PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 5 October 2025

Conflict and Coordination Between Data Sovereignty and Digital Trade Liberalisation: An Analysis of Cross-Border Data Flow Policies in China and the EU

Xun Zhu[1]

[1] National University of Singapore, Singapore
Correspondence: Xun Zhu, National University of Singapore, Singapore.

doi:10.56397/SLJ.2025.10.07

Abstract

The digital economy faces a fundamental contradiction between the principles of digital trade liberalisation and the emerging demands of data sovereignty. This study analyzes this tension by conducting a comparative examination of the data governance frameworks of China and the European Union (EU). It contrasts China's state-centric approach with the EU's human rights-oriented model. The analysis demonstrates how these divergent models create significant non-tariff barriers to digital trade, clashing with the international liberalisation principles. It proposes several pathways for coordination to mitigate this tension. These include philosophical alignment on global justice, perfecting international trade rules with clear security exceptions, and strengthening regulatory cooperation.

Keywords: data sovereignty, digital trade liberalisation, cross-border data flow, international trade law

1. Introduction

In today's worldwide economic landscape, digital commerce and data transfer have brought about a radical transformation in the essence and extent of international business transactions. As data becomes a strategic resource, cross-border data flow supports all aspects of modern commerce, from supply chain management to digital service provision. [1] However, this digital transformation has created a fundamental contradiction between the principle of trade liberalisation and the idea of data sovereignty.[2] The "pre-internet" consensus, as represented by the agreements of the World Trade Organization (WTO), centered around facilitating the unhindered movement of goods and services across national borders.[3] Today, however, stakeholders in both developed and developing nations increasingly advocate

[1] Lateef MA. (2025). Digital Sovereignty in Global Trade: Analysing WTO Governance of Data Flows. *Beijing Law Review*, *16*, 875.

[2] Gao HS. (2021). Data Sovereignty and Trade Agreements: Three Digital Kingdoms. *SSRN Electronic Journal*.

[3] Appleton B. (2025). Digital Sovereignty vs. Trade Liberalization: India's Algorithm Disclosure Dilemma. Balsillie Case Studies. <https://balsilliecases.ca/case-study/digital-sovereignty-vs-trade-liberalization-indias-algorithm-disclosure-dilemma/> accessed 20 October 2025.

sovereign control of the data generated within their territories, citing concerns over national security, economic policy and citizens' privacy.[1] This has resulted in a "fragmentation of data privacy laws", creating legal uncertainty and threatening the integrity of the worldwide digital economy.[2]

At the heart of the conflict lies the matter of how cross-border data movements ought to be regulated within the context of international trade regulations. This study aims to tackle this issue by conducting a comparative examination of the data management systems in China and the EU. First, it establishes the theoretical foundations by contrasting the notion of data sovereignty with the principles of trade liberalisation. Second, it conducts a comparative analysis of Chinese and EU legal policies, identifying specific points of the conflict. Finally, it explores potential pathways for coordination, with the aim of establishing a sustainable equilibrium between the justifiable authority to regulate and the necessity of open digital commerce.

2. Theoretical Foundations of Data Sovereignty and Digital Trade Liberalisation

2.1 Data Sovereignty: Concept, Models, and Developments in the Digital Age

Sovereignty serves as a cornerstone of international law and a fundamental principle guiding international relations. Jean Bodin, the 16th-century thinker, was among the first to articulate a systematic theory of sovereignty, defining it as the "absolute and perpetual power of a commonwealth", a supreme authority unrestrained by the laws it creates.[3] The Dutch jurist Hugo Grotius further developed the international dimensions of sovereignty, analysing its internal and external perspectives. Internally, sovereignty denotes a state's right to control persons, events and things within its territorial boundaries. Externally, it denotes a state's right to be free from interference by other sovereign states.[4]

The advent of the digital age has extended this principle into a new domain. Data sovereignty and cyberspace sovereignty are now considered developments in sovereignty theory. Scholars generally consider data sovereignty as originating from cyber sovereignty, viewing it as a subset thereof.[5]

