BRILL | NIJHOFF

JOURNAL OF WORLD INVESTMENT & TRADE 26 (2025) 575–620

The Journal of World Investment & Trade Law • Economics • Politics
brill.com/jwit

Law and Digital Transformation in the Indo-Pacific: An International Economic Law Perspective

Julien Chaisse
School of Law, City University of Hong Kong, Hong Kong SAR
julien.chaisse@cityu.edu.hk

Georgios Dimitropoulos
College of Law, Hamad Bin Khalifa University, Doha, Qatar
gdimitropoulos@hbku.edu.qa

Irma Mosquera
Leiden Law School, Leiden University, Leiden, The Netherlands
i.j.mosquera.valderrama@law.leidenuniv.nl

Accepted 1 May 2025 | Published online 25 June 2025

Abstract

The Indo-Pacific has become a key site for legal responses to the global digital economy. While the region includes several advanced digital markets, major differences in infrastructure and regulatory capacity remain. Governments are introducing domestic, regional, and plurilateral instruments that affect how trade, investment, and data flows are handled. This article argues that these efforts mark a wider turn in international economic law, away from harmonization and toward coordination through interoperability and mutual recognition. Yet law does not always improve outcomes. New rules can encourage cooperation, but they can also exclude or reinforce geopolitical tension. This article examines how governments across the Indo-Pacific are building legal tools that respond to digital expansion while managing external pressure and internal

* The views expressed in this article are those of the authors alone. This introductory piece to the symposium "Law and Digital Transformation in the Indo-Pacific" forms part of a broader collaborative project launched in 2023 with the support of the Economic Research Institute for ASEAN and East Asia (ERIA). The project involved two events: an online workshop held on 18 October 2024 and a conference hosted at Leiden University in November 2024.

Published with license by Koninklijke Brill BV | DOI:10.1163/22119000-12340376
 | ISSN: 1660-7112 (print) 2211-9000 (online)

constraints. These experiments are uneven and incomplete, but they reveal how the region is moving from passive rule-taker to active contributor in setting terms for the global digital economy.

Keywords

regulatory coordination – interoperability – plurilateralism – cross-border data flows – digital trade – Artificial Intelligence – sovereignty – investment law

1 Introduction

The growth of the digital economy in recent years has changed the conditions under which production, trade, and investment take place. Technologies such as artificial intelligence, blockchain, the Internet of Things, and digital platforms have transformed how business is carried out in sectors like manufacturing, finance, healthcare, and retail.[1] These tools have lowered the barriers to cross-border activity. They reduce paperwork, cut transaction costs, and allow information to move almost instantly. Companies that once had no access to international markets are now able to join global supply chains, reach consumers abroad, and operate in multiple countries with fewer intermediaries. The legal and institutional consequences of these developments are becoming more apparent, especially in trade procedures, investment regulation, and taxation.[2]

1 See generally International Bank for Reconstruction and Development (IBRD), *World Development Report 2021: Data for Better Lives* (World Bank Publications 2021); United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future* (United Nations Publications 2024).

2 See generally World Trade Organization (WTO), *World Trade Report: The Future of World Trade: How Digital Technologies are Transforming Global Commerce* (World Trade Organization 2018); Bruno Casella and Lorenzo Formenti, 'FDI in the Digital Economy: A Shift to Asset-Light International Footprints' (2018) 25 Transnational Corporations 101; Matthew Stephenson, 'Digital FDI: Policies, Regulations and Measures to Attract FDI in the Digital Economy' (2020) World Economic Forum White Paper (September 2020) <https://www3.weforum.org/docs/WEF_Digital_FDI_2020.pdf>; Stephanie Honey, 'Trends in Domestic and International Digital Regulations in Asia and the Pacific' in *The Role and Future of Digital Economy Agreements in Developing Asia and the Pacific* (Asian Development Bank 2025) 1 <https://www.adb.org/publications/digital-economy-agreements-asia-pacific> both accessed 29 April 2025.

This special issue builds on the existing scholarship surrounding digital trade rule-making,[3] focusing on the approaches to digital governance in the Indo-Pacific region.[4] The Indo-Pacific provides a unique context for examining the intersection of digitalization and law.[5] Its significant diversity, geopolitical

3 See eg Henry Gao, 'Digital Economy Partnership Agreement Provisions on Data Flow, Cybersecurity, and Privacy: Challenges and Policy Suggestions for Developing Countries' in *The Role and Future of Digital Economy Agreements in Developing Asia and the Pacific* (Asian Development Bank 2025) 37 <https://www.adb.org/publications/digital-economy-agreements-asia-pacific> accessed 29 April 2025; Andrew D Mitchell and Neha Mishra, 'Data at the Docks: Modernizing International Trade Law for the Digital Economy' (2018) 20 Vanderbilt Journal of Entertainment and Technology Law 1073; Dusheng Zhai, 'RCEP Rules on Cross-Border Data Flows: Asian Characteristics and Implications for Developing Countries' (2024) Asia Pacific Law Review 24; Dan Ciuriak and Maria Ptashkina, 'The Digital Transformation and the Transformation of International Trade' (2018) ICTSD and IDB Issue Paper (January 2018) 25–31 <https://zbw.eu/econis-archiv/bitstream/11159/1651/1/the-digital-transformation-and-trade-ciuriak-and-ptashkina.pdf> accessed 29 April 2025; Mira Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation' (2017) 51 UC Davis Law Review 65, 132; Mira Burri, 'Trade Law 4.0: Are We There Yet?' (2023) 26 JIEL 90; Henry Gao, 'The Regulation of Digital Trade in the TPP: Trade Rules for the Digital Age' in Julien Chaisse, Henry Gao and Chang-fa Lo (eds), *Paradigm Shift in International Economic Law Rule-Making: TPP as a New Model for Trade Agreements?* (Springer Singapore 2017); Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21 Vanderbilt Journal of Entertainment and Technology Law 549; Nicolette Butler and Jasem Tarawneh, 'A BIT of Protection for Non-Fungible Tokens: Digital Assets as a Catalyst for Economic Growth' (2024) 25 JWIT 93; Shin-Yi Peng, 'Digital Trade' in Daniel Bethlehem and others (eds), *The Oxford Handbook of International Trade Law* (2nd edn, OUP 2022); Neha Mishra, *International Trade Law and Global Data Governance: Aligning Perspectives and Practices* (Hart Publishing 2024); Georgios Dimitropoulos, 'Digital Plurilateralism in International Economic Law: Towards Unilateral Multilateralism?' (2025) 26 JWIT 116.

4 What sets the Indo-Pacific apart is its diversity, its strategic position in global affairs, and the pace of its economic development. These features create a setting where the connection between digital growth and legal regulation takes on specific forms not seen elsewhere. Unlike North America, Europe, or Africa, the Indo-Pacific offers a different set of experiences. At the same time, it provides insights that can inform both regional cooperation and broader international efforts.

5 This Special Issue conceptualizes the Indo-Pacific as an economic region comprising countries bordering the Indian and Pacific Oceans, including South Asia, Southeast Asia, East Asia, Western Asia and Oceania. The scope of 'Asia' as a region has long been contested, with geographic terms, such as the Asia-Pacific, East Asia, and Indo-Pacific lacking universally accepted definitions. National governments and international organizations, including the United Nations, the Asia-Pacific Economic Cooperation (APEC), and the WTO, have developed their own interpretations to delineate these regions. Instead of focusing on exhaustive definitions or rigidly demarcating the region's boundaries, this analysis centers on the broader area's economic dynamics, technological innovation, and regulatory initiatives. It

importance, and economic weight establish it as an important focus area for enhancing our understanding of the legal and economic implications of digital transformation more broadly.

