 DOI:10.5281/ZENODO.16792040

RECONCILING SOVEREIGNTY AND SEAMLESSNESS: LEGAL CHALLENGES OF CROSS-BORDER DATA FLOWS IN THE INDO-PACIFIC

BY VASUNDHARA RAJE[1] & RISHI KUMAR[2]

ABSTRACT

In the modern fast-digitised world economy, international data flows are important for trade, innovation, and global cooperation. Yet, legally governing these flows raises tremendous tensions between national data sovereignty and wanting a free and open Internet. The Indo-Pacific region, where there is a coexistence of different political regimes and regulatory systems, illustrates this conflict in a striking way. Meanwhile, nations such as India advocate for "data localisation" to take control of key digital infrastructure, and others, like Japan and Singapore, lead the charge for interoperable models such as the "Data Free Flow with Trust" (DFFT). This divergence is one that raises profound questions regarding data governance in the future of a geopolitically strained and technologically rapidly changing region.

This paper assesses the legal framework of cross-border data transfers in the Indo-Pacific, specifically how varying approaches to data protection affect regional integration, digital trade, and human rights. It analyses key legislations, including India's Digital Personal Data Protection Act, 2023;[3] the GDPR's extraterritoriality;[4] and ASEAN's Cross-Border Data Flow Mechanism,[5] alongside recent bilateral and plurilateral agreements like the Indo-Pacific Economic Framework (IPEF). By doctrinal and comparative inquiry, the paper examines whether the available legal tools can be harmonised without intruding on state autonomy or jeopardising privacy safeguards. In addition, the abstract underlines

[1] The author (I) is a law student at Dr. Ram Manohar Lohiya National Law University, Lucknow
[2] The author (II) is a law student at Dr. Ram Manohar Lohiya National Law University, Lucknow
[3] Digital Personal Data Protection Act 2023 (India)
[4] 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 (General Data Protection Regulation) [2016] OJ L119/1
[5] ASEAN, *Framework on Personal Data Protection* (ASEAN, 22 November 2016) https://asean.org/wp-content/uploads/2021/01/ASEAN-Framework-on-PDP.pdf accessed 25 July 2025

the difficulties of surveillance issues, digital colonialism, and the absence of effective multilateral norms on data transfers. It further discusses the possibility of a regionally anchored, principle-driven regime that balances trust, transparency, and technological neutrality. The research ends with policy suggestions for developing interoperable standards that respect data protection while ensuring secure cross-border digital environments within the Indo-Pacific. At a moment of rising digital nationalism and cyber threat, this article contends for a collaborative legal framework based on mutual recognition, responsibility, and respect for human rights—one that makes the Indo-Pacific not just a battleground of digital geopolitics but a laboratory for open and future-proof data governance.

Keywords: Cross-border Data Flows, Data Protection, Digital Sovereignty, Indo-Pacific Legal Frameworks, Interoperable Data Governance.

INTRODUCTION

The Indo-Pacific region of strategic interdependence, economic development, and geopolitical sophistication is experiencing digital change. At the heart of this change is the increasing significance of data as a strategic resource. Cross-border data flows, transferred across borders through digital networks, are essential for e-commerce, financial services, AI systems, logistics, and other key sectors. But as digital interdependence grows, sovereign states increasingly claim jurisdiction over data collection, storage, processing, and transfer across borders. This conflict between sovereignty and seamlessness defines one of the significant legal challenges of the digital era in the Indo-Pacific.[6]

"Data sovereignty" responds to international concerns regarding privacy, cybersecurity, and digital colonialism. India, China, and Indonesia have introduced or suggested requirements for data localisation, compelling data to be processed or stored within domestic borders.[7] These are legitimate responses to surveillance, economic domination, and digital dependence concerns. But they also carry the danger of breaking the open internet, sabotaging the multilateral trade architecture, and killing innovation. On the other hand, smooth data flows

[6] Mira Burri, 'Data Governance in Trade Agreements: The Pitfalls of Legal Adaptation' (2021) 20(2) World Trade Review 282

[7] Digital Personal Data Protection Act 2023 (India); ECLAC, *Digital Trade Regulatory Landscape in Asia-Pacific: Data Flows and Data Localisation Measures* (2021) https://www.unescap.org/kp/2021/digital-trade-regulatory-landscape-asia-pacific-data-flows-and-data-localisation-measures accessed 25 July 2025

encourage efficiency, competitiveness, and globalisation of supply chains, which is particularly important in an area as economically connected as the Indo-Pacific.[8]