While data itself is intangible, it possesses certain physical attributes. Network data storage and infrastructure are typically located within a country's borders, and storage devices are usually owned by the state or corporations. Data transmission relies on national infrastructure such as power grids and cables. [6] The implementation of the idea of state sovereignty to data includes data storage devices within a nation's territory, which may be located in its territorial waters, land, or airspace. Under this framework, unauthorized access to data and its storage infrastructure by a foreign state is construed as a violation of the host state's sovereignty.[7]

2.2 Digital Trade Liberalisation: Core Principles Under the GATS Framework

Under the World Trade Organization (WTO), the General Agreement on Trade in Services (GATS)[8] has been set up. It serves as the main multilateral tool for regulating service trade, which encompasses digital or cross-border services. Its objective is to build a dependable and foreseeable framework of regulations for international service trade and to promote its gradual liberalisation.

The GATS places general duties on member states that are critical for digital trade. Article II establishes the principle of Most-Favoured-Nation Treatment. [9] This principle mandates that the WTO members should not show discrimination among their trading partners. Article XVII contains the obligation of National Treatment.[10] It states that member countries must treat foreign services

[1] Bradford A. (2023). *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

[2] Li L. (2025). Data Sovereignty and National Security: Governance Challenges and Pathways in the Digital Age. *Global Review of Humanities, Arts, and Society*, *1*, 49.

[3] Pohle J and Thiel T. (2020). Digital Sovereignty. *Internet Policy Review*, *9*.

[4] Diesselhorst M. (1982). Hugo Grotius and the Freedom of the Seas. *Grotiana*, *3*, 11.

[5] Newman H. (2021). *OF PRIVACY and POWER: The Transatlantic Struggle over Freedom and Security.* Princeton University Press.

[6] Pierucci F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, *4*.

[7] Dan Jerker B Svantesson. (2017). *Solving the Internet Jurisdiction Puzzle*. Oxford University Press.

[8] General Agreement on Trade in Services (adopted 15 April 1994, entered into force 1 January 1995) 1869 UNTS 183 ('GATS').

[9] ibid art II.

[10] ibid art XVII.

and service providers at least as favorably as their domestic counterparts. However, this is subject to the conditions and limitations specified in their schedules of commitments.

Despite these foundational principles, the GATS framework is structurally ill-equipped to address the realities of the modern digital economy for several reasons.[1] First, it was negotiated and concluded before the widespread commercialisation of the internet, and thus contains no specific provisions on digital commerce, data circulation and data localisation. Second, it is not clear whether digital products ought to be regarded as "merchandise" under the General Agreement on Tariffs and Trade or as "services" under the GATS. This differentiation has substantial legal and economic ramifications. Third, the core GATS duties of market entry and national treatment are applicable only to those service sectors that a member has explicitly included in its schedule of commitments. This approach of using a positive list means that many digitally service sectors remain outside the scope of binding liberalisation commitments for a majority of the WTO members. This legal vacuum has allowed the divergent models of data sovereignty to flourish with few multilateral constraints, setting the stage for direct conflict.

3. Manifestations of Conflict in EU-China Cross-Border Data Flow Policies

3.1 Different Value Orientations Toward Data Sovereignty in Digital Trade

3.1.1 The China Model: Security-Oriented Approach

China's approach to data governance is explicitly state-centric, driven by the dual objectives of national security and economic development. The guiding philosophy is "cyber sovereignty", which treats cyberspace as a domain subject to the same principles of state control as physical territory. Within this framework, data is viewed not primarily as a private asset or personal right, but as a strategic national resource and a "fifth factor of production" in conjunction with land, labour, capital and technology.

The model is operationalized through a complex legal system, comprising the Personal Information Protection Law (PIPL), the Data Security Law (DSL) and the Cybersecurity Law (CSL). The system creates a hierarchical framework for data categorization according to its significance to the national interest. The DSL delineates "important data" and "core national data". The latter pertains to information pertaining to national security, the vital arteries of the national economy, crucial elements of people's daily lives and substantial public interests. Such kind of data is subject to the most stringent regulations, including mandatory data localisation requirements for Critical Information Infrastructure (CII) operators and stringent security assessments carried out by the Cyberspace Administration of China (CAC) before any transfer across national borders. This essentially establishes a data export licensing method, reflecting the core principle that the state has final rights of control over data generated within the border.[2]

3.1.2 The EU Model: Human Rights-Oriented Approach

The EU model operates on a human rights-oriented strategy. It assigns significant importance to the safeguarding of basic human rights. It is committed to ensuring that these rights are respected even outside its geographical limits, either through the domestic law of the recipient country or by specific contractual arrangements.