The Indo-Pacific region is at a crossroads. It serves as a global nexus of digital and economic activity but faces a critical governance gap. This is not limited to fragmented regulations; it reflects deeper systemic issues. Cybersecurity vulnerabilities undermine trust in cross-border digital trade and data flows.[6] Supply chains, increasingly reliant on digital tools, lack cohesive frameworks to ensure resilience and transparency. Fiscal misalignment, particularly around taxing digital services, creates inefficiencies and potentially stifles innovation. Countries with underdeveloped digital infrastructure, limited internet penetration, or regulatory uncertainty often lack the institutional readiness needed to engage in digital trade and/or attract digital investment. This disparity hinders equitable participation in regional supply chains and global commerce.

Existing regional initiatives, including ASEAN's digital frameworks and OECD's tax principles, have advanced certain technical standards. Still, tensions remain between the desire to preserve domestic control and the practical necessity of cross-border regulatory coordination. While ASEAN has made efforts to harmonize practices (such as through the ASEAN Agreement on Electronic Commerce and the more recent model clauses for cross-border data flows)[7] gaps persist, especially at the phase of implementation. Reconciling national sovereignty with regional interdependence continues to pose a significant challenge. Without strategic regulatory alignment, the region risks entrenching systemic inefficiencies, disparities, and divides. This would

---

emphasizes interconnected markets, trade flows, and shared priorities, such as infrastructure development, technological integration, environmental management, and reducing developmental disparities. The region's importance stems from its role in global production networks, digital economies, and resource exchanges, alongside cooperative efforts to address transnational economic challenges through coordinated policies and partnerships. See eg Asian Development Bank, *Asian Economic Integration Report 2022: Advancing Digital Services Trade in Asia and the Pacific* (Asian Development Bank 2022).

6 Recent modelling by the OECD and WTO confirms that data governance choices carry significant economic consequences. Regulatory misalignment across jurisdictions not only raises compliance costs but may also depress trade (and GDP), particularly in digitally connected economies. In contrast, cooperative models that align regulatory trust and openness are shown to deliver widespread economic benefits; see OECD and WTO, *Economic Implications of Data Regulation: Balancing Openness and Trust* (OECD Publishing 2025) <https://doi.org/10.1787/aa285504-en> accessed 17 May 2025.

7 ASEAN, 'Model Contractual Clauses for Cross Border Data Flows' (2021) <https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf> accessed 29 April 2025.

disrupt supply chains, hinder digital innovation, and exacerbate geopolitical tensions. A lack of cohesive action risks undermining the Indo-Pacific's position as a global leader in the digital economy.

The integration of the digital economy within the Indo-Pacific region is particularly significant because of the substantial economic and strategic importance of the region.[8] The Indo-Pacific is home to some of the most dynamic and rapidly growing economies, including China, India, Japan, South Korea, and Southeast Asian nations like Singapore and Malaysia. These countries collectively represent a significant portion of the global population and economic activity, making the Indo-Pacific a critical area for digital economic initiatives.[9] At the same time, countries in the region are at different stages of digital development – some are leading in technological innovation, while others are still in the process of building their digital infrastructure.[10] The digital divide remains a significant challenge in the Indo-Pacific, with disparities in digital access and literacy between urban and rural areas and among different socioeconomic groups.[11] Bridging this requires targeted efforts to expand digital literacy programs, improve access to affordable devices and Internet services, and create inclusive policies that ensure that all segments of society can benefit from digital advancements. Digital integration could further drive economic development by opening new markets, fostering innovation, and enhancing competitiveness in the Indo-Pacific. India and Indonesia, for example, characterized by substantial populations and expanding middle classes, offer significant potential for the growth of digital trade and services. The adoption of digital technologies in these nations has the capacity to improve economic conditions and the delivery of public services, and overall contribute to an elevated standard of living.

The region's position as a trade corridor connecting East and West has made it central to regulatory developments in international economic law. Decisions made by Indo-Pacific governments on data governance, digital taxation,

8 Executive Office of the President, National Security Council, 'Indo-Pacific Strategy of the United States' (The White House, February 2022) <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf> accessed 29 April 2025.

9 More than 50% of the global gross domestic product (GDP) is projected to be produced in Asia by 2050; Asian Development Bank, *Asia 2050: Realizing the Asian Century* (Asian Development Bank 2011) 1 <https://www.adb.org/sites/default/files/publication/28608/asia2050-executive-summary.pdf> accessed 29 April 2025.

10 See Anita Prakash, Lurong Chen, and Rashesh Shrestha, 'Policy and Economic Imperatives for Participation in and Expansion of the Digital Economy in the Indo-Pacific' 26(4) JWIT 621–47 in this Special Issue.

11 ibid.

electronic commerce or investment screening, now carry direct consequences for the evolution of legal norms worldwide. Strengthened digital connectivity in the Indo-Pacific has the potential to enhance economic resilience by further integrating the region into the global economy, expanding the range of economic activities, and reducing reliance on traditional industries. Digital collaboration can also act as a foundation for wider economic cooperation, fostering a sense of shared prosperity and community among the region's diverse economies. Furthermore, in a period marked by evolving geopolitical and geoeconomic tensions, the capacity of Indo-Pacific nations to cooperate regionally and establish a robust regional digital economy may contribute to global stability and economic security. A second term for Donald Trump as President has reintroduced considerable political and legal uncertainty, marked by increased tariffs on Asia – particularly East Asia,[12] and renewed pressure on allies to decouple from China. The Trump administration's unilateralist orientation and explicit use of trade and technology restrictions as tools of foreign policy complicate efforts to build a stable regional digital economy. This raises a fundamental question for the Indo-Pacific: can legal frameworks built on coordination and openness endure in a climate of intensifying global protectionism and strategic decoupling? Existing agreements face the risk of fragmentation as countries seek to hedge against potential shifts in U.S. trade policy or the imposition of technology-related restrictions. The design of regional agreements and institutions will need to anticipate external volatility and include fallback provisions capable of sustaining digital integration, even amid deteriorating diplomatic relations.

This article sets the analytical groundwork for the special issue. It identifies the legal and regulatory fragmentation that currently hampers digital integration across the Indo-Pacific and proposes an approach grounded in coordination without full-scale legal unification. The special issue builds on this foundation through contributions examining the interplay between national legal systems, regional institutions, and emerging digital economy instruments. Together, the articles aim to refine how international economic law can respond to fast-evolving technological and geopolitical circumstances.

The article proceeds in five sections, each building upon the previous. Section 2 outlines the global context within which digital governance is evolving and then examines how selected Indo-Pacific jurisdictions have begun to construct legal and institutional responses to digital economic

12 See Office of the United States Trade Representative, '2025 National Trade Estimate Report on Foreign Trade Barriers' (31 March 2025) <https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf> accessed 27 March 2025.

activity. This comparative foundation establishes the conditions against which regional coordination must be understood. Section 3 turns to core regulatory domains – data protection, cybersecurity, intellectual property, and digital taxation – where legal responses remain fragmented despite clear economic interdependence. These areas serve as pressure points that test the capacity of existing rules to handle digital trade and investment. Section 4 addresses the legal and institutional consequences of this fragmentation. It identifies forms of cooperation emerging across agreements and institutions that aim to facilitate digital integration without requiring formal legal unification. Section 5 concludes and introduces the broader special issue, which extends the analysis through thematically aligned contributions focused on the emerging elements of digital governance across the region.

2 Fragmentation as a Starting Point, Not a Failure

Digital integration in the Indo-Pacific cannot be understood in isolation. It must be situated within broader global developments that are altering how trade, investment, and data flows are regulated. Across advanced and emerging economies alike, governments are experimenting with legal tools to manage digital activity beyond borders. These trends have begun to influence regulatory design across the Indo-Pacific, where countries face sharply different starting points. Some have moved quickly to establish national policies and legal regimes that support innovation, secure infrastructure, and encourage international cooperation. Others remain constrained by gaps in infrastructure and connectivity, institutional capacity, as well as regulatory updating. This section first considers global and regional trends before turning to selected jurisdictions that have taken the lead in building legal and institutional models with wider impact.