Balancing national sovereignty of data with the requirements of Indo-Pacific cross-border integration creates nuanced legal complexities. The regulatory environment within Indo-Pacific states is fragmented, with diverse privacy, cybersecurity, and data governance standards. In addition, the increase in bilateral and multilateral trade agreements—e.g., the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, the Regional Comprehensive Economic Partnership, and the Indo-Pacific Economic Framework for Prosperity- brings overlapping commitments and frictions between national regulatory autonomy and trade liberalisation.[9]

The question of law at the centre of this controversy is whether international law and regional approaches can adapt to hold multiple national interests together while allowing safe and unencumbered data flows. How do legal systems achieve interoperability between jurisdictions without undermining constitutional and strategic discretion? The response demands a balanced analysis of normative data regulation approaches, domestic law-trade agreement relationships, and the burgeoning jurisprudence relating to digital rights and state sovereignty. This paper examines these tensions in law and suggests a harmonised but adaptable regulatory model that upholds state autonomy while promoting trust and predictability within cross-border data regimes.[10]

UNDERSTANDING CROSS-BORDER DATA FLOWS: DRIVERS AND RISKS

Cross-border data flows are the movement of digital data across borders via the internet or digital infrastructure. Data flows are the foundation of today's economic and governance systems and support cloud computing, global value chains, financial transactions, digital communications, and artificial intelligence. The size and magnitude of such flows are huge in the Indo-Pacific, which is home to over 60% of the global GDP and a fast-growing digital

[8] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies* (OECD 2021) https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm accessed 25 July 2025

[9] CPTPP (signed 8 March 2018, entered into force 30 December 2018); RCEP (signed 15 November 2020, entered into force 1 January 2022); IPEF (Framework Agreement, launched 23 May 2022)

[10] Anupam Chander and Uyên P Lê, 'Data Nationalism' (2015) 64 Emory LJ 677

marketplace. Legal issues in their governance arise from their transnational character, challenging the enforceability and applicability of territorial laws in the digital world.[11]

Economic Drivers of Cross-Border Data Flows: Cross-border data flows are the key drivers of innovation and global commerce efficiency. As a necessity for e-commerce, remote services, and international financial transactions, smooth digital transactions are vital for small and multinational enterprises. Cloud-based applications, frequently based in data centres beyond the user's location, rely on encrypted free data flow. According to a McKinsey Global Institute report, cross-border data flows contributed more to GDP growth than global goods trade between 2010 and 2020.[12] Open data flows are critical to economic competitiveness for countries in the Indo-Pacific like Singapore, Japan, and Australia, which have established themselves as regional digital hubs.[13]

In addition, rising economies like India and Vietnam aim to harness data-driven industries like fintech, healthtech, and edtech to drive local growth and connect with the world. Digitisation of trade, logistics, and customs procedures under programmes like the ASEAN Single Window is based on interoperable digital platforms, emphasising the importance of cross-border data flow frameworks.[14]

Strategic and Governance Risks: Uncontrolled data flows present several legal and strategic issues despite these economic necessities. Governments are concerned with data-led surveillance, foreign domination of key infrastructure, and exploiting citizens' data. Cybersecurity threats—from state-sponsored attacks to ransomware targeting critical sectors—have prompted countries to assert greater control over data. The Edward Snowden revelations and the extraterritorial reach of laws like the United States' Foreign Intelligence Surveillance Act (FISA) have deepened suspicions about global data flows being conduits for digital imperialism.[15]

---

[11] Anupam Chander, 'Data Nationalism' (2013) 64(3) Emory Law Journal 677

[12] McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows* (March 2016) https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows accessed 25 July 2025

[13] Jane Kelsey, 'The Risks of New Mega-Agreements in the Asia Pacific Region: TPPA, RCEP and Trade in Services' (2017) 50(1) Journal of World Trade 11

[14] ASEAN, *ASEAN Single Window* https://asw.asean.org accessed 25 July 2025

[15] United States, Foreign Intelligence Surveillance Act of 1978, 50 USC §§ 1801–1885; Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Metropolitan Books 2014)

Additionally, the lack of harmonised privacy standards creates regulatory uncertainty. For example, information safeguarded under the General Data Protection Regulation of the European Union might not enjoy the same level of protection in countries without strong privacy legislation. Such a disparity erodes users' trust as well as cross-border business compliance. While countries like Japan and South Korea have aligned closely with GDPR in the Indo-Pacific, others, such as India and Indonesia, are still enacting comprehensive data protection regimes.