This principle was tested many times by the transatlantic data flow frameworks. The EU-US Safe Harbor Agreement (invalidated by the Court of Justice of the European Union in 2015),[3] and its successor, the Privacy Shield (struck down in 2020), were both found to be insufficient.[4] These legal rulings were spurred by concerns about the inappropriate utilization of EU citizens' data and the broad access to such data by US intelligence services, all without providing a degree of protection that was "substantially equivalent".

The implementation of the General Data

[1] Irion K, Yakovleva S and Bartl M. (2016). Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements. *SSRN Electronic Journal*.

[2] Angela Zhang. (2021). *CHINESE ANTITRUST EXCEPTIONALISM: How the Rise of China Challenges Global Regulation*. Oxford University Press.

[3] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, paras 8-10.

[4] Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Schrems II) [2020] ECLI:EU:C:2020:559, paras 12-15.

Protection Regulation (GDPR) [1] in 2018 represented a pivotal juncture, codifying the EU's strict data protection legal standards into a directly applicable regulation. Under the GDPR, when personal data is transferred outside the EU, it is required to adhere to specific binding protective measures and data protection stipulations. Crucially, it prohibits data transfers to jurisdictions where public authorities can access such data without meaningful limitations and where individuals lack effective legal recourse. Compared to the 1995 Directive[2], the GDPR significantly improves data protection requirements, marking a milestone in the fields of data security and personal privacy.

3.2 Digital Trade Liberalisation as a Threat to Data Sovereignty

For states that prioritise data sovereignty, unfettered digital trade poses a direct threat to regulatory autonomy and national interests. The borderless digital market promoted by free-trade poses challenges to the state's ability to enforce domestic laws, safeguard citizens' privacy and maintain national security. This perceived loss of control is a primary driver of data sovereignty measures.

The core of this threat lies in the inherent sensitivity of data. Unrestricted cross-border data flows imply that sensitive information, ranging from personal health records to critical infrastructure data, may be transmitted to and stored in foreign jurisdictions, resulting in major security risks. States fear such data could be accessed by foreign intelligence agencies or subjected to inferior legal standards. For developing states, these anxieties are amplified by fears of "digital colonialism", where the economic value of domestic data is extracted by dominant foreign technology firms, exacerbating existing economic disparities. [3] Consequently, many of the developing states view unfettered data liberalisation as a mechanism that disproportionately benefits a few technologically advanced economies at the expense of broader global security and development. Thus, when entities such as China or the EU implement controls on data outflows, these actions are often not regarded as protectionism but as essential exercises of sovereignty necessary to safeguard citizens and strategic interests.

3.3 Data Localisation as a Barrier to Digital Trade

Following the exposure of major data security incidents, such as Edward Snowden's revelations, global concerns over data security have intensified. In response, numerous countries have enacted data localisation policies. Consequently, non-tariff barriers, traditionally seen in the trade of goods, now emerge in digital trade.[4]

These localisation measures negatively impact the liberalisation in several respects. First, they create significant barriers to market entry and increase compliance costs for multinational corporations. Data localisation regulations stipulate that data has to be kept and processed within the territorial boundaries of a nation. To meet this requirement, multinational corporations must either invest heavily in establishing local servers and data centers or outsource these operations to domestic service providers, both of which raise their costs. A prominent example is China's CSL, which stipulates that operators of CII are required to store all personal details and significant data gathered within China on domestic servers. In cases where data needs to be transferred overseas, it has to undergo a rigorous security evaluation by the CAC. This has become the de facto standard across numerous industries, including finance, energy and transportation, rendering cross-border data transfer the exception rather than the norm. From a trade law perspective, this policy constitutes a clear barrier under the GATS. For multinational corporations, such a regulation can be seen as a violation of market access commitments, as it imposes conditions on the cross-border supply of services that were not specified in the agreement. This, in turn, unfairly hinders their entry into the Chinese market and prevents them from competing on par with domestic

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Date Protection Regulation) [2016] OJ L 119/1 ('GDPR').