2.1 *Global Templates, Regional Divergence*

The digital economy is undergoing profound transformation owing to the rapid advancement of technologies, such as AI, blockchain, and 5G.[13] These innovations not only enhance efficiency and productivity across various sectors, but also create new paradigms for commerce, communication, and data management. AI is transforming industries by enabling advanced data analytics, enhancing decision-making, and automating sectors like manufacturing,

13 See generally Don Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence* (McGraw-Hill 1997).

healthcare, and finance. It fosters personalized services, streamlined operations, and cost savings, driving economic growth and innovation. Meanwhile, blockchain technology provides a secure, decentralized way to record transactions and manage data, with applications in supply chains, digital identity, and smart contracts. Its transparency and security help combat fraud, ensure data integrity, and build trust in digital transactions, creating more efficient systems that propel the global digital economy. The arrival of 5G technology marks a major advancement in telecommunications, offering high speeds, low latency, and the ability to connect numerous devices at once, thus driving the growth of IoT. 5G significantly boosts the digital economy by facilitating real-time data exchange, supporting AI and blockchain deployment, and enhancing digital connectivity.

These trends also have significant legal implications and necessitate new regulatory developments. The rise of AI requires new laws to address ethical issues, data privacy, and accountability. Similarly, blockchain technology needs regulations to regulate financial transactions and smart contracts built on its infrastructure. Its decentralized nature challenges existing regulatory methods, calling for innovative solutions to ensure security and compliance. The rollout of 5G technology raises legal issues about spectrum allocation, data privacy, and cybersecurity.[14] Regulators need to create policies for fair spectrum access, data protection, and network security. Existing telecom laws must be updated to address increased data traffic and new services. Moreover, financial regulations should adapt to oversee fintech and protect consumers in digital payments.

E-commerce stands out as a clear example of how digital technologies are opening up new possibilities while introducing serious complications, especially across the Indo-Pacific. The sector has been expanding quickly in this part of the world, shaking up how people shop and how businesses operate. Countries like China, India, and Indonesia are seeing explosive growth in online retail, with millions of consumers turning to the internet for everyday purchases. Companies such as Alibaba, Flipkart, and Tokopedia are racing to keep up, pushing into new markets and offering everything from groceries to digital services.[15] This surge is fuelling broader economic momentum and sparking new developments in areas like online advertising, supply chain management, and financial technology.

14 See eg Xu Qian, 'Redefining International Law Paradigms: Charting Cybersecurity, Trade, and Investment Trajectories Within Global Legal Boundaries' (2024) 25 JWIT 295.

15 See generally Jong Woo Kang and Grendell Vie Magoncia, *E-commerce Evolution in Asia and the Pacific: Opportunities and Challenges* (Asian Development Bank 2023).

Moreover, driven by the proliferation of mobile payment solutions and fintech innovation, the Indo-Pacific has seen a sharp rise in digital payments.[16] Countries, such as China and India, are leading with platforms, such as Alipay, WeChat Pay, and Paytm, which offer convenient, secure, and efficient payment methods for consumers and businesses.[17] The adoption of digital payments has accelerated financial inclusion, particularly in rural and underserved areas, by providing access to financial services that were previously out of reach.

However, these trends also posit challenges that need to be addressed to fully realize their potential. The rapid growth of digital services requires robust infrastructure, including reliable internet connectivity, secure data centres, and efficient logistics networks. Governments and private-sector players must invest in building and upgrading this infrastructure to support the continued expansion of the digital economy for all. In addition, there is a need for comprehensive regulatory frameworks that address issues, such as data privacy, cybersecurity, and consumer protection.[18] According to the World Bank, it is more likely for a country to have in place an e-commerce law over a data protection law.[19] Ensuring that these regulations are synchronized across the region, can facilitate cross-border digital trade and investment, creating a more resilient and inclusive digital economy.

2.2 *Competing Centres of Legal Innovation*

Countries across the broader Indo-Pacific region have been establishing legal standards and practices that are shaping global trade norms. China is obviously a special case; not only because of its dominant position in the digital economy but also because of its unique regulatory approach, which aims to balance innovation with tight control measures. Data localization and cybersecurity measures emphasize the goal of promoting economic interests alongside protecting national security.[20] As China continues to expand its Digital Silk Road

16 Martin Chorzempa, 'Cross-Border Payments' in *The Role and Future of Digital Economy Agreements in Developing Asia and the Pacific* (Asian Development Bank 2025) 95 <https://www.adb.org/publications/digital-economy-agreements-asia-pacific> accessed 29 April 2025.

17 Ignacio Carballo, 'Understanding Asia-Pacific: Where the Future of Fintech is Shaped' (*PCMI*, 23 August 2023) <https://paymentscmi.com/insights/asia-pacific-fintech-industry/> accessed 29 April 2025.

18 See Section 3 below.

19 IBRD (n 1).

20 See generally Dan Svantesson, 'Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines' (2020) OECD Digital Economy Papers 301, 8 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/12/data-localisation-trends-and-challenges_d775fe8a/7fbaed62-en.pdf> accessed 29 April 2025.

as part of the Belt and Road Initiative, international trade and investment laws are evolving to accommodate the growing influence of digital infrastructure and technology standards from China across the Indo-Pacific and beyond.[21]

Japan and South Korea's leadership in AI, robotics, and the IoT, underscores the potential of establishing regional legal standards for emerging technologies.[22] The development of regional digital standards must also be understood in the context of China's assertive and wide-reaching strategy in digital technologies. Firms like Huawei, Alibaba, and DJI are exporting not just products but protocols, often bundled with infrastructure through state-backed initiatives like the Digital Silk Road.[23] These exports carry regulatory implications, particularly as more Indo-Pacific states adopt Chinese-built platforms that come with embedded technical norms and data governance

21 See generally Matthew S Erie and Thomas Streinz, 'The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance' (2021) 54 NYU Intl L & Pol 1.

22 See Yoshija Walter, 'Managing the Race to the Moon: Global Policy and Governance in Artificial Intelligence Regulation – A Contemporary Overview and an Analysis of Socioeconomic Consequences' (2024) 4 Discover Artificial Intelligence <https://link.springer.com/content/pdf/10.1007/s44163-024-00109-4.pdf> accessed 29 April 2025. Walter examines Japan's regulatory approach to artificial intelligence, which promotes innovation while imposing responsibility through its Social Principles of Human-Centric AI. This framework centres on human dignity, inclusion, and sustainability. Rather than imposing rigid controls, it favours flexible, sector-specific guidance, supported by statutory instruments such as the 2003 Act on the Protection of Personal Information; see Act on the Protection of Personal Information (APPI), Act No 57 of 2003 (JPN). South Korea has not previously implemented specific laws or statutory regulations targeting AI; however, this is set to change with the recent passage of a proposed Act on Promotion of the AI Industry and Framework for Establishing Trustworthy AI by the National Assembly (Science, Technology, Information, Broadcasting and Communications Committee, 'Gugjoe Gwabang-wi Beob-an2sowi, "Metabeoseubeob" Mich "Ingongineungbeob" Deung Uigyeol [National Assembly Defense Subcommittee 2 passes the "Metaverse Act" and "Artificial Intelligence Act"' (14 February 2023) <https://www.assembly.go.kr/portal/bbs/B0000051/view.do?nttId=2095056&menuNo=600101&sdate=&edate=&pageUnit=10&pageIndex=1https://www.assembly.go.kr/portal/bbs/B0000051/view.do?nttId=2095056&menuNo=600101&sdate=&edate=&pageUnit=10&pageIndex=1> accessed 29 April 2025). Once enacted, the law will consolidate seven AI-related bills introduced since 2022. It aims to support the development of the AI sector while introducing safeguards for users through mandatory notification procedures and certification requirements; see also Hyun Park Do, Eunjung Cho and Yong Lim, 'A Tough Balancing Act – The Evolving AI Governance in Korea' (2024) 18 East Asian Science, Technology and Society: An International Journal 135.