The Risk of Digital Fragmentation: Among the most urgent dangers national data flow control poses is the threat of a splintered internet or "splinternet." Localisation requirements, restrictive licensing, and disparate cybersecurity standards risk balkanising cyberspace. Such protectionism in cyberspace jeopardises international trade, hampers innovation, and raises costs for businesses operating across borders.[16]

Moreover, restrictive data regimes unduly burden smaller Indo-Pacific economies across cross-border platforms and foreign nations' cloud facilities. The inability to make interoperable legal frameworks might exacerbate regional digital divides and compromise inclusive development goals.

Balancing Innovation and Regulation: Hence, the task is to reconcile the economic benefits of frictionless cross-border data flows with legitimate regulatory interests in security, privacy, and sovereignty. Data localisation will deliver some degree of control over data governance, but neither at zero cost nor as a panacea. Legal frameworks must evolve to adopt risk-based, interoperable models that facilitate trust while preserving the open character of the internet.

LEGAL LANDSCAPE OF DATA FLOWS IN THE INDO-PACIFIC

Indo-Pacific countries have a patchwork of legal regimes that regulate cross-border data flows. These regimes vary significantly in scope, enforcement, and philosophies, from free data transfer liberal regimes to national security and data sovereignty-based authoritarian regimes. Grasping this regulatory complexity is necessary for comprehending the complexities of the region's law and avenues for harmonisation.[17]

---

[16] Internet Society, *Splinternet: Addressing the Risk of Internet Fragmentation* (2022) https://www.internetsociety.org/resources/doc/2022/splinternet-report/ accessed 25 July 2025

[17] Graham Greenleaf, 'Global Data Privacy Laws 2023: Despite Instability, 174 Laws Show GDPR Dominance' (2023) 184 Privacy Laws & Business International Report 10

India: Emphasis on Sovereignty and Localisation: India's data flows policy is heavily driven by its data sovereignty vision that holds the contention that data produced by Indian citizens and businesses should be controlled by and subject to Indian laws and regulations. This vision came of age with the draft Personal Data Protection Bill, 2019, subsequently replaced by the Digital Personal Data Protection Act, 2023. While the new Act softens the previously rigid localisation requirements, it still allows the government to restrict cross-border transfers in the interest of national security or public order.[18]

India has also implemented sector-specific localisation mandates. For example, the RBI requires that all payment data be stored exclusively on servers located in India.[19] International technology companies have pushed back against these demands for escalating compliance expenses and hindering operational freedom. The Indian government, however, argues that localisation is more secure, enhances privacy of citizens, and provides law enforcement access.

Japan: A Proponent of Data Free Flow with Trust (DFFT): Japan offers a mirror model, embracing Data Free Flow with Trust (DFFT)—a model that was first proposed by former Prime Minister Shinzo Abe during the 2019 G20 Summit.[20] Japan's Act on the Protection of Personal Information (APPI) is compatible to a high degree with the GDPR, supporting data transfer to jurisdictions with suitable safeguards in place. The main regulatory authority is the Personal Information Protection Commission (PPC), which oversees ensuring accountability and international cooperation.[21]

Japan's regulatory framework is based on interoperability and not uniformity. It fosters interrecognition of privacy standards while enhancing international data transfers. Japan has concluded an adequacy agreement with the EU and actively participates in forums such as the G7 Digital and Tech Ministers' Meetings, reflecting its global digital engagement.

Australia: Privacy-Based Conditional Transfer Regime: Australia governs cross-border flows of data under the Privacy Act 1988, which places limitations on releasing personal information to foreign recipients unless specific conditions are fulfilled. These involve making

---

[18] *Digital Personal Data Protection Act 2023* (India)
[19] Reserve Bank of India, *Storage of Payment System Data*, RBI/2017-18/153 DPSS.CO.OD.No.2785/06.08.005/2017-18 (6 April 2018)
[20] Shinzo Abe, 'Toward Data Free Flow with Trust (DFFT)' (World Economic Forum, 23 January 2019) https://japan.kantei.go.jp/98_abe/statement/201901/_00001.html accessed 25 July 2025
[21] Act on the Protection of Personal Information 2003 (Japan); Personal Information Protection Commission (PPC), *Overview* https://www.ppc.go.jp/en/ accessed 25 July 2025

sure the foreign country possesses equivalent legal safeguards or seeking consent from the individual after making them aware of available privacy threats.[22]