[2] Directive 95/46/E C of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[3] Couldry N and Mejias UA. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

[4] Meltzer JP. (2015). The Internet, Cross-Border Data Flows and International Trade. *Asia & the Pacific Policy Studies*, 2, 90.

service suppliers. Second, these measures increase operational costs and reduce trade opportunities for all parties. The free flow of data across borders is instrumental in lowering the costs for businesses to find trading partners and expand overseas. In contrast, data localisation complicates the connection between importers and exporters. [1] This complexity effectively shrinks potential market size and diminishes companies' ability to use data analytics to identify new customers and seize trade opportunities.

4. Pathways to Coordinate Data Sovereignty and Digital Trade Liberalisation

4.1 Philosophical Coordination: Inclusive Development Based on the Values of Global Justice

The construction of a global legal framework is an active and interactive process of coordinated action, joint participation and mutual respect among sovereign states, rather than a hegemonic effort where states compete for dominance and marginalise others. [2] Data security concerns national, public and citizen interests, making international data cooperation a common need for all countries.

First, this requires respecting cultural differences and resisting data hegemony.[3] In the context of globalisation, digital trade has promoted cultural exchange, but it has also triggered conflicts due to differing cultures and value systems across regions. Therefore, international data cooperation must, while respecting and safeguarding the data sovereignty of all nations, construct a global data governance framework that acknowledges and embraces cultural pluralism. All countries should actively promote positive interactions in the digital space and enhance cross-cultural understanding.

Simultaneously, it is imperative to address unequal rights in digital trade. The de facto "data hegemony" restricts the digital economic development of developing countries through extraterritorial measures or market monopolization. To counter these challenges, affected countries should actively coordinate through bilateral or multilateral channels with other countries, regions and international organisations with similar concerns, in order to jointly resist unilateralism and hegemonism.

Second, coordination must involve safeguarding fundamental human rights and strengthening security governance.[4] The ultimate goal of data governance is to promote and protect human rights, and an effective governance model requires comprehensive measures that give equal weight to both technology and law. At the national level, all countries need to strengthen digital infrastructure and develop indigenous technology to narrow the digital divide. Meanwhile, domestic laws must strictly regulate acts that infringe personal privacy and data safeguarding. At the international level, while enjoying the dividends of the digital economy, all countries must jointly assume governance responsibilities, ensuring that the concept of the rule of law pervades every aspect of data-related operations. At the legislative level, a compatible and interoperable system of digital rules should be built through international coordination and cooperation. At the enforcement level, strategic cooperation on cybersecurity should be deepened, establishing effective mechanisms for intelligence sharing and joint operations. At the judicial level, international judicial assistance should be strengthened to jointly combat transnational cybercrime, thereby fostering a stable, transparent and secure global cyber legal environment.

4.2 Rule Coordination: Perfecting the International Legal System for Digital Trade

4.2.1 Formulating Internationally Unified Digital Trade Rules

For a long time, the global digital trade has been dominated by developed states. However, the digital capabilities of developing countries have shown accelerated growth in recent years, accompanied by increasing calls to share in economic and security benefits. This underscores the need for coordination by a unified international organization. The current landscape of international organisations is complex and fragmented across monetary,

[1] AARONSON S. (2015). Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security. *World Trade Review*, *14*, 671.

[2] Kingsbury B, Krisch N and Stewart RB. (2005). The Emergence of Global Administrative Law. *SSRN Electronic Journal*. <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1361&context=lcp> accessed 20 October 2025.

[3] Cohen JE. (2016). The Regulatory State in the Information Age. *Theoretical Inquiries in Law*, *17*.

[4] Dencik L. (2025). "Rescuing" Data Justice? Mobilising the Collective in Responses to Datafication. *Information, Communication & Society*, 1.

investment and trade domains, making it difficult to form a coherent system for data protection. In this context, the WTO is the ideal venue to assume this responsibility. It has extensive experience in rule-making, and it can play a positive role in multilateral negotiations among member states. Furthermore, major economies within the WTO should take the lead. For example, China, Russia, the US and the EU need to break the existing framework and spearhead the drafting of a new multilateral agreement specifically for digital trade. Through negotiation, they can regulate cross-border digital trade, address various legal issues in separate clauses and apply them to specific WTO members.