23 Angela Huyue Zhang, *Chinese Antitrust Exceptionalism: How the Rise of China Challenges Global Regulation* (OUP 2021) 144–47.

models.[24] South Korea's emphasis on developing a high-speed internet network, fostering digital literacy, and supporting tech startups has resulted in a vibrant digital ecosystem. This environment has attracted substantial foreign direct investments and has enabled South Korean companies to become global leaders in technology and innovation. South Korea's digital policies and innovation ecosystems serve as models for other countries to enhance their digital economies.

Singapore has identified the digital economy as a niche for growth.[25] Singapore's strategic investments in digital infrastructure and regulatory frameworks have cemented its status as a key player in global digital trade.[26] Smart Nation Singapore initiative plays a central role in its industrial strategy, integrating digital technologies across sectors.[27] In Singapore, digital economy initiatives have led to the development of robust e-commerce ecosystems supported by advanced logistics and payment systems. This has boosted domestic economic activity and positioned the country as a regional and international hub for digital trade. This includes fostering digital economy industries, developing digital infrastructure, and promoting the adoption of AI, IoT, and cybersecurity to drive economic growth and increase global competitiveness.

24 A very salient example comes from Western Asia. Baidu's Apollo Go self-driving taxi service will launch in Dubai and Abu Dhabi, starting with trials in 2025 and aiming for commercial driverless operations by 2026. In Dubai, a partnership with the Roads & Transport Authority targets 100 taxis initially, scaling to 1,000 by 2028, while in Abu Dhabi, a collaboration with Autogo plans the capital's largest autonomous fleet. This follows WeRide's earlier entry via Uber in Abu Dhabi and aligns with Dubai's goal of 25% autonomous journeys by 2030; See Graham Hope, 'Chinese Self-Driving Taxis to Launch in Dubai, Abu Dhabi' (*IoT World Today*, 19 February 2024) <https://www.iotworldtoday.com/transportation-logistics/chinese-self-driving-taxis-to-launch-in-dubai-abu-dhabi> accessed 27 March 2025. This showcases Chinese tech's growing Middle East presence, as well highlights China's expanding influence in setting standards for emerging digital infrastructure abroad. The deployment of Chinese driverless car technology in Western Asia occurs alongside the concurrent expansion of Waymo's autonomous vehicle operations in various cities in the US; see Waymo, 'Waymo One' (Waymo, 2025) <https://waymo.com/waymo-one/> accessed 6 April 2025. Waymo is a subsidiary of Alphabet Inc., the parent company of Google.

25 Neil Lee, Metta Ni and Augustin Boey, 'The Scale-up State: Singapore's Industrial Policy for the Digital Economy' (2024) Southeast Asia Working Paper Series Paper 11 <http://eprints.lse.ac.uk/123885/1/Southeast_Asia_Working_Paper_11.pdf> accessed 29 April 2025.

26 See 'Singapore Country Commerce Guide – eCommerce' (International Trade Administration, 5 January 2024) <https://www.trade.gov/country-commercial-guides/singapore-ecommerce> accessed 29 April 2025.

27 Smart Nation Singapore, 'Growth' <https://www.smartnation.gov.sg/goals-of-sn2/growth/> accessed 29 April 2025.

Singapore's approach to digital technologies is actually supported by an open trade policy, which is underpinned by numerous Preferential Trade Agreements (PTAs) and Digital Economy Agreements (DEAs), which aim at ensuring that Singapore remains a key player in global supply chains.[28]

Australia's proactive digital economy policies reflect a commitment to fostering a conducive environment for digital trade and investment. The country's strategic initiatives, such as the Digital Economy Strategy 2030 and the Digital Business Plan, underscore the importance of aligning domestic legal frameworks with international standards to promote digital trade.[29] Australia's Digital Economy Strategy 2030 aims to position the country as a leader in the global digital economy by fostering innovation, enhancing digital capabilities, and enabling seamless digital transactions.[30] A primary focus is placed on digital infrastructure, particularly the development of 5G networks, cloud computing, and secure data environments, which are regarded as essential to Australia's broader digital transformation.[31] This infrastructure is intended

28 The Trade Agreement Provisions on Electronic-commerce and Data (TAPED) dataset provides a comprehensive mapping of digital trade provisions in PTAs since 2000, encompassing over 465 agreements. It includes 130 coded items addressing digital trade, IP, services, government procurement, trade in goods, exceptions, and emerging issues. Mira Burri, Maria Vásquez Callo-Müller and Kholofelo Kugler, 'TAPED: Trade Agreement Provisions on Electronic Commerce and Data' (University of Lucerne, 20 November 2024) <https://unilu.ch/taped> accessed 29 April 2025. See also Section 3.4 below.

29 Australia's Digital Economy Strategy 2030 and Digital Business Plan reflect a concerted effort to build a reliable environment for digital trade. These initiatives support data security, skills development, and infrastructure investment, while aligning domestic rules with international benchmarks. Their design facilitates cross-border data flows and promotes compatibility with global digital systems, reinforcing Australia's role in wider digital integration efforts. See Yoonee Jeong, 'Enhancing Policy and Regulatory Approaches to Strengthen Digital, Platform, and Data Economies' (2023) ADB Sustainable Development Working Paper Series 91 <https://www.adb.org/sites/default/files/publication/935711/sdwp-091-digital-platform-data-economies.pdf> accessed 29 April 2025, which discusses regional strategies aimed at supporting economic growth through digital transformation.

30 The Digital Economy Strategy 2030 outlines Australia's roadmap to becoming a global digital leader, projecting an economic boost of USD 315 billion through digital transformation and up to 250,000 new jobs by 2025. It emphasizes strategic investment in digital skills, infrastructure, and regulatory alignment to maintain competitiveness. See Department of the Prime Minister and Cabinet, Commonwealth of Australia, 'Digital Economy Strategy 2030' (Commonwealth of Australia 2021).

31 A report on Australia's digital identity strategy outlines the creation of a secure, interoperable system intended to serve both public and private sectors. It underscores the importance of consistent legal standards to support trust, functionality, and cross-sector application in digital identity governance. See Rajiv Shah, 'The Future of Digital Identity in Australia' (2022) ASPI International Cyber Policy Centre Policy Brief Report 66/2022

to support both large corporations and small and medium-sized enterprises (SMEs), facilitating their integration into the global digital economy.

Innovation constitutes another significant component of the strategy, with an emphasis on supporting emerging technologies, such as AI, blockchain, and quantum computing. The government promotes collaboration between public and private sectors to create an environment conducive to digital start-ups, offering financial and regulatory support through initiatives, such as the Digital Business Plan. This plan, launched alongside the broader strategy, seeks to lower regulatory obstacles and increase investment in digital transformation, particularly for businesses transitioning to digital operations following the pandemic. The strategy also prioritizes the development of trust through robust cybersecurity norms and policies. It aligns national regulations with international standards on data privacy, digital rights, and cybersecurity.

Emerging markets, such as India, Indonesia, Malaysia, and Vietnam present vast – often untapped – opportunities for digital economy expansion – but also highlight the challenges of harmonizing legal frameworks across diverse regulatory environments. India's approach to developing digital technologies and fostering its digital economy is often presented in contrast to that of China. India's digital economy is rapidly expanding, driven by initiatives, such as Digital India, which aims to transform the country into a digitally empowered society.[32] India's focus on digital infrastructure development has been instrumental to its economic transformation. Further investments in India's digital infrastructure, such as expanding broadband access and promoting digital literacy, are crucial for sustaining this growth trajectory. The Digital India initiative emphasizes the need for legal frameworks that support digital payments, data protection, and cybersecurity. Overall, India's approach to the digital economy emphasizes a service-led, consumer internet ecosystem, leveraging its vast digital population; initiatives like Digital India aim at driving both financial inclusion and entrepreneurship, fostering a relatively more market-driven model compared to China. While China seeks to secure technological dominance and economic resilience through strategic investments, India aims to empower its citizens with accessible digital tools.