The Australian government has suggested reforms to enhance privacy enforcement and enhance transparency in cross-border transfers. It is also a participating economy in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system, which fosters accountability and recognition among participating economies.[23]

China: Cyber-Sovereignty and National Security: China follows one of the most restrictive regimes of data governance in the Indo-Pacific. Under its Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (PIPL, 2021), it requires stringent localisation of data and security reviews for cross-border transfer.[24]

The Chinese model relies on the concept of cyber-sovereignty, under which it is believed that the state maintains full jurisdiction over digital infrastructure and data in the country. Companies transmitting "important data" or "personal information" out of the country have to undergo security examinations by the Cyberspace Administration of China (CAC). This approach is designed to prevent foreign surveillance and protect state interests, but it has drawn criticism for limiting transparency, commercial freedom, and cross-border digital trade.

Southeast Asia: Fragmented but Evolving Regimes: Southeast Asian states have considerable heterogeneity in data regulation. Singapore's Personal Data Protection Act (PDPA) permits cross-border transfers on the premise that the receiving country offers equivalent protection or contractual arrangements are in place. It also becomes a member of the APEC CBPR system.[25]

On the other hand, Indonesia's Personal Data Protection Law (2022) provides stronger regulation and a new data protection body, though it is early in implementation. Malaysia and Thailand have enacted similar legislation, but differ in enforcement and institutional capacity.

As a regional bloc, ASEAN has come up with the ASEAN Framework on Digital Data Governance, whose principles advocate for harmonisation and trust-based data flows. The

---

[22] *Privacy Act 1988* (Cth) (Australia) s 13B
[23] APEC, *Cross-Border Privacy Rules (CBPR) System* https://www.apec.org/groups/committee-on-trade-and-investment/electronic-commerce-steering-group/cross-border-privacy-rules-system accessed 25 July 2025
[24] *Cybersecurity Law* (2017), *Data Security Law* (2021), and *Personal Information Protection Law* (2021) (People's Republic of China)
[25] Personal Data Protection Act 2012 (Singapore); see also APEC CBPR participation list (n 7)

framework is, however, non-binding and rather acts as a guide rather than an enforceable legislation.

Role of Multilateral and Bilateral Agreements: In addition to domestic laws, Indo-Pacific countries increasingly use trade agreements to shape data governance.

- The Comprehensive and Progressive Agreement for Trans-Pacific Partnership includes provisions prohibiting data localisation and requiring parties to allow cross-border data flows for business purposes.
- Regional Comprehensive Economic Partnership among 15 nations in the Asia-Pacific region offers greater flexibility by enabling members to implement restrictive measures for public policy goals.
- The United States-led Indo-Pacific Economic Framework for Prosperity has a pillar of digital trade supporting interoperable standards and trust in data governance.[26]

These treaties establish a multilayered legal regime in which national sovereignty meets international binding commitments. They provide channels of harmonisation but can also lead to legal conflict where domestic policies clash with treaty provisions.

SOVEREIGNTY VS. SEAMLESSNESS: A REGULATORY DILEMMA

The constitutional challenge of governing cross-border data flows in the Indo-Pacific is one of balancing two frequently competing imperatives: digital sovereignty, which prioritises state control over data within the national realm, and seamlessness, which prioritises the frictionless flow of information between jurisdictions. This section analyses the regulatory dilemma at the heart of this tension and evaluates how states can balance these competing goals within legal frameworks.

Data Localization and the Assertion of Sovereignty: Data localisation policies' return is part of a wider trend of re-establishing sovereignty in digital regulation. Localisation is the legal requirement for data—specifically sensitive personal or critical sectoral data—to be stored or

[26] CPTPP (signed 8 March 2018, entered into force 30 December 2018); RCEP (signed 15 November 2020, entered into force 1 January 2022); White House, *Fact Sheet: Indo-Pacific Economic Framework for Prosperity* (23 May 2022) https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-indo-pacific-economic-framework-for-prosperity/ accessed 25 July 2025

processed inside a given jurisdiction. Governments that implement such policies claim that they do so because such measures are needed to:

1. Ensure national security and surveillance resilience.
2. Enhance law enforcement access to digital evidence.
3. Protect citizen privacy under domestic standards.
4. Stimulate the local data infrastructure and tech ecosystem.

As noted earlier, India explains this rationale. Its data localisation policies have been defended on digital self-reliance and constitutional accountability. In the same vein, China's data localisation and cybersecurity examinations under the Data Security Law indicate apprehensions about foreign access and strategic data vulnerabilities.[27]

Nonetheless, localisation has been decried as a type of digital protectionism. Opponents claim that its practice raises compliance costs for foreign business, deters investment, and undermines cloud-based services that are based on global infrastructure.[28] Moreover, localisation can lead to data silos that can stifle innovation in AI and machine learning, both of which are dependent on big, varied, and cross-border datasets.[29]

Interoperability and Regulatory Alignment: The Case for Seamlessness: On the other side of the spectrum lies interoperability—the ability of different jurisdictions to recognise and respect each other's data protection standards while enabling legal data flows. This approach is embodied in models like the EU's adequacy decisions under the GDPR, APEC's Cross-Border Privacy Rules (CBPR), and Japan's Data Free Flow with Trust (DFFT).[30]

Interoperability aims to enhance seamlessness through consistent rules and reciprocal trust and accountability frameworks. It enables jurisdictions to maintain regulatory independence and agree to common baseline standards. Legal tools that enable such frameworks include

- Contractual Clauses (for instance, Standard Contractual Clauses);
- Binding Corporate Rules (BCRs) for group-to-group transfers;

[27] Ministry of Electronics and Information Technology (MeitY), 'Draft Personal Data Protection Bill 2019' (Government of India, 2019); Data Security Law of the People's Republic of China (2021)
[28] Anupam Chander and Uyen P Le, 'Data Nationalism' (2015) 64 Emory LJ 677
[29] Anirudh Burman, 'The Case Against Data Localization' (Carnegie India, 6 April 2020) https://carnegieindia.org/2020/04/06/case-against-data-localization-pub-81413 accessed 20 July 2025
[30] OECD, 'Data Free Flow with Trust (DFFT)' (2022) https://www.oecd.org/digital/data-free-flow-with-trust.htm accessed 20 July 2025

- Certification regimes and sandboxes regulation;
- Global adequacy or equivalency evaluations.[31]

In the Indo-Pacific region, these frameworks have been supported by Japan and Australia. Singapore's accession to the APEC CBPR and the Global Cross-Border Privacy Rules Forum demonstrates its intent of having smooth but secure flows of data. These models offer an alternative to hard localisation by allowing controlled, lawful, and accountable data transfers.[32]

The Trade-Off: Legal Fragmentation vs. Strategic Autonomy: The central dilemma, therefore, lies in the trade-off between legal harmonisation (which promotes seamlessness) and strategic autonomy (which enables sovereignty). A harmonised approach facilitates regulatory predictability for businesses and enhances regional integration, but may constrain domestic policymaking on sensitive issues such as cybersecurity and intelligence.

Conversely, uncoordinated assertions of sovereignty can fragment the digital ecosystem, causing legal uncertainty, duplication of compliance regimes, and retaliatory regulatory barriers. The result is a paradox: while governments seek to control, the technologies they regulate—cloud computing, blockchain, and AI—are inherently transnational.

This legal dualism is most apparent in trade law. Although agreements such as the CPTPP and USMCA limit data localisation and promote freer flows, they usually feature national security exceptions that allow states to evade such provisions when their critical interests are involved.[33] Consequently, legal certainty is undermined by opaque and erratically enforced exceptions.

Judicial and Constitutional Implications: Domestic courts have begun to confront these tensions. In India, the Supreme Court's landmark ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India recognised informational privacy as a fundamental right under Article 21.[34] This creates a constitutional obligation to protect personal data, but also places limits on arbitrary data transfers or surveillance.

---

[31] European Commission, 'Standard Contractual Clauses (SCCs)' (2021) https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en accessed 20 July 2025

[32] APEC Secretariat, 'Cross-Border Privacy Rules System' (APEC, 2023) https://cbprs.blob.core.windows.net/files/APEC-CBPRs-Overview.pdf accessed 20 July 2025

[33] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) (signed 8 March 2018, entered into force 30 December 2018) art 14.11; United States-Mexico-Canada Agreement (USMCA) (entered into force 1 July 2020) art 19.11

[34] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1

Likewise, in the European Union, the Court of Justice struck down the EU-US Privacy Shield in the decision Schrems II, on the grounds of insufficient protection against foreign spying. This jurisprudence indicates that frictionless data flows can't be at the expense of constitutional protections and due process.

In the Indo-Pacific, many jurisdictions still develop constitutional jurisprudence on digital rights. However, the trend suggests that regulatory reconciliation must be rooted in constitutional values and international cooperation. Balancing these frameworks is a policy issue and a rule-of-law imperative.

COMPARATIVE JURISPRUDENCE AND GLOBAL MODELS

Considering the cross-border data flow challenges under the law in the Indo-Pacific, it is illuminating to consider the broader world and assess how other large jurisdictions contend with the same tensions. The experiences of the European Union, the United States, and China, each with distinct legal traditions, deliver valuable understandings into managing the balance between data sovereignty and digital integration. Their frameworks also have extraterritorial importance, impacting foreign standards and policymaking in the Indo-Pacific province.

The European Union: GDPR and the Principle of Adequacy: The EU's General Data Protection Regulation (GDPR) is the globe's most comprehensive data protection regime, which is reported to have extraterritorial application. It has a robust regime for personal information collection, processing, and transfer, based on data minimisation, limitation of purpose, and user consent.[35]

Notably, Chapter V of the GDPR regulates cross-border data transfers with only an allowance if the destination country ensures equal protection as specified by the European Commission. Japan, South Korea, and the UK are considered adequate, while others, such as the US and India, must use contractual measures such as Standard Contractual Clauses (SCCs).[36]

The CJEU Schrems II ruling invalidating the EU-US Privacy Shield proved the GDPR's strong position on data flows to third countries with weak protection against surveillance. The ruling

[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1

[36] Id. ch. V; see also European Commission, Adequacy Decisions, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited July 24, 2025)

reinforced that fundamental rights like data protection and judicial remedy will not be subjected to negotiations in the EU's legal system.[37]

In the case of Indo-Pacific countries wanting to integrate into the EU, regulatory convergence or recognition is most important. Japan's implementation of GDPR, which led to the signing of the world's first adequacy agreement with mutual recognition, guarantees the benefit of adopting interoperable standards.

The United States: Sectoral and Surveillance-Oriented Model: In contrast to the EU, the United States has a sector-specific and laissez-faire data regulation regime. There are federal laws such as the Health Insurance Portability and Accountability Act and the Children's Online Privacy Protection Act (COPPA) that deal with particular areas, whereas general frameworks are decentralised. There is no federal omnibus data protection law, though states like California have enacted significant legislation such as the California Consumer Privacy Act and California Privacy Rights Act (CPRA).[38]

From a cross-border perspective, U.S. laws emphasise surveillance and national security. The USA PATRIOT Act, the Foreign Intelligence Surveillance Act (FISA), and Executive Order 12333 authorise broad government access to data held by companies, even when stored abroad. These provisions have raised serious concerns in foreign jurisdictions about the vulnerability of data transferred to U.S.-based entities.[39]

To address transatlantic tensions, the U.S. and EU launched the EU-U.S. Data Privacy Framework 2023 to succeed the deceased Privacy Shield. Although this framework brings with it surveillance mechanisms such as the Data Protection Review Court, it is yet to be tested under European court scrutiny. Indo-Pacific nations, especially those in negotiations for digital trade agreements with the U.S., need to balance these risks of surveillance when formulating data flow policies.

China: Comprehensive Control through National Security Laws: China's data governance regime is different because of its emphasis on state control and cyber-sovereignty. Through the

[37] Case C-311/18, *Data Protection Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems* (Schrems II), ECLI:EU:C:2020:559 (July 16, 2020)
[38] See California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100–1798.199 (West 2020); California Privacy Rights Act of 2020, Cal. Proposition 24 (2020)
[39] See Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c (2018); USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); Exec. Order No. 12,333, 3 C.F.R. 200 (1981)

Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (2021), China has established an expansive system that:

1. Classifies data according to sensitivity (for example, "important data," "core data");
2. Needs localisation of specific data types;
3. Mandates security assessments before cross-border transfers;
4. Grants enforcement powers to the Cyberspace Administration of China (CAC).[40]

China's laws reflect a national security-driven approach, tightly regulating foreign access to Chinese data and tech infrastructure. The extraterritorial jurisdiction of the Data Security Law enables China to extend its jurisdiction even to offshore companies handling data about Chinese citizens or interests.

Though strengthening domestic control, this strategy may alienate China from international digital markets. It has led to friction with Western digital companies, several of which have curtailed operations in China due to compliance burdens and censorship risks. The Chinese model has influenced countries like Vietnam and Russia, but is viewed warily by liberal democracies concerned about rights-based governance.

Lessons for the Indo-Pacific: These global models illustrate diverging styles of regulation:

- The EU system prioritises openness and fundamental rights and features robust controls and judicial oversight.
- The US model prioritises commercial freedom and entrepreneurship, with more inconsequential privacy protection and extensive state incursion.
- The Chinese model requires central control and prioritises sovereignty, security, and political obedience.

For Indo-Pacific countries, the answer is to look for a hybrid model which blends openness with national interest, interoperability with no sacrifice of sovereignty, and respect for rights with the possibility of growth. Japan and Singapore have managed the balancing act and used global cooperation without sacrificing local values.

[40] Cybersecurity Law of the People's Republic of China (2017) (China); Data Security Law of the People's Republic of China (2021) (China); Personal Information Protection Law of the People's Republic of China (2021) (China)

In addition, as geopolitics intensifies in the Indo-Pacific, the ability to engage with different models without being dominated by a single digital bloc will define regional strategic and legal independence. Building regional norms aligned with international norms rather than copying en masse from alien systems will be key in creating an even-keel legal framework for cross-border data regulation.

TOWARD A HARMONIZED FRAMEWORK FOR THE INDO-PACIFIC

Given the complex interplay between national sovereignty, economic interdependence, and digital innovation, the Indo-Pacific must develop a legal architecture that balances flexibility with consistency. A harmonised framework for cross-border data flows is essential to reduce legal uncertainty and fragmentation and foster regional trust, cybersecurity cooperation, and digital economic growth. This section proposes a path forward based on shared legal principles, institutional coordination, and multilateral diplomacy.

Guiding Principles for Regional Harmonization: Harmonisation does not need identical laws but demands functional equivalence, an intercommunicated commitment to core values such as privacy protection, data security, transparency, and accountability. Indo-Pacific states could start by choosing baseline principles such as:

1. Lawful and Fair Processing – Data should be collected and used following legal authority and respect for individual rights.
2. Purpose, Limitation, and Minimisation – Data should be used only for specified, legitimate purposes and kept no longer than necessary.
3. Cross-Border Transfer Mechanisms – Transfers should be permitted where equivalent protections or enforceable safeguards exist.
4. Redress and Oversight – Individuals should have access to remedies for misuse, and enforcement should be independent and transparent.[41]

These principles are already incorporated in current instruments such as the OECD Privacy Guidelines, the APEC Privacy Framework, and the ASEAN Digital Data Governance

[41] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD 2013) https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf accessed 25 July 2025

Framework.[42] Their execution through national laws could give a flexible and culturally relevant platform for regional legal convergence.

Institutional Coordination and Regulatory Dialogues: One of the key barriers to harmonisation is the lack of institutional dialogue between data protection authorities (DPAs), trade negotiators, and security agencies. Indo-Pacific countries should establish inter-regional regulatory networks to:

- Exchange best practices on cross-border enforcement.
- Coordinate responses to cyber incidents involving personal or sensitive data;
- Facilitate peer learning on impact assessments and compliance tools;
- Create a shared certification or trustmark system.

Given their global reputations and regulatory maturity, Japan's Personal Information Protection Commission (PPC) and Singapore's Personal Data Protection Commission (PDPC) could lead in convening such platforms.[43] The Global CBPR Forum provides a working model for such collaboration, where economies mutually recognise certification standards without diluting domestic authority.[44]

Digital Trade as a Vehicle for Legal Convergence: Digital trade agreements have increasingly become legal instruments for data governance. Provisions related to data flow obligations, data localisation prohibitions, and source code and algorithms protection now feature prominently in regional trade deals.[45] The CPTPP, DEPA (Digital Economy Partnership Agreement), and IPEF Digital Trade Pillar reflect these trends.

A regional digital compact—modelled on DEPA—could be initiated among willing Indo-Pacific states to:

- Establish a plurilateral cross-border data transfer framework.
- Set up dispute resolution mechanisms for digital trade frictions.

---

[42] ASEAN, *ASEAN Framework on Digital Data Governance* (2018) https://asean.org/book/asean-framework-on-digital-data-governance/ accessed 25 July 2025

[43] Personal Information Protection Commission (Japan), *International Cooperation* https://www.ppc.go.jp/en/personal/aboutus/cooperation/ accessed 25 July 2025

[44] Global CBPR Forum, *Charter and Governance* https://globalcbpr.org accessed 25 July 2025

[45] DEPA, *Digital Economy Partnership Agreement* (2020) https://www.mti.gov.sg/-/media/MTI/Resources/FTA/DEPA/Annexes/DEPA-Chapter-Data-Governance.pdf accessed 25 July 2025

- Create joint norms on algorithmic accountability, cloud sovereignty, and data portability.

Such a compact need not be binding at the outset. A "variable geometry" approach, letting countries to enter specific modules (e.g., privacy, AI ethics, cybersecurity) as per their enthusiasm, would ensure inclusivity and respect for domestic policy constraints.[46]

Addressing the Geopolitical and Security Dimension: Data governance is not just a legal issue but a geostrategic one, especially in the Indo-Pacific, where digital infrastructure, submarine cables, and cloud services are part of great power competition. Regional data harmonisation must account for:

- Supply chain resilience in data infrastructure (e.g., diversification of cloud storage and undersea cable networks);
- Cybersecurity cooperation, including threat intelligence sharing and joint incident response frameworks;
- Avoidance of techno-bloc formation, which could deepen digital fragmentation and undermine multilateralism.[47]

ASEAN-led mechanisms like the ASEAN Digital Ministers' Meetings and ADGMIN Joint Declarations could be expanded to facilitate inclusive security dialogues. The Quad (Australia, India, Japan, and the US) may also act as a platform to pilot secure, rights-respecting data sharing models, especially in serious sectors like health, defence, and financial services.

Engaging Civil Society and Private Sector Stakeholders: Legal harmonisation efforts must engage beyond state actors. Civil society groups, academic institutions, and technology companies have a vital role in:

- Shaping ethical standards for AI and data use;
- Monitoring the implementation and abuse of cross-border flow regulations;
- Developing privacy-enhancing technologies (PETs) and open-source compliance tools.

[46] Mira Burri, 'Modular Approach to Digital Trade Governance' (2022) 56(3) *Journal of World Trade* 425
[47] Kristina Irion, 'Digital Infrastructure and the Geopolitics of Data Sovereignty' (2021) 12 *Digital Policy, Regulation and Governance* 187

As seen in the Global Forum on Cyber Expertise (GFCE) and Internet Governance Forum (IGF), public-private partnerships can help democratise digital policymaking and ensure that regulatory solutions reflect societal interests, not just state security imperatives.[48]

CONCLUSION

The regulation of cross-border data flows in the Indo-Pacific is at a significant legal and political juncture. As the region is growing more digitised and economically interdependent, never before have the stakes in managing how data crosses national borders been higher. On the one hand, states extend greater control over data for reasons of sovereignty, security, and accountability to regulate. On the other hand, untrammelled flows of information are essential to innovation, commerce, and integration. The conflict between these conflicting imperatives—seamlessness and sovereignty—is one of the most complex legal challenges of the internet age.

The Indo-Pacific regulatory environment is characterised by deep heterogeneity. Some states, such as India and China, have shifted towards localisation and strict controls based on strategic and political imperatives. Some, including Japan, Australia, and Singapore, have chosen more interoperable and trustworthy environments that allow responsible data flows and privacy preservation. This fragmentation in regulation makes it challenging to evolve an integrated regional digital economy and exposes businesses, consumers, and governments to legal threats.

Yet, complete convergence is neither politically feasible nor normatively desirable. Instead, the region must pursue a model of legal harmonisation through functional equivalence—developing shared norms and interoperable standards that respect national autonomy while promoting regional trust. Trade agreements, regional compacts, and multilateral dialogues can serve as vehicles to institutionalise such cooperation, provided they include strong privacy safeguards, accountability mechanisms, and flexible participation formats.

A successful regulatory model must also recognise the role of judicial oversight, constitutional protections, and civil society engagement. The emerging jurisprudence in the Indo-Pacific—most notably from the Indian Supreme Court in the Puttaswamy case—underscores the centrality of fundamental rights in any data governance framework. Moreover, public trust in

[48] Global Forum on Cyber Expertise (GFCE), *Strategic Engagement and Programmes* https://thegfce.org accessed 25 July 2025

 DOI:10.5281/ZENODO.16792040

digital systems will depend on robust enforcement, transparency, and remedy mechanisms that transcend political expediency.

Ultimately, reconciling sovereignty with seamlessness in the governance of cross-border data flows is not a zero-sum game. It needs a recalibration of legal frameworks to smash a balance between control and openness, security and innovation, autonomy and cooperation. With its diversity of systems and shared commitment to growth, the Indo-Pacific is uniquely positioned to develop a new paradigm of regional digital governance—one that can serve as a model for a multipolar and interconnected digital world.

***