4.2.2 Establishing Security Exception Clauses for Digital Trades

A more effective approach to rule coordination involves refining the use of exception clauses within digital trade agreements. Both regional and multilateral agreements, like the GATS, the Regional Comprehensive Economic Partnership (RCEP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), include stipulations that enable states to diverge from liberalisation obligations to protect essential public interests.[1] For example, Article XIV of the GATS bis offers a security exemption that permits members to enforce methods deemed "necessary for the protection of essential security interests".[2] Historically, this clause has been largely self-judging, granting significant deference to national governments. However, the WTO jurisprudence, such as the Russia-Measures concerning Traffic in Transit panel report,[3] clarified that the application of security exceptions is subject to a review carried out in good faith and cannot be completely immune from examination.[4]

To prevent abuse and ensure predictability, future digital trade agreements should clarify the scope and application of security exceptions.[5] For example, states could be required to demonstrate a clear and direct link between a data-restrictive measure and a specific, identifiable security threat, rather than relying on vague or broad economic security claims. Agreements could also specify procedural protection, such as notification requirements, transparency obligations and periodic review of security measures. Furthermore, a necessity test could be adopted, requiring states to show that no less restrictive alternative is available to achieve the security objective. Additionally, exceptions could be limited to clearly defined circumstances, such as cyberattacks, threats to critical infrastructure or emergencies in international relations, and be subject to independent dispute settlement review.

4.3 Regulatory Coordination: Strengthening the International Regulatory Mechanism for Digital Trade

4.3.1 Promoting the Integrated Development of Existing Regulatory Models

The slow progress of negotiations for the Trade in Services Agreement and the Transatlantic Trade and Investment Partnership indicates that, given the significant divergences in values and interests among countries, it is extremely challenging to negotiate a universally applicable regime for cross-border data flows.[6] Such attempts are costly and often fail to reach consensus. Therefore, rather than starting from scratch and risking further stalemate, a more pragmatic path is to build upon the existing regulatory models widely accepted by the international community, and to promote interoperability and mutual recognition between different regional paradigms through strengthened cooperation.

Currently, the mainstream global regulations for cross-border data flows follow two typical models. One is the EU model, represented by the GDPR, which relies on "adequacy decisions" for countries or regions supplemented by Standard Contractual Clauses and Binding

[1] Svetlana Yakovleva and Kristina Irion. (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, *10*, 201.

[2] GATS, art XIV *bis*.

[3] WTO, *Russia: Measures Concerning Traffic in Transit* (26 April 2019) WT/DS512/R.

[4] Lapa V. (2020). The WTO Panel Report in Russia -Traffic in Transit: Cutting the Gordian Knot of the GATT Security Exception? *Questions of International Law, Zoom-in*, *69*, 5. <https://www.qil-qdi.org/wp-content/uploads/2020/05/02_WTO-Security-exceptions_LAPA_FIN.pdf> accessed 20 October 2025.

[5] Wenjia Zuo. (2024). General Exceptions in the Digital Trade Environment: Challenges and Reforms under Article 20 of GATT and Article 14 of GATS. *Journal of Education, Humanities and Social Sciences*, *39*, 77.

[6] Lomotey RK, Kumi S and Deters R. (2022). Data Trusts as a Service: Providing a Platform for Multi-Party Data Sharing. *International Journal of Information Management Data Insights*, *2*, 100075.

Corporate Rules (BCRs).[1] The second model is the APEC, exemplified by the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (CBPR) system, which is a co-regulatory model based on the accountability of organisations.[2]

Although rooted in different legal traditions and differing in regulatory intensity, mandatory nature and mechanism flexibility, the two models are not fundamentally incompatible.[3] In essence, both aim to bridge regulatory gaps between jurisdictions and establish acceptable baseline protection standards for the secure and free flow of data within their regions. Specifically, there are points of convergence. First, there is an overlap in their scope of application. The BCRs primarily govern internal data transfers within multinational corporations (MNCs), while the CBPR applies to enterprises in the Asia-Pacific region, including MNCs.[4] Second, their core mechanisms are highly similar. Both require organisations to adopt internal privacy policies that comply with their respective standards. Third, their fundamental principles are aligned in spirit. The basic principles of data processing in the GDPR are highly consistent with the nine core principles of the APEC Privacy Framework, such as purpose limitation and data security. Fourth, both frameworks serve as a baseline. They set a "floor" for data protection standards, not a "ceiling", allowing participating jurisdictions and enterprises to adopt stricter measures beyond the baseline.[5]

In fact, the EU's Article 29 Working Party and the APEC Data Privacy Subgroup have long engaged in dialogue on cross-border enforcement cooperation. The two parties established a joint working group to explore the possibility of achieving mutual recognition and compatibility between the two frameworks based on common principles. They have jointly published "Common Referential on the EU System and APEC System Structures". This reference document provides a detailed analysis of the compliance and certification requirements for the BCR and the CBPR, and offers an informal practical checklist for enterprises seeking joint certification.

If the two models eventually achieve institutional integration, data could potentially flow freely between CBPR-certified and BCR-approved organisations, exempting them from duplicate certification. Although this mutual recognition is still in preliminary stages, the close economic and trade ties between the EU and the APEC region will undoubtedly drive further cooperation.

4.3.2 Establishing a Cooperative Organisation for Inter-Regional Data Supervisory Authorities

To fully realise the potential of cross-border data flows for sustainable digital trade, all stakeholders must act in a coordinated, unified and cross-industry manner. Internet platforms naturally transcend geographical limitations, connecting data subjects across different legal jurisdictions and involving the legal systems of multiple countries.[6] When cross-border data flows give rise to legal disputes, issues such as the extraterritorial effect of domestic laws, choice of law and the extraterritorial enforcement of judgments emerge. Crucially, national data supervisory authorities are limited by their sovereign borders and lack the capacity to effectively supervise data once it has left their country. In view of this, it is difficult to ensure that the rights of data subjects are adequately protected and effectively remedied by relying solely on the data supervision and enforcement agencies of a single country.[7] Therefore, international cooperation mechanisms are crucial to the global governance of cross-border data flows.

This requires the establishment of regional cooperative organisations for data supervision to foster dialogue and cooperation among

[1] GDPR, art 45.

[2] Graham Greenleaf. (2019). Global Convergence of Data Privacy Standards: EU GDPR and APEC CBPR Compared. *International Data Privacy Law*, *34*, 85.

[3] Marfia F, Fornara N and Nguyen T-VT. (2017). A Framework for Managing Data Provider and Data Consumer Semantic Obligations for Access Control. *AI Communications*, *30*, 67.

[4] Zrenner J et al. (2019). Usage Control Architecture Options for Data Sovereignty in Business Ecosystems. *Journal of Enterprise Information Management*, *32*, 477.

[5] Zhu J. (2021). The Personal Information Protection Law: China's Version of the GDPR? *Columbia Journal of Transnational Law Bulletin*.

[6] Sullivan C. (2019). EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era. *Computer Law & Security Review*, *35*, 380.

[7] Cappiello C et al. (2019). Data Ecosystems: Sovereign Data Exchange among Organizations (Dagstuhl Seminar 19391). *Dagstuhl reports*, *9*, 134.

regulatory authorities. [1] In recent years, recognising the complexity of regulating cross-border data flows, various jurisdictions including the EU, South Korea, Japan and Singapore have established data supervisory authorities. Against this background, a cooperative organization among data supervisory authorities can be constructed. Through regular meetings and other mechanisms, it could promote in-depth discussions among members on new trends and regulatory policies in the field of cross-border data, facilitate consensus on data processing standards, and provide member parties with an international platform integrating information sharing, enforcement coordination and cooperation.

Given that each authority has independent enforcement powers within its jurisdiction, member parties might consider ceding specific rights to such a cooperative organization, endowing it with limited supranational enforcement capabilities. As a result, the body would have the authority to assess, investigate and even punish specific cross-border data activities, and take the lead in the construction of a complementary dispute-resolution mechanism.

4.3.3 Coordinating Principles for the Extraterritorial Application of Domestic Rules

There is an inherent contradiction between the globality of data flow and the regionality of data legislation, which makes jurisdictional conflicts an inevitable problem. To safeguard the rights and welfare of domestic data subjects and manage data resources, states often extend the extraterritorial reach of their domestic laws. A prime illustration of this is the long-arm jurisdiction of the GDPR.[2] This extraterritorial impact is not limited to the data processing operations of entities based in the EU. It also encompasses the activities of non-EU entities that either provide goods or services to data subjects within the EU or monitor such data subjects.[3] This unilateral assertion of jurisdiction significantly expands administrative enforcement beyond traditional territorial limits, raising legitimacy concerns. First, it may constitute undue interference with the law enforcement sovereignty of other nations, conflicting with the principles of sovereign equality and international comity. Second, this model does not satisfy the practical requirements of the "effects principle". Without judicial assistance and administrative cooperation from the host country, EU supervisory authorities effectively lack the ability to complete investigations and enforcement abroad. If forced implementation occurs, such supervision may become nominal and could provoke trade retaliation or diplomatic disputes. Third, overly broad jurisdictional claims impose high operational and regulatory costs on the EU itself.[4]

Therefore, a system of "jurisdiction by agreement" offers an important solution to this regulatory predicament.[5] To manage conflicts arising from extraterritorial application of national rules, parties could reach consensus on the methods and limits of jurisdiction through international negotiation, taking into account all parties' interests and mutually ceding some powers.

Two specific approaches to coordination are possible. First, the multilateral treaty approach. Countries with significant cross-border data exchanges could jointly sign a "Mutual Recognition and Enforcement of Jurisdiction Agreement". Such an agreement should clearly define the conditions, scope, limits and methods for exercising jurisdiction. It also needs to establish a periodic review mechanism to dynamically adjust the treaty provisions and enforcement standards based on actual cases. Second, the domestic law approach. When drafting domestic data regulations, countries could introduce a mechanism of jurisdictional deference. For example, depending on the nature of a dispute, the circumstances of the parties and the degree of interest and concern, jurisdiction could be ceded to the country with the closest connection, the most convenient jurisdiction or the greatest interest.

5. Conclusion

Through the two different legal frameworks of China and the EU, this study has demonstrated

[1] Arnell P et al. (2021). Police Cooperation and Exchange of Information under the EU–UK Trade and Cooperation Agreement. *New Journal of European Criminal Law*.

[2] GDPR, art 3.

[3] Kuner C. (2021). Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. *SSRN Electronic Journal*.

[4] Jerker D. (2013). *Extraterritoriality in Data Privacy Law*. Ex Tuto.

[5] Berman PS. (2014). From Legal Pluralism to Global Legal Pluralism. *SSRN Electronic Journal*.

the profound and multidimensional conflict between the principles of data sovereignty and digital trade liberalisation. Both regimes set up barriers to cross-border data flows. The pathways to coordination lie not in global unification, but in pragmatic and multi-level interaction. [1] This involves leveraging any existing flexibility in trade law and learning from innovative balancing mechanisms in new regional agreements. By encompassing legitimate regulatory diversity, the inherent tension can be managed, preserving the immense economic and social benefits of a connected, open and reliable global digital ecosystem.

References

Primary Sources

Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II) [2020] ECLI:EU:C:2020:559

Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650

Directive 95/46/E C of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

General Agreement on Trade in Services (adopted 15 April 1994, entered into force 1 January 1995) 1869 UNTS 183

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Date Protection Regulation) [2016] OJ L 119/1

Secondary Sources

AARONSON S. (2015). Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security. *World Trade Review*, *14*, 671.

Appleton B. (2025). Digital Sovereignty vs. Trade Liberalization: India's Algorithm Disclosure Dilemma. Balsillie Case Studies. <https://balsilliecases.ca/case-study/digital-sovereignty-vs-trade-liberalization-indias-algorithm-disclosure-dilemma/>

Arnell P et al. (2021). Police Cooperation and Exchange of Information under the EU–UK Trade and Cooperation Agreement. *New Journal of European Criminal Law*.

Berman PS. (2014). From Legal Pluralism to Global Legal Pluralism. *SSRN Electronic Journal*.

Bradford A. (2023). *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

Cappiello C et al. (2019). Data Ecosystems: Sovereign Data Exchange among Organizations (Dagstuhl Seminar 19391). *Dagstuhl reports*, *9*, 134.

Cohen JE. (2016). The Regulatory State in the Information Age. *Theoretical Inquiries in Law*, *17*.

Couldry N and Mejias UA. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

Dencik L. (2025). "Rescuing" Data Justice? Mobilising the Collective in Responses to Datafication. *Information, Communication & Society*, 1.

Diesselhorst M. (1982). Hugo Grotius and the Freedom of the Seas. *Grotiana*, *3*, 11.

Gao HS. (2021). Data Sovereignty and Trade Agreements: Three Digital Kingdoms. *SSRN Electronic Journal*.

Greenleaf G. (2018). Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018. *SSRN Electronic Journal*.

Irion K and Yakovleva S. (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, *10*, 201.

Irion K, Yakovleva S and Bartl M. (2016). Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements. *SSRN Electronic Journal*.

[1] Neal Kushwaha, Przemyslaw Roguski and Bruce W Watson, 'Up in the Air: Ensuring Government Data Sovereignty in the Cloud' [2020] 2020 12th International Conference on Cyber Conflict.

Jerker D. (2013). *Extraterritoriality in Data Privacy Law*. Ex Tuto.

Kingsbury B, Krisch N and Stewart RB. (2005). The Emergence of Global Administrative Law. *SSRN Electronic Journal.* <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1361&context=lcp>

Kuner C. (2021). Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. *SSRN Electronic Journal*.

Kushwaha N, Roguski P and Watson BW. (2020). Up in the Air: Ensuring Government Data Sovereignty in the Cloud. 2020 12th International Conference on Cyber Conflict.

Lapa V. (2020). The WTO Panel Report in Russia -Traffic in Transit: Cutting the Gordian Knot of the GATT Security Exception? *Questions of International Law, Zoom-in*, *69*, 5. <https://www.qil-qdi.org/wp-content/uploads/2020/05/02_WTO-Security-exceptions_LAPA_FIN.pdf>

Lateef MA. (2025). Digital Sovereignty in Global Trade: Analysing WTO Governance of Data Flows. *Beijing Law Review*, *16*, 875.

Li L. (2025). Data Sovereignty and National Security: Governance Challenges and Pathways in the Digital Age. *Global Review of Humanities, Arts, and Society*, *1*, 49.

Lomotey RK, Kumi S and Deters R. (2022). Data Trusts as a Service: Providing a Platform for Multi-Party Data Sharing. *International Journal of Information Management Data Insights*, *2*, 100075.

Marfia F, Fornara N and Nguyen T-VT. (2017). A Framework for Managing Data Provider and Data Consumer Semantic Obligations for Access Control. *AI Communications*, *30*, 67.

Meltzer JP. (2015). The Internet, Cross-Border Data Flows and International Trade. *Asia & the Pacific Policy Studies*, *2*, 90.

Newman H. (2021). *OF PRIVACY and POWER: The Transatlantic Struggle over Freedom and Security.* Princeton University Press.

Pierucci F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, *4*.

Pohle J and Thiel T. (2020). Digital Sovereignty. *Internet Policy Review*, *9*.

Sullivan C. (2019). EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era. *Computer Law & Security Review*, *35*, 380.

Svantesson DJB. (2017). *Solving the Internet Jurisdiction Puzzle*. Oxford University Press.

Zhang A. (2021). *CHINESE ANTITRUST EXCEPTIONALISM: How the Rise of China Challenges Global Regulation*. Oxford University Press.

Zhu J. (2021). The Personal Information Protection Law: China's Version of the GDPR? *Columbia Journal of Transnational Law Bulletin*.

Zrenner J et al. (2019). Usage Control Architecture Options for Data Sovereignty in Business Ecosystems. *Journal of Enterprise Information Management*, *32*, 477.

Zuo W. (2024). General Exceptions in the Digital Trade Environment: Challenges and Reforms under Article 20 of GATT and Article 14 of GATS. *Journal of Education, Humanities and Social Sciences*, *39*, 77.