Indonesia's rapid digital transformation, spearheaded by initiatives, such as 'Making Indonesia 4.0', illustrates the increasing need for legal structures

<https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2022-11/The%20future%20of%20digital%20identity%20in%20Australia.pdf> accessed 29 April 2025.

32 Ministry of Electronics and Information Technology, Government of India, 'Digital India' <https://www.meity.gov.in/sites/upload_files/dit/files/Digital%20India.pdf> accessed 29 April 2025.

that facilitate digital trade and investment. Making Indonesia 4.0, developed in 2018, is a roadmap towards 2030 that aims to help make the country a leader in the digital economy.[33] The roadmap is further supported by initiatives, such as the 'Movement Toward 100 Smart Cities' – initiated the year before.[34] The National Strategy for AI (2020-2045) (Stranas KA) was published in August 2020 by the Agency for the Assessment and Application of Technology (BPPT).[35] The strategy provides a national roadmap for developing AI between 2020 and 2045. Stranas KA's four key focus areas of action emphasize Ethics and Policies; Infrastructure and Data; Talent Development; and Industrial Research and Innovation.[36] Finally, the 2045 Digital Indonesia Vision was launched in 2023 by the Ministry of Communication and Information Technology.[37] Compared to similar frameworks in other countries, cybersecurity is at the core of the vision.[38]

Malaysia has developed an overarching digital strategy too. MyDIGITAL is a national digital development strategy drafted to complement national development policies,[39] such as the latest industrial plan, the New Industrial Master Plan 2030.[40] Based on MyDIGITAL, the Malaysia Digital Economy Blueprint

33 'Indonesia Country Commerce Guide – Digital Economy' (International Trade Administration, 19 September 2024) <https://www.trade.gov/country-commercial-guides/indonesia-digital-economy> accessed 29 April 2025.

34 James Fox, 'Smart Cities Cooperation: Indonesia and Finland' (ASEAN Briefing, 29 June 2022) <https://www.aseanbriefing.com/news/smart-cities-cooperation-indonesia-and-finland/> accessed 29 April 2025.

35 'Artificial Intelligence Innovation Summit 2025' <https://ai-innovation.id>; see also OECD.AI, 'National AI Strategy – Strategi Nasional Kecerdasan Artifisial' (OECD.AI, 6 September 2022) <https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-26968> both accessed 29 April 2025. The BPPT falls now under Indonesia's National Research and Innovation Agency.

36 New Zealand Embassy in Jakarta, 'Indonesia's National Strategy for Artificial Intelligence – July 2023' (New Zealand Foreign Affairs & Trade, July 2023) <https://www.mfat.govt.nz/en/trade/mfat-market-reports/indonesias-national-strategy-for-artificial-intelligence-july-2023> accessed 29 April 2025.

37 Ministry of Communication and Informatics Republic of Indonesia, 'Digital Indonesia Vision 2045' <https://digital2045.id/> accessed 29 April 2025.

38 Azizah Saffa, 'Indonesia's Digital Vision 2045: Cybersecurity at the Core' (OpenGov Asia, 31 May 2024) <https://opengovasia.com/2024/05/31/indonesias-digital-vision-2045-cybersecurity-at-the-core/> accessed 29 April 2025.

39 Strategic Change Management Office, Economic Planning Unit of the Prime Minister's Department, 'MyDigital and 4iR' <https://www.malaysia.gov.my/portal/content/31187> accessed 29 April 2025.

40 Ministry of Investment, Trade and Industry of Malaysia, 'New Industrial Master Plan 2030' (31 January 2025) <https://www.nimp2030.gov.my/> accessed 29 April 2025.

has been developed.[41] On top of that, there is also a National Fourth Industrial Revolution Policy (2023).[42]

Vietnam's prioritization of digital transformation as a key driver of economic growth under its Vietnam Digital Transformation Agenda necessitates the development of legal frameworks that support e-government, smart cities, and digital industries.[43] As Vietnam's digital economy continues to expand, legal frameworks must evolve to address the complexities of digital trade and investment.

The countries of the Indo-Pacific have moved beyond the role of simple technology adopters, particularly in areas, such as AI, the IoT, and cybersecurity. In the broader Indo-Pacific region, economically advanced as well as emerging economy countries have also demonstrated their potential as global digital standard-makers. Using domestic paradigms, they are actively promoting regional and global legal frameworks aimed at combining digital trade and cross-border data flows (CBDFs) with data protection and national security;[44] making thus a significant impact on the rules and practices of the global digital economy.

3 Regulatory Pressure Points and Asymmetric Legal Responses

Across the Indo-Pacific, digital trade and investment increasingly intersect with domestic regulatory policy. From data privacy to IP enforcement and taxation, the legal instruments governing digital activity remain highly diverse. This section examines the regulatory consequences of this divergence. Some Indo-Pacific countries have adopted robust data protection, cybersecurity, and intellectual property rules, while often aligning their laws with global reference legal frameworks – such as the GDPR and WIPO treaties – though these remain contested outside the European sphere.[45]

41 Economic Planning Unit, Prime Minister's Department, 'Malaysia Digital Economy Blueprint' (February 2021) <https://www.ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf> accessed 29 April 2025.

42 Economic Planning Unit, Prime Minister's Department, 'National Fourth Industrial Revolution (4IR) Policy' (July 2021) <https://www.ekonomi.gov.my/sites/default/files/2021-07/National-4IR-Policy.pdf> accessed 29 April 2025.

43 'Vietnam Digital Transformation Agenda' (OpenDevelopment Vietnam, 9 December 2023) <https://vietnam.opendevelopmentmekong.net/topics/vietnam-digital-transformation-agenda/> accessed 29 April 2025.

44 See eg Zhai (n 3).

45 See generally Graham Greenleaf, 'Global Data Privacy Laws 2023: 162 National Laws and 20 Bills' (2023) 178 Privacy Laws & Business International Report 1.

However, significant disparities in digital governance remain across the region. Emerging markets, including Indonesia and Malaysia, but also Cambodia, Laos, and Vietnam, are still in the process of developing robust legislation. This divergence underscores the need for greater regional cooperation, as gaps in governance can impede CBDFs and cybersecurity resilience – both of which are crucial to the digital economy. Regional initiatives, such as the 2015 APEC Cross-Border Privacy Rules (CBPR) (hereinafter APEC CBPR)[46] and ASEAN's collaborative frameworks provide avenues for creating a cohesive legal infrastructure. Such efforts are essential in enabling the Indo-Pacific to fully realize its potential as a leader in the global digital economy and to enhance digital connectivity.[47]

This section examines the regulatory consequences of digitalization in the Indo-Pacific, focusing on areas where legal uncertainty or fragmentation creates barriers to trade and investment. Countries across the region have adopted divergent approaches to data protection and privacy, often reflecting different institutional priorities, economic models, and international affiliations. Cybersecurity remains a pressing concern, with governments pursuing regulatory measures that range from voluntary guidelines to binding statutory regimes. Legal protections for digital intellectual property have evolved unevenly, exposing enforcement gaps and raising questions about cross-border recognition. Taxation of digital business activity presents another point of divergence, as states experiment with digital services taxes, nexus rules, and unilateral reporting obligations in the absence of global consensus. These sectoral differences underscore the broader difficulty of achieving regulatory coordination, though a number of initiatives (including regional agreements and plurilateral frameworks) offer early signs of potential convergence in key areas.

3.1 *Privacy and Data Transfers Without Common Rules*

Disparities in data protection and privacy laws are major concerns in the Indo-Pacific region. Most Indo-Pacific countries now have data privacy laws in

46 'APEC Privacy Framework' (August 2017) <https://www.apec.org/apecapi/publication/getfile?publicationId=42d9fa81-f683-46a8-858b-1cde61fdb8f8> accessed 29 April 2025.

47 However, these instruments are not widely adopted by countries. According to Greenleaf, the APEC CBPR framework has not been extensively used even though it was presented as an alternative to EU standards of data protection by non-EU countries, such as the United States, Australia, Canada, and Mexico; see Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (2012) 2 International Data Privacy Law 68, 75.

place or are in the process of developing them.[48] Countries, such as Japan and South Korea, have implemented comprehensive data protection frameworks modelled after the EU's GDPR. For example, Japan's Act on the Protection of Personal Information (APPI), revised in 2021,[49] and South Korea's Personal Information Protection Act (PIPA), amended most recently in 2023,[50] both reflect GDPR-style data governance, particularly in terms of consent requirements and cross-border transfer conditions. In contrast, India's recently enacted Digital Personal Data Protection Act (DPDPA) adopts only select elements of the GDPR model, reflecting a more distinct policy path. The DPDPA applies solely to digital data and introduces a negative list approach for international transfers, avoiding wholesale adoption of the adequacy-based system used in Europe.[51] Other countries have less stringent or outdated regulations or are still in the process of developing their normative framework. After years in the making, the Personal Data Protection (PDP) Law – Law No. 27 of 2022 of Indonesia was eventually adopted in 2022.

In a 2021 study commissioned by the Economic Research Institute for ASEAN and East Asia (ERIA) and conducted by one of the authors of this article, the challenges of digital connectivity related to taxation in Asia and the Pacific were addressed. When collecting tax information by means of traditional and digital sources (such as with the use of AI and blockchain technology), tax administrations need to ensure the protection and safeguard of data privacy and taxpayer's rights (for example, confidentiality, and object in case of decisions taken based only on algorithm/automated processing of data). In order to safeguard these rights, the study recommended the update of data protection laws,[52] based on the EU's GDPR, as well as for countries

48 See under the 'Asia-Pacific' tab in the UNCTAD's database: UNCTAD, 'Data Protection and Privacy Legislation Worldwide' (14 December 2021) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 29 April 2025. This widespread adoption reflects a growing recognition of the importance of data protection in the region.

49 Act on the Protection of Personal Information (APPI), Act No 37 of 2021 <https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en#:~:text=Article%201The%20purpose%20of,the%20proper%20and%20effective%20application> accessed 17 May 2025.

50 Personal Information Protection Act (PIPA), Act No 19234 of 2023 (ROK).

51 Latham & Watkins LLP, 'India's Digital Personal Data Protection Act 2023 vs the GDPR: A Comparison' (August 2023) <https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf> accessed 29 April 2025.

52 Research carried out by Greenleaf shows that the 1995 Data Protection Directive has been used extensively by countries outside Europe, including by countries in Asia and the Pacific. Some examples are Macau, the Republic of Korea, Taiwan, Malaysia, Hong

to become signatories of international conventions, such as the EU-Council of Europe Convention on the Automatic Processing of Personal Data, including big data which is open to third countries (non-EU Council of Europe members).[53] The same study also recommended that Asian countries

> be aware of the challenges that tax administrations face in the collection of tax information (traditional and digital sources) and invest in their data management strategies. These strategies should be (i) long-term strategies and (ii) take into account the use of diagnostic, predictive, and prescriptive analytics. Furthermore, countries should also invest in improving their digital infrastructure, which includes the introduction of common transmission systems and software for the analysis of big data.[54]

One of the most challenging issues today is reconciling data sovereignty with CBDFs.[55] Varying national laws on privacy protection and data localization create significant obstacles to international data transfers. Some countries in the Indo-Pacific adopt more liberal approaches, while others align more closely with GDPR-style regulations. Taiwan[56] and India,[57] for example, allow data to cross their borders by default. Australia applies a reasonableness test to entities disclosing personal information overseas.[58] Similarly, under the

---

Kong, Australia, New Zealand, India, Japan, and Vietnam. See Greenleaf, 'Global Data Privacy Laws 2023' (n 45) 75. See also Graham Greenleaf, 'A World Data Privacy Treaty? "Globalisation" and "Modernisation" of Council of Europe Convention 108' in Normann Witzleb and others (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (CUP 2014).

53 Irma Mosquera Valderrama, 'An ASEM Model of Cooperation in Digital Economy Taxation: Digitalisation and New Technologies' in Anita Prakash (ed), *13th Asia-Europe Meeting* (*ASEM*) *Summit: Multilateral Cooperation for a Resilient, Sustainable and Rules-Based Future for ASEM* 86, 105–07.

54 ibid 107.

55 Han-Wei Liu, 'Data Localization and Digital Trade Barriers: ASEAN in Megaregionalism' in Pasha L Hsieh and Bryan Mercurio (eds), *ASEAN Law in the New Regional Economic Order: Global Trends and Shifting Paradigms* (CUP 2019); Jingting Liu, Ulrike Sengstschmid and Yixuan Ge, 'Facilitating Data Flows Across ASEAN: Challenges and Policy Directions' (First Version: 21 August 2023; Current Version: 30 August 2023) Lee Kuan Yew School of Public Policy, Asia Competitiveness Institute, Research Paper #19-2023 <https://lkyspp.nus.edu.sg/docs/default-source/aci/acirp202319.pdf> accessed 6 April 2025.

56 Personal Data Protection Act 2023 (TWN), art 21.

57 Digital Personal Data Protection Act 2023 (IND), ss 16–17.

58 See *Privacy Act 1988* (Cth), later amended by *Privacy and Other Legislation Amendment Act 2024* (Cth), *Privacy Amendment* (*Enhancing Privacy Protection*) *Act 2012, sch 1, pt 3, principle 8.1*(*a*) (Cth).

latest version of Korea's PIPA, the reasonableness test is also employed.[59] Meanwhile, Japan and other jurisdictions in the region maintain stricter restrictions on cross-border data transfers.[60] But even the countries pursuing more open approaches allow for broad-based restrictions of CBDFs. At the same time, the most recent re-iterations of the Chinese legislation governing CBDFs are more open compared to the past.[61]

The inconsistent regulatory environment surrounding data governance may generate barriers and give rise to compliance issues and legal contradictions. One possible measure to reduce the risks posed by regulatory disparities involves the adoption of data protection laws that meet the stringent requirements of the GDPR. However, this could lead Indo-Pacific jurisdictions to implement legal standards that are not aligned with their domestic legal traditions. A regional alignment specifically of CBDF regulation might be a better alternative. Regional agreements, such as the APEC CBPR, might help address such concerns.[62] Furthermore, instruments, such as the Council of Europe Convention on the Automatic Processing of Personal Data, can also provide models for coordination across regions, such as between the Indo-Pacific and the EU, as well as possibly Africa, and the Americas.

3.2 *Cybersecurity Governance as Institutional Stress Test*

The Indo-Pacific region's digital economies are marked by a divergence in cybersecurity regulations. Disparities arise as advanced economies with comprehensive cybersecurity rules and policies often conflict with the less stringent regulations found in emerging markets; this often creates substantial

59 Article 17(4) of PIPA permits personal information transfers without the data subject's consent if they remain within the scope reasonably related to the original purpose of collection, subject to conditions prescribed by Presidential Decree. These conditions consider potential disadvantages to the data subject and the implementation of necessary security measures, such as encryption.

60 APPI, art 28.

61 See Personal Information Protection Law of the People's Republic of China 2021, ch III; Data Security Law of the People's Republic of China 2021, 'Network Data Security Management Regulation 2024' Regulations on Cross-Border Data Flows 2024. See Guang Ma and Hong Wu, 'Cross-border Data Flow Supervision in China's Free Trade Zones: Security and Compliance Rules' (2025) Asia Pacific Law Review <https://doi.org/10.1080/10192557.2025.2471312> accessed 29 April 2025 (arguing that recent FTZ measures – especially in Beijing, Hainan, and Tianjin – allow outbound data transfers under pilot mechanisms that incrementally relax DSL/PIPL compliance obligations, reflecting a shift toward pragmatic regulatory experimentation).

62 See Subsection 4.3 below.

barriers to digital trade and investment. In this respect, addressing cybersecurity remains essential to fostering robust digital integration across the Indo-Pacific.

Certain advanced jurisdictions, such as Japan, South Korea, and Singapore, have implemented rigorous cybersecurity measures. Japan's Basic Act on Cybersecurity (BAC) provides a foundational framework for cybersecurity across critical infrastructure.[63] It mandates that both national and local governments actively collaborate with private operators to enhance cybersecurity resilience, establishing clear public-private roles in cyber incident response and prevention. Under Article 25 of the BAC, the Cybersecurity Strategy Headquarters is responsible for formulating Japan's Cybersecurity Strategy,[64] while the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) implements and oversees these measures.[65] The BAC was further amended in 2018 to establish a Cybersecurity Council, a platform allowing government agencies and business operators to share critical threat intelligence, ultimately facilitating a coordinated approach to cybersecurity governance across sectors.[66] Additionally, Japan's Telecommunication Business Act (TBA) governs the confidentiality of communications handled by telecommunications carriers, prohibiting the unauthorized disclosure of communication data, including access logs and IP addresses.[67] While the TBA aims to protect

63 The Basic Act on Cybersecurity was promulgated on 12 November 2014 to establish a structured approach to cybersecurity policy in Japan. See Basic Act on Cybersecurity, Act No 104 of 2014, later amended by Act No 68 of 2022 (JPN).

64 Article 25 of Japan's Basic Act on Cybersecurity establishes the Cybersecurity Strategy Headquarters (CSHQ), responsible for drafting and overseeing Japan's cybersecurity strategy. The CSHQ sets standards for cybersecurity across government bodies, evaluates critical incidents, and coordinates policy across agencies. This ensures cohesive national cybersecurity measures; see ibid art 25.

65 The NISC is established and operates under the Basic Act on Cybersecurity, specifically enabled by amendments related to Article 25. The NISC, working under the Cybersecurity Strategy Headquarters, has a mandate to implement Japan's cybersecurity strategy, coordinate incident responses, and oversee cybersecurity standards across governmental agencies and critical infrastructure.

66 The 2018 amendment to the Basic Act on Cybersecurity established the Cybersecurity Council under Article 17. The Council aims to address the increasingly sophisticated nature of cyber threats through shared intelligence and a unified incident response structure. This collaborative model aligns with global cybersecurity practices that emphasize public-private partnerships, allowing Japan to create a more resilient, adaptive cybersecurity posture across essential service providers.

67 Telecommunications Business Act, Act No 86 of 1984 (JPN), governs the confidentiality of communications through Article 4, which mandates that telecommunications carriers must protect the secrecy of communications they handle; see Hideki Iide, 'Japan's Telecommunications Industry: Industrial Organization' (1990) 19 Japanese Economic

communication privacy, it also presents operational challenges for telecommunications carriers, who must navigate this framework when handling cyber threat data. To clarify these responsibilities, Japan's Ministry of Internal Affairs and Communications (MIC) has issued interpretative guidelines through the Council on the Stable Use of the Internet.[68] These guidelines outline lawful data-sharing practices among carriers to combat cyber threats effectively without infringing on communication privacy rights.[69] Furthermore, Japan's APPI imposes strict requirements on business operators for managing personal data.[70] This includes mandatory breach notifications to the Personal Information Protection Commission and affected individuals under specific conditions, ensuring accountability and compliance with data privacy standards.[71] Business operators are permitted to share information on cyber threats only within the framework of these data protection laws, which poses particular constraints when such data overlaps with personal information. Together, Japan's cybersecurity and data protection regulations fundamentally reflect a sophisticated and structured approach to cybersecurity, balancing

Studies, 61. Article 4 prohibits carriers from disclosing communication data, such as access logs and IP addresses, without proper authorization, ensuring privacy protections for users within the telecommunications sector.

68 See eg Shuya Hayashi, 'The Concept of "Communications" and "Broadcasting" in the Era of Digital Convergence' in Hitoshi Mitomo and Mikio Kimura (eds), *Broadcasting in Japan: Challenges and Opportunities* (Springer Singapore 2022).

69 The MIC, in collaboration with the Cybersecurity Council, released the Guidance for Sharing and Disclosure of Information on Damage from Cyberattacks. These guidelines, developed by a study group comprising the MIC, the NISC, the National Police Agency, the Ministry of Economy, Trade and Industry, and the Japan Computer Emergency Response Team Coordination Center/Coordination Center, outline specific lawful practices for sharing data related to cyberattack damage among telecommunications carriers and relevant organizations, with a focus on maintaining communication confidentiality standards while enhancing cybersecurity response capabilities. See Japan Cybersecurity Council Steering Committee, 'Saiba Kogeki Higai Ni Kakaru Joho No Kyoyu Kohyo Gaidansu [Guidance for Sharing and Disclosure of Information on Damage from Cyberattacks]' (Ministry of Internal Affairs and Communications, 8 March 2023) <https://www.soumu.go.jp/main_content/000867112.pdf> accessed 29 April 2025.

70 Wataru Aikawa, 'Japan's Cybersecurity Policy' in Hitoshi Mitomo (ed), *Telecommunications Policies of Japan* (Springer Singapore 2020).

71 The amended APPI, effective from 1 April 2022, mandates that organizations must notify the Personal Information Protection Commission and affected individuals of data breaches under certain conditions. These conditions include incidents involving sensitive data, risks of unauthorized use, breaches affecting over 1,000 individuals, or breaches likely to cause harm. Notifications to the Personal information Protection Commission must begin with an initial report within three to five days, followed by a detailed final report within 30 days. See APPI 2003, later amended by Act No 37 of 2021, art 26.

privacy and security through specific obligations that foster sectoral accountability. These domestic laws serve as exemplars within the Indo-Pacific for constructing resilient cyber defenses while aligning public-private responsibilities to manage cyber incidents. Japan's regulatory approach thus helps to measure the many cross-border challenges that other Indo-Pacific jurisdictions will face in achieving cybersecurity standardization.

Similarly, South Korea's Cybersecurity Management System enforces robust security practices through a comprehensive legal framework.[72] Under the Act on the Protection of Information and Communications Infrastructure, operators of critical infrastructure are mandated to report cybersecurity incidents promptly and undergo regular cybersecurity audits.[73] These legal requirements ensure strict compliance and accountability, while also incorporating stringent penalties for non-compliance. Additionally, the PIPA complements these measures by safeguarding personal data and enhancing transparency in data handling practices.[74] In fact, South Korea not only elevates standards of accountability and transparency but also establishes a rigorous benchmark for regulatory structures. This integrated approach serves as another advanced model for other jurisdictions seeking to strengthen their cybersecurity governance through robust legal mechanisms.

Other countries, focus on private-sector accountability. Australia's Security of Critical Infrastructure Act[75] mandates comprehensive compliance for private entities involved in critical infrastructure, including incident reporting and threat mitigation.[76]

---

72 Natasha Wood, 'South Korea's 2024 Cyber Strategy: A Primer' (CSIS, 2 August 2024) <https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer> accessed 29 April 2025.

73 Dong Hyeon Kim and Do Hyun Park, 'Automated Decision-Making in South Korea: A Critical Review of the Revised Personal Information Protection Act' (2024) 11 Humanities and Social Sciences Communications <https://www.nature.com/articles/s41599-024-03470-y> accessed 29 April 2025.

74 Jae Jeon Seung, Myung Seok Go and Ju Hyun Namgung, 'Use of Personal Information for Artificial Intelligence Learning Data Under the Personal Information Protection Act: The Case of Lee-Luda, An Artificial-Intelligence Chatbot in South Korea' (2022) 31 Asia Pacific Law Review 55.

75 Australia's Security of Critical Infrastructure Act 2018 (SOCI Act), especially following 2021–2022 amendments, requires critical infrastructure entities to implement incident response, threat mitigation, and risk management programs. *Security of Critical Infrastructure Act 2018* (Cth), later amended by *Security Legislation Amendment* (*Critical Infrastructure*) *Act 2021* (Cth) and *Security Legislation Amendment* (*Critical Infrastructure Protection*) *Act 2022* (Cth).

76 Department of Home Affairs, '2023–2030 Australian Cyber Security Strategy' (Commonwealth of Australia, 22 November 2023), <https://www.homeaffairs.gov.au/cyber-secu

Still, across jurisdictions, there is a growing emphasis on risk-based regulation. While definitions and applications of risk vary, the underlying principle offers a foundation for cross-border cooperation. Its inclusion in US-led trade instruments, such as the USMCA and the US-Japan Digital Trade Agreement, suggests growing influence beyond North America.[77] In the ASEAN context, the ASEAN Cybersecurity Cooperation Strategy facilitates regional coordination on cybersecurity without mandating uniform regulatory standards.[78] This flexibility permits member states to retain domestic control over data regulations while promoting a cooperative regional response through initiatives like the ASEAN-Japan Cybersecurity Capacity Building Centre, which provides cybersecurity training for officials.[79] This approach strengthens regional cyber resilience without compromising national sovereignty, illustrating a collaborative yet adaptable model for regional cooperation.

On the international front, alignment challenges are compounded by differing levels of treaty adoption. For example, reluctance from some Indo-Pacific nations to ratify the Budapest Convention on Cybercrime limits cross-border collaboration on cybercrime investigation efforts.[80] Countries, such as India and China, have opted not to ratify the Budapest Convention, expressing concerns over sovereignty and perceived imbalances in data access provisions, particularly regarding cross-border data requests and transborder access

---

rity-subsite/files/2023-cyber-security-strategy.pdf> accessed 29 April 2025; see also Gary Waters, 'National Cyber Emergency Policy for Australia: Critical Infrastructure' in Greg Austin (ed), *National Cyber Emergencies: The Return to Civil Defence* (Routledge 2020).

77 United States-Mexico-Canada Agreement (entered into force 1 July 2020) art 19.15; US-Japan Digital Trade Agreement (entered into force 1 January 2020) art 8.

78 The ASEAN Cybersecurity Cooperation Strategy, adopted on 28 January 2022 during the 2nd ASEAN Digital Ministers' Meeting, outlines non-binding regional coordination frameworks to strengthen cybersecurity across member states, focusing on capacity building and collaborative response mechanisms rather than uniform regulatory standards. See ASEAN Secretariat, '2021-2025 ASEAN Cybersecurity Cooperation Strategy' (1 February 2023) <https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf> accessed 29 April 2025.

79 The ASEAN-Japan Cybersecurity Capacity Building Centre, established in 2018 with support from the Japan-ASEAN Integration Fund, offers specialized cybersecurity training for ASEAN Member States. This initiative focuses on enhancing the skills of officials and critical infrastructure operators to fortify the region's cybersecurity capabilities. See 'ASEAN-Japan Cybersecurity Capacity Building Centre' (AJCCBC) <https://ajccbc.ncsa.or.th/about-us/> accessed 29 April 2025. See also Yu-Kyung Kim and others, 'Evaluating Cybersecurity Capacity Building of ASEAN Plus Three Through Social Network Analysis' (2023) 24 Journal of Internet Technology 495.

80 Convention on Cybercrime (2001) ETS 185.

without mutual assistance.[81] Japan and the Philippines, by contrast, have ratified the Convention, recognising the benefits of structured cooperation in responding to cross-border cyber threats. In other parts of the region, national preferences concerning data jurisdiction and privacy protection continue to influence the extent of engagement with international treaty commitments.

Data localization laws in countries, such as Indonesia and Vietnam, also significantly impact regional interoperability.[82] These laws require certain types of data, particularly the ones that are sensitive to national security, to remain within domestic borders. This aims to bolster digital sovereignty but challenges cross-border digital trade. Domestic mandates often conflict with regional and international data transfer standards, such as the APEC CBPR, revealing regulatory tensions that Indo-Pacific economies face in attempting to achieve both (cyber)security and economic integration.

A more coordinated cybersecurity strategy would help enhance the Indo-Pacific's digital competitiveness. Such a cybersecurity strategy would have to respect national diversity while setting high standards. Japan's sophisticated model, with its structured public-private coordination and strong data protection laws, could serve as a benchmark for advancing regulatory alignment. However, rather than strict uniformity, the focus should be on developing flexible, adaptable standards that allow emerging economies to adopt best practices at their own pace. This approach would encourage secure, compliant digital interactions across member states, enabling the region to build a unified digital economy that is resilient, legally predictable, and open to innovation.

3.3 *Digital IP Enforcement Across Fragmented Jurisdictions*

The rise of digital platforms and technologies has introduced new IP challenges, such as digital piracy and the protection of software and algorithms. As a result, IP laws in the Indo-Pacific should reflect the digital context and ensure robust protection for digital innovations while facilitating technology sharing. Traditional legal measures are often insufficient to address rapid, unidentifiable infringements, leading to the use of digital rights management

81 Lennon Yao-Chung Chang and Han-Wei Liu, 'Ensuring Cybersecurity for Digital Services Trade' in Jong Woo Kang and others (eds), *Unlocking the Potential of Digital Services Trade in Asia and the Pacific* (Asian Development Bank 2022).

82 Indonesia's data localization laws, particularly Law Number 71 Year 2019 concerning Electronic System and Transaction Operations (The Republic of Indonesia State Gazette Year 2019 Number 185), and Vietnam's Cybersecurity Law (Cybersecurity Law, 24/2018/QH14, mandate local storage of specific data categories, including personal data of their citizens. These localization mandates may deter investments and limit the growth of cross-border digital services in these countries as well as within the region.

(DRM) and detection algorithms.[83] However, without unified international regulations, these technological approaches are limited. Current strategies include aligning IP laws internationally and employing AI for automated enforcement, though comprehensive digital IP protection remains complex.

Advanced economies in the region, such as Japan and South Korea, have well-developed IP laws that provide strong protection for digital innovation.[84] For instance, Japan's Copyright Act and South Korea's Patent Act are aligned with the WIPO treaties, ensuring strong IP protection and enforcement.[85] The robust IP protections in Japan and South Korea contribute positively to digital trade by providing a secure environment for investments in digital technologies and intellectual assets. These protections encourage foreign firms to operate with reduced risk of IP theft, thereby enhancing cross-border innovation. For the Indo-Pacific regulatory environment, these frameworks set a high standard for IP governance, signalling to other nations the economic benefits of strengthened IP enforcement aligned with international standards.

By contrast, some Indo-Pacific countries may have less stringent IP protection, leading to legal uncertainties in protecting digital assets. For example, despite recent developments, countries, such as Indonesia, still face challenges in fully aligning IP laws with international standards.[86] Strengthening enforcement mechanisms, promoting regional cooperation as well as aligning IP laws with some WIPO treaties, will remain essential to address cross-border IP issues and facilitate the exchange of information and expertise.

---

83 Traditional IP laws struggle against the speed and scale of online infringements. DRM systems, which use encryption to restrict access, aim to prevent unauