing frameworks and promote a risk-based approach to regulation, although they remain non-binding. At the WTO, discussions around digital trade, including data flows, have intensified in recent years under the Joint Statement Initiative on E-Commerce. This initiative seeks to establish baseline rules for cross-border data transfers, data localization, and source code disclosure. However, progress has been slow due to divergent positions among member states, especially between countries favoring open data environments and those advocating for national control over digital assets (Goode, 2023).

The coexistence of these various legal instruments reflects the fragmented and contested nature of global data governance. While some frameworks promote liberalization and interoperability, others reinforce national control and regulatory divergence. This legal heterogeneity creates both opportunities and challenges for states, businesses, and individuals operating in a digitized global economy.

4.2. National Responses and Data Localization Laws

In response to the perceived inadequacies of international regulation and the growing importance of data as a strategic asset, many countries have adopted national laws that impose restrictions on the cross-border movement of data. These responses are often grounded in concerns about sovereignty, security, economic competitiveness, and cultural preservation. China has taken one of the most assertive approaches to data localization through its Cybersecurity Law, Data Security Law, and Personal Information Protection Law (PIPL). These laws require that certain categories of data, particularly those classified as "important" or "sensitive," be stored and processed within China. Transfers of personal data abroad must undergo security assessments and meet specific compliance criteria. The Chinese model reflects a highly centralized and security-driven approach to digital sovereignty, prioritizing state control over openness and interoperability (Jiang et al., 2022).

Russia has similarly enacted stringent data localization laws that require companies collecting personal data from Russian citizens to store and process such data within Russian territory. The 2015 amendment to the Federal Law on Personal Data mandates localization as a condition for operating in the Russian digital market. Non-compliance can result in heavy fines and access restrictions, as demonstrated in high-profile enforcement actions against global technology firms. India, while still finalizing its comprehensive data protection law, has proposed various localization requirements through drafts of the Personal Data Protection Bill. These drafts have included mandates for storing critical personal data within India and restricting the transfer of sensitive data without government approval (An, 2022).

In the European Union, the GDPR does not impose blanket localization requirements but instead sets out a rigorous framework for international data transfers. The regulation's emphasis on adequacy, safeguards, and accountability allows for conditional data mobility while ensuring that data exported from the EU remains subject to fundamental rights protections. Nonetheless, the EU's evolving digital strategy, including its plans for a European data space and cloud sovereignty initiatives, signals a move toward greater control over digital infrastructure and data flows (Joerges, 2023). These developments illustrate the EU's attempt to strike a balance between global integration and regulatory autonomy.

For global businesses, these national responses create a fragmented regulatory environment that increases compliance costs and operational complexity. Multinational companies must navigate conflicting legal obligations, invest in localized data infrastructure, and adjust their data governance strategies to meet the demands of diverse jurisdictions. This regulatory divergence can hinder innovation, reduce economies of scale, and limit access to global markets (Marco, 2021). From a legal perspective, the proliferation of localization laws raises fundamental questions about the compatibility of national sovereignty with international commitments, particularly in trade and human rights law.

4.3. Conflict of Laws and Jurisdictional Dilemmas

One of the most pressing legal challenges in transnational data governance is the conflict of laws arising from the extraterritorial application of national

regulations. As states seek to assert control over digital activities affecting their citizens or interests, they increasingly enact laws that apply beyond their borders. This practice, while often justified by the borderless nature of cyberspace, generates legal uncertainty and jurisdictional overlap. For instance, the extraterritorial reach of the GDPR requires non-EU companies to comply with EU data protection standards if they offer goods or services to EU residents or monitor their behavior online. This has led to complex compliance scenarios for businesses based in jurisdictions with divergent or less stringent privacy laws (Perez, 2022).

Simultaneously, the CLOUD Act empowers U.S. authorities to compel data disclosures from American companies, even if the data is stored abroad. This creates situations where a company may be caught between conflicting legal duties—obligated to disclose data under U.S. law while prohibited from doing so under foreign data protection laws (Haagensen, 2023). Such conflicts not only place businesses in precarious legal positions but also strain diplomatic relations and judicial cooperation between states. In some cases, courts have had to mediate these tensions, but judicial rulings are often jurisdiction-specific and fail to establish universally accepted norms.

These jurisdictional dilemmas are further compounded by the use of mutual legal assistance treaties (MLATs), which are slow, bureaucratic, and often ill-suited to the rapid pace of digital communication. As a result, states and corporations alike are exploring alternative mechanisms, such as data access agreements, cross-border privacy rules, and regional compacts, to navigate legal incompatibilities (Ahmed, 2021). However, without harmonized legal standards or coordinated enforcement mechanisms, the risk of legal fragmentation remains high.

Another critical dimension of these conflicts is enforcement. Even when laws are extraterritorial in scope, their practical enforcement depends on jurisdictional presence, mutual recognition, and compliance incentives. Governments often lack the ability to enforce their laws against foreign entities with no physical or economic nexus to their territory. This enforcement gap creates a patchwork of legal effectiveness and reinforces asymmetries in transnational governance. For instance, while large technology firms may comply with GDPR to maintain access to the EU market, smaller firms or those without EU ties may disregard these obligations without consequence (Ghadery, 2021).

The lack of coherence in legal approaches to cross-border data governance poses a fundamental challenge to the development of a stable and predictable digital order. It undermines trust among states, creates barriers to innovation, and exposes individuals to inconsistent protections. As scholars have emphasized, the solution may lie not in the assertion of unilateral jurisdiction, but in the creation of transnational legal frameworks that respect sovereignty while promoting interoperability and rights-based governance (Kotiswaran & Palmer, 2021). Achieving this balance will require sustained dialogue, institutional innovation, and a commitment to legal pluralism that accommodates diverse normative traditions without sacrificing legal certainty or human dignity.

5. Key Legal Dilemmas in Transnational Governance

5.1. Sovereignty vs. Openness

One of the most prominent legal tensions in contemporary transnational governance arises from the clash between the traditional notion of state sovereignty and the foundational principles of an open, interconnected internet. As states increasingly assert digital sovereignty through legislation, infrastructure controls, and policy frameworks, the vision of a borderless, globally integrated internet is being challenged. Digital sovereignty, in this context, is often invoked as a response to geopolitical anxieties, concerns over foreign surveillance, and the perceived loss of control over data generated within national territories. Governments argue that without the ability to regulate digital infrastructure and cross-border data flows, they cannot fulfill their constitutional obligations to protect national security, ensure economic independence, and uphold the rights of their citizens (Lilipaly et al., 2023). This defensive posture has led to a proliferation of data localization mandates, national cloud projects, and restrictions on foreign digital service providers.

However, such assertions of sovereign control stand in sharp contrast to the principles of the open internet and global digital trade, which rely on interoperability, seamless data mobility, and minimal barriers to information exchange. The open internet has long been

promoted by international organizations, civil society actors, and many private sector stakeholders as a means to enhance innovation, promote free expression, and enable equitable access to knowledge and services. In this vision, cyberspace should remain a shared global commons, governed by decentralized, multi-stakeholder processes rather than unilateral national decisions (Sourgens et al., 2024). The legal architecture supporting openness includes frameworks like the WTO's General Agreement on Trade in Services and cross-border privacy rules that promote regulatory alignment and mutual recognition.

The tension between sovereignty and openness becomes especially visible in multilateral settings where divergent regulatory philosophies compete for dominance. While some countries support binding international rules that facilitate open data flows and reduce digital trade barriers, others insist on maintaining sovereign prerogatives to regulate data according to national interests. This divergence undermines consensus in international forums such as the WTO's Joint Statement Initiative on E-Commerce, where negotiations have been slowed by disagreements over the permissibility of data localization and source code disclosure requirements (Goode, 2023). The European Union, for example, has promoted a rights-based approach that seeks to reconcile digital openness with strong privacy protections under the GDPR, whereas countries like China and Russia have emphasized absolute control over domestic digital ecosystems, citing national security and cultural integrity concerns (Jiang et al., 2022).

In evaluating the legitimacy of digital sovereignty within multilateral legal regimes, it is essential to consider both the historical evolution of sovereignty and the unique characteristics of cyberspace. Traditional international law grants states the right to regulate activities within their borders, but cyberspace challenges the spatial assumptions that underpin this right. Digital interactions routinely transcend national boundaries, often involving multiple jurisdictions simultaneously. This raises questions about whether unilateral assertions of control are legally and practically viable, especially when they impose obligations or restrictions on foreign entities without due regard for international comity or reciprocal enforcement mechanisms (Joerges, 2023). The legitimacy of digital sovereignty, therefore, hinges on its compatibility with broader norms of international cooperation, proportionality, and respect for transnational rights.

Yet, limiting digital sovereignty purely in the interest of openness can also be problematic. For states in the Global South or those lacking technological autonomy, unregulated openness may expose them to exploitation by powerful foreign tech firms, data colonialism, and the erosion of local cultures and industries. Advocates of postcolonial legal critique argue that digital sovereignty can serve as a form of self-determination, enabling states to shape their digital futures and protect their populations from external dominance (Sarcar, 2024). This perspective calls for a nuanced understanding of sovereignty not as a barrier to cooperation, but as a necessary precondition for equitable participation in global digital governance.

5.2. Fragmentation of Legal Norms

The rapid and uncoordinated proliferation of national laws regulating digital data has given rise to significant legal fragmentation in the transnational governance of cyberspace. As countries adopt divergent legal standards for data protection, cybersecurity, digital taxation, and platform regulation, the global legal landscape becomes increasingly disjointed. This fragmentation is not merely a matter of technical inconsistency; it reflects deeper political and normative divergences that make harmonization difficult. Legal scholars have emphasized that this trend undermines the predictability and coherence essential for both public governance and private enterprise (Leonelli, 2021).

One clear example of such fragmentation is the discrepancy between the EU's GDPR and the U.S. approach to data regulation. While the GDPR enshrines a comprehensive and enforceable set of rights for individuals and imposes strict conditions on international data transfers, the U.S. legal regime remains largely sectoral and driven by law enforcement priorities. The incompatibility between these regimes has led to repeated legal disputes, including the invalidation of data transfer frameworks such as the EU-U.S. Privacy Shield by the Court of Justice of the European Union, which found that U.S. surveillance practices violated fundamental rights under EU law (Haagensen, 2023). These rulings create uncertainty for businesses

relying on cross-border data flows and complicate efforts to develop shared compliance mechanisms.

In addition to transatlantic discrepancies, legal fragmentation is evident in Asia, where countries such as India, South Korea, Japan, and China have adopted varied and often conflicting approaches to data governance. India's proposed data protection framework, for instance, includes extensive localization requirements and government access provisions, while Japan has signed agreements recognizing the adequacy of EU data protection standards (An, 2022). China's data laws prioritize national security and require extensive pre-transfer assessments, adding another layer of regulatory divergence (Feng, 2023). These inconsistencies create a patchwork of obligations that multinational companies must navigate, increasing compliance costs and legal exposure.

Legal fragmentation also affects enforcement and judicial cooperation. With different jurisdictions asserting their own regulatory models and enforcement priorities, there is little incentive or ability to coordinate cross-border investigations, resolve disputes, or ensure consistent remedies for rights violations. This lack of coordination is particularly evident in cases involving global technology firms accused of violating multiple national laws. These firms may face concurrent investigations, conflicting court orders, or contradictory compliance demands, leading to a phenomenon legal scholars describe as "jurisdictional collision" (Ghadery, 2021).

The implications for global interoperability are profound. When legal regimes are misaligned, it becomes difficult to develop common standards for data transfer, authentication, encryption, or liability. Technical solutions such as data sandboxes, federated systems, or regional data hubs may alleviate some tensions, but they cannot substitute for legal harmonization. Moreover, fragmentation undermines the normative foundations of international law by weakening the principle of legal certainty and eroding mutual trust between states (Marco, 2021). In this context, efforts by organizations like the OECD to promote cross-border privacy rules and interoperability frameworks are crucial, but their non-binding nature limits their effectiveness in compelling alignment (Duval, 2022).

From a legal theory perspective, the challenge is to reconcile pluralism with coherence. While legal diversity reflects the legitimate sovereignty of states and their varying social values, excessive divergence risks turning the digital domain into a legal minefield. The goal should not be uniformity but interoperability: legal systems should be able to coexist without undermining each other's core principles or creating untenable burdens for transnational actors. Achieving this requires sustained normative dialogue, reciprocal recognition mechanisms, and the development of shared regulatory baselines that respect local autonomy while enabling global cooperation.

5.3. Human Rights and Data Protection

Safeguarding fundamental human rights in an increasingly fragmented digital world presents a formidable challenge, particularly in relation to privacy, freedom of expression, and access to information. These rights, enshrined in international legal instruments such as the International Covenant on Civil and Political Rights, are increasingly exercised and restricted online. The regulation of cross-border data flows directly impacts these rights, especially when personal information is transferred to jurisdictions with weaker legal protections or different normative standards. The disparity in data protection regimes across countries means that individuals may lose meaningful control over their personal data once it crosses a border (Ahmed, 2021).

The GDPR has set a global benchmark by establishing a strong rights-based framework that includes data minimization, purpose limitation, and explicit consent. It empowers individuals with enforceable rights such as access, rectification, and erasure of personal data, and imposes accountability mechanisms on data controllers and processors. However, not all countries provide equivalent protections. In many jurisdictions, privacy rights are either weakly defined or subordinated to state interests such as surveillance, censorship, or national security (Du, 2022). This divergence creates scenarios where data transferred from a rights-respecting jurisdiction may be subject to mass surveillance or unauthorized use in another, without effective legal recourse for affected individuals (Perez, 2022).

Freedom of expression also suffers when states impose content-based restrictions or mandate platform censorship under vague or overly broad digital regulations. In authoritarian contexts, digital

sovereignty is often invoked to justify internet shutdowns, surveillance of dissidents, or the blocking of foreign websites and services. These practices violate international human rights norms and restrict the civic space necessary for democratic participation. Even in democratic societies, debates continue over the extent to which private platforms can moderate content without infringing on free speech or enabling disinformation (Liu, 2024).

The extraterritorial nature of digital regulation complicates accountability for rights violations. When a company based in one jurisdiction processes data collected in another and stores it in a third, determining which legal framework applies and where remedies should be sought becomes a complex legal puzzle. Victims of data misuse or censorship often face insurmountable barriers in seeking redress, especially when responsible actors are shielded by sovereign immunity, lack a presence in the victim's country, or operate under divergent legal standards (Canfield, 2021). Moreover, the growing privatization of digital governance—where corporate actors control large segments of the online environment—raises questions about the applicability of human rights obligations to non-state entities (Kotiswaran & Palmer, 2021).

To address these challenges, some scholars advocate for the recognition of transnational digital rights that bind both states and corporations, regardless of jurisdiction. This would require a paradigm shift in international law, emphasizing the universality of rights over the territoriality of regulation. Others suggest strengthening mechanisms for international cooperation, such as mutual legal assistance treaties, global oversight bodies, and cross-border data trusts that operate under shared legal and ethical principles (Canfield, 2023).

Ultimately, ensuring that human rights are respected in cross-border data governance demands more than legal technicalities—it requires a commitment to global justice, inclusive governance, and ethical responsibility. As data becomes increasingly central to personal identity, economic opportunity, and political participation, the legal systems that govern its flow must be designed to uphold the dignity and autonomy of individuals, regardless of where they reside or which platform they use. This is not merely a regulatory challenge but a moral imperative in the digital age.

6. Toward Harmonization or Strategic Decoupling?

The future of global digital governance stands at a crossroads, where efforts toward legal harmonization compete with rising trends of strategic decoupling. This dichotomy reflects the struggle between building inclusive, interoperable frameworks that facilitate the free flow of data and asserting national control over information as a means of protecting economic, political, and cultural interests. On one side of the spectrum are initiatives that aim to develop cohesive, rule-based systems for transnational data governance. Organizations like the Organisation for Economic Co-operation and Development (OECD) and G20 digital economy groups have taken the lead in encouraging international cooperation and trust-based models for managing cross-border data flows. On the other side is a growing emphasis on digital sovereignty and data protectionism, especially among states that view the control of digital infrastructure as essential to safeguarding national interests. These competing impulses underscore the legal, geopolitical, and ethical challenges inherent in governing the global digital space. The OECD has played a pivotal role in shaping norms and guidelines for the governance of cross-border data flows, particularly through its frameworks on privacy, data protection, and digital security. Its 2013 revised guidelines on the protection of privacy and transborder flows of personal data emphasized principles such as accountability, transparency, and user empowerment, all intended to facilitate international data transfers while safeguarding individual rights (Feng, 2023). More recently, the OECD has advanced the concept of trusted government access to personal data held by the private sector, seeking to harmonize practices and build consensus on acceptable limitations for state surveillance. This initiative reflects a broader recognition that divergent surveillance regimes and regulatory fragmentation hinder trust and cooperation among jurisdictions. The OECD's approach remains voluntary and non-binding, yet its normative influence has been significant, especially among developed economies that align with its liberal democratic values.

Similarly, G20 digital economy groups have taken steps to promote regulatory coherence through frameworks that support digital innovation and inclusiveness. The G20 Osaka Leaders' Declaration in 2019 introduced the

concept of "Data Free Flow with Trust" (DFFT), which acknowledges the importance of unrestricted data movement while emphasizing the need for trust-enhancing regulatory standards. This initiative was designed to reconcile the global nature of data flows with national concerns about privacy, cybersecurity, and consumer protection (Goode, 2023). However, despite its ambitious rhetoric, the implementation of DFFT has faced serious challenges. Not all G20 members share the same views on data governance, and the absence of enforceable commitments has limited the initiative's effectiveness in bridging legal divides.

The limitations of these harmonization efforts are particularly evident in the continued divergence of national data laws. Countries like China, Russia, and India have advanced comprehensive regulatory frameworks that prioritize domestic control over data infrastructure and restrict outbound data transfers. China's Personal Information Protection Law (PIPL), for example, imposes strict conditions on cross-border data transfers, requiring security assessments and contractual guarantees that align with state-prescribed standards (Jiang et al., 2022). The law reflects a broader strategy of digital protectionism, where data is treated not merely as a resource to be governed but as a sovereign asset integral to national development and security. In Russia, data localization laws mandate that personal data collected from Russian citizens be stored and processed on servers located within the country, a requirement enforced through blocking measures and financial penalties against non-compliant entities (Lilipaly et al., 2023).

This turn toward strategic decoupling signals a departure from the earlier liberal vision of a unified, global internet. Strategic decoupling entails the deliberate disentanglement of digital infrastructure, standards, and supply chains between major geopolitical blocs. The concept has gained traction in the wake of escalating tensions between the United States and China, where concerns over national security, technological dependence, and cyber espionage have prompted calls for digital self-reliance. In the United States, legislative actions restricting the use of Chinese technology in telecommunications infrastructure, combined with export controls on advanced semiconductors, exemplify a policy direction that prioritizes strategic autonomy over global integration (Sarcar, 2024). This orientation is mirrored in China's promotion of indigenous innovation and efforts to build a sovereign internet that minimizes reliance on Western platforms and protocols (An, 2022). Strategic decoupling also reflects a shift in how states conceptualize digital resilience. Rather than viewing interdependence as a stabilizing force, policymakers increasingly regard it as a vulnerability to be mitigated through national capacity-building and diversification. Legal scholars have warned that such strategies may lead to a balkanization of the internet, where incompatible technical standards and regulatory regimes erect barriers to interoperability and inhibit global cooperation (Leonelli, 2021). In this fragmented environment, the risk is that countries will prioritize short-term strategic interests over long-term collective gains, undermining trust and institutional coordination in the process.

Despite these centrifugal forces, there remain avenues for reinvigorating transnational legal cooperation. One promising direction is the development of interoperability mechanisms that enable legal systems to function alongside each other without requiring full harmonization. This model, sometimes referred to as "functional equivalence," allows jurisdictions to recognize foreign legal regimes as adequate or compatible, provided they achieve comparable outcomes in terms of rights protection and accountability (Perez, 2022). The EU's adequacy decisions under the GDPR illustrate this approach, wherein the European Commission assesses whether a third country offers a level of data protection essentially equivalent to that of the EU. While the adequacy process is rigorous and politically sensitive, it provides a pathway for legal recognition without requiring the wholesale adoption of EU norms.

Another potential mechanism for cooperation is the establishment of bilateral or regional data transfer agreements, modeled after the APEC Cross-Border Privacy Rules (CBPR) system. These agreements enable participating economies to develop shared accountability standards and promote business interoperability while respecting local legal traditions. Although the CBPR system has not achieved global adoption, it offers a template for flexible, scalable cooperation that balances regulatory diversity with the need for shared governance (Canfield, 2023). Regional frameworks, such as the African Union's Convention on

Cyber Security and Personal Data Protection and the ASEAN Framework on Digital Data Governance, also demonstrate the potential for South-South cooperation in shaping alternative governance models based on local priorities and collective bargaining power (Mahardika, 2022).

Furthermore, the rise of transnational legal networks involving regulators, judges, and scholars can facilitate normative convergence through informal exchanges and capacity-building initiatives. These networks, often organized around issue-specific forums or academic collaborations, help disseminate best practices, interpret complex legal developments, and foster mutual understanding across legal cultures (Duval, 2022). Such interactions contribute to the gradual alignment of legal concepts and regulatory philosophies, even in the absence of formal treaties or harmonized legislation. For example, judicial dialogues between the Court of Justice of the European Union and constitutional courts in other jurisdictions have influenced the interpretation of privacy rights and data protection principles across borders (Haagensen, 2023).

At the same time, it is important to recognize the role of private actors in shaping the future of transnational data governance. Large technology firms, standard-setting bodies, and advocacy organizations wield significant influence over the design, implementation, and evolution of digital regulation. Their participation in multi-stakeholder initiatives and policy consultations can either bridge or deepen the gap between national and international norms. For instance, private companies that operate globally often advocate for clear, consistent rules to reduce compliance burdens and enhance legal certainty. Some have voluntarily adopted global data protection standards that exceed domestic legal requirements in order to maintain user trust and regulatory legitimacy (Canfield, 2021). However, critics argue that relying on corporate self-regulation risks privileging business interests over public accountability and may reinforce existing power imbalances in digital governance (Kotiswaran & Palmer, 2021).

Looking ahead, the trajectory of transnational legal governance in the digital domain will likely depend on the ability of states and institutions to reconcile the dual imperatives of sovereignty and cooperation. A purely nationalist approach risks entrenching fragmentation and undermining the universality of digital rights. Conversely, overly ambitious harmonization efforts that ignore local contexts and asymmetries may provoke resistance and exacerbate inequalities. The path forward requires a principled pluralism—an approach that embraces diversity while building common ground through dialogue, mutual respect, and legal interoperability.

The future of harmonization or strategic decoupling is not predetermined. It will be shaped by political will, normative commitments, and institutional innovation. Whether the global community can move toward a shared legal framework for data governance or continues down a path of fragmentation and rivalry will depend on the choices made in this pivotal moment. Ultimately, the legitimacy and resilience of transnational digital governance hinge on the development of legal systems that are both adaptive and principled—capable of addressing the dynamic realities of cyberspace while upholding the foundational values of human dignity, accountability, and collective security.

7. Conclusion

The governance of cross-border data flows and the assertion of digital sovereignty present one of the most significant legal challenges of the contemporary era. As the world becomes increasingly interconnected through digital networks, the legal frameworks that govern data must grapple with issues that transcend traditional territorial boundaries. The core dilemma lies in balancing the legitimate interests of states to regulate data within their jurisdictions with the need to preserve the openness, interoperability, and universality of the global internet. This tension has created a fragmented and often contradictory legal landscape, where national laws, regional regulations, and international initiatives frequently collide rather than converge.

The concept of digital sovereignty has gained prominence as states seek to reassert control over the data generated within their borders, often in response to concerns over foreign surveillance, technological dependence, and the dominance of global technology firms. While these concerns are not unfounded, the rise of digital sovereignty has often manifested in the form of restrictive policies such as data localization laws, national cloud mandates, and unilateral regulatory assertions. These measures, while aimed at safeguarding national interests, risk creating digital silos that hinder

global innovation, restrict the free flow of information, and undermine cooperative governance.

In contrast, efforts to harmonize data governance through international and regional frameworks reflect an aspiration to build a cohesive legal order that facilitates digital trade, protects individual rights, and promotes global collaboration. Initiatives led by the OECD, the G20, and other multilateral institutions have sought to create common principles and accountability standards that can guide cross-border data flows. However, these efforts have faced significant obstacles due to divergent regulatory philosophies, geopolitical rivalries, and the absence of enforceable commitments. The result is a patchwork of legal regimes that businesses, governments, and individuals must navigate, often with considerable legal and operational uncertainty.

At the heart of the current impasse is a deeper conflict between two visions of the digital future. One envisions a globally integrated digital ecosystem governed by shared norms, open standards, and multistakeholder participation. The other prioritizes national autonomy, strategic decoupling, and the development of sovereign digital infrastructures. Both models carry benefits and risks. A globally integrated system offers efficiency, scale, and broad access to knowledge and services, but it may also concentrate power in the hands of a few dominant actors and expose states to external vulnerabilities. Conversely, a sovereignty-driven model may enhance national control and protect cultural and economic interests, but it risks isolating countries from global opportunities and fragmenting the legal foundations of cyberspace.

Amid these competing pressures, the way forward must involve a pragmatic and principled approach to legal pluralism. Rather than seeking full uniformity or absolute independence, states and institutions should aim for interoperability—legal frameworks that respect national differences while ensuring compatibility and mutual recognition. This requires ongoing dialogue, trust-building, and the development of mechanisms that allow for reciprocal oversight, rights protection, and data mobility. The concept of functional equivalence, where different legal systems are accepted as providing comparable levels of protection, offers a promising path for reconciling divergent approaches.

Equally important is the recognition that digital governance is not solely the domain of states. Private actors, civil society organizations, and transnational networks play a crucial role in shaping the rules and norms that govern the digital environment. Their participation in norm-setting processes, standard development, and policy consultations adds critical perspectives and contributes to a more inclusive and balanced governance model. As data becomes increasingly central to economic, political, and social life, ensuring that its governance reflects broad and diverse interests is essential to legitimacy and resilience.

The future of cross-border data governance will depend on the ability of the international community to move beyond zero-sum approaches and toward shared responsibility. The current moment offers both a challenge and an opportunity: a challenge to overcome legal fragmentation, distrust, and unilateralism, and an opportunity to design a global data governance system that upholds fundamental rights, fosters innovation, and reinforces cooperation across borders. Navigating this path will require legal creativity, political commitment, and a shared vision of digital justice that transcends national boundaries while honoring local contexts. Only through such a balanced and collaborative approach can the promise of the digital age be fully realized for all.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Ahmed, A. (2021). Transnational Legal Orders and Global Health. 203-216. https://doi.org/10.1093/oxfordhb/9780197547410.013.9

An, Y. (2022). Study on the Legal Regulation of Multinational Corporations on Environmental Human Rights. https://doi.org/10.2991/aebmr.k.220603.066

Canfield, M. (2021). Transnational Food Law. 269-290. https://doi.org/10.1093/oxfordhb/9780197547410.013.12

Canfield, M. (2023). The Anthropology of Legal Form: Ethnographic Contributions to the Study of Transnational Law. *Law & Social Inquiry*, *48*(1), 31-47. https://doi.org/10.1017/lsi.2022.19

Crowley, K., Stewart, J., Kay, A., & Head, B. (2020). Reconsidering Borders. 75-96. https://doi.org/10.1332/policypress/9781447333111.003.0005

Du, Z. (2022). Human Rights Violations by Multinational Corporations and the Outlet to Judical Difficulties. https://doi.org/10.2991/aebmr.k.220603.108

Duval, A. (2022). Taking Feminism Beyond the State: FIFA as a Transnational Battleground for Feminist Legal Critique. *International Journal of Constitutional Law*, *20*(1), 277-298. https://doi.org/10.1093/icon/moac019

Feng, C. J. (2023). The Human Rights Obligations of Multinational Corporations and Their Regulation. *Highlights in Business Economics and Management*, *16*, 394-400. https://doi.org/10.54097/hbem.v16i.10605

Ghadery, F. (2021). Contextualization as a (Feminist) Method for Transnational Legal Practice. 707-726. https://doi.org/10.1093/oxfordhb/9780197547410.013.32

Goode, R. (2023). Transnational Commercial Law and Impediments to Its Development. 319-336. https://doi.org/10.1093/oso/9780198889762.003.0019

Haagensen, N. (2023). Legal Strategies at the Governance Precipice: Transnational Lawyers in the European Union's Sovereign Debt Crisis (2010–2012). *Law & Social Inquiry*, *49*(3), 1715-1746. https://doi.org/10.1017/lsi.2023.67

Jiang, A., Zong, W., & Shi, Q. (2022). Cooperation Between China and ASEAN in Combating Wildlife Trade Under the Framework of Regional Legal System. *Asia Social Science Academy*, *9*(1), 75-94. https://doi.org/10.51600/jass.2022.9.1.75

Joerges, C. (2023). Transnational Constitutionalism – Conflicts-law Constitutionalism – Economic Constitutionalism: The Exemplary Case of the European Union. *Journal of Law and Society*, *50*(S1). https://doi.org/10.1111/jols.12438

Kotiswaran, P., & Palmer, N. (2021). Transnational Criminal Law: A Field in the Making. 179-202. https://doi.org/10.1093/oxfordhb/9780197547410.013.8

Leonelli, G. C. (2021). The Postmodern Normative Anxiety of Transnational Legal Studies. 113-132. https://doi.org/10.1093/oxfordhb/9780197547410.013.5

Lilipaly, N. F., Tuhulele, P., & Daties, D. R. A. (2023). Pertanggungjawaban Pelaku Penyelundupan Migran Lintas Negara Ditinjau Dari Hukum Internasional. *Tatohi Jurnal Ilmu Hukum*, *3*(7), 651. https://doi.org/10.47268/tatohi.v3i7.1850

Liu, D. (2024). Borderline Content and Platformised Speech Governance: Mapping TikTok's Moderation Controversies in South and Southeast Asia. *Policy & Internet*, *16*(3), 543-566. https://doi.org/10.1002/poi3.388

Mahardika, A. G. (2022). Politik Hukum Dalam Penanganan Covid-19: Pendekatan Yuridis Dalam Sistem Hukum Indonesia. *Yurispruden Jurnal Fakultas Hukum Universitas Islam Malang*, *5*(2), 211. https://doi.org/10.33474/yur.v5i2.9005

Marco, A. D. (2021). Sports Economy and Fight Against Corruption: Which Limits to the Sporting Organisations Autonomy? *European Business Law Review*, *32*(Issue 5), 877-904. https://doi.org/10.54648/eulr2021031

Minas, S. (2021). Transnational Legal Education in China. 1137-1152. https://doi.org/10.1093/oxfordhb/9780197547410.013.52

Perez, O. (2022). Transnational Networked Authority. *Leiden Journal of International Law*, *35*(2), 265-293. https://doi.org/10.1017/s0922156521000728

Sarcar, A. (2024). Circumventing the Nation: How to Develop a Postcolonial Archive on Public Health in India. *Revue Internationale Des Études Du Développement*, *256*, 203-226. https://doi.org/10.4000/131ll

Sourgens, F. G., Baldwin, E., & Banet, C. (2024). The Transnational Law of Renewable Energy. https://doi.org/10.1093/law/9780198894520.001.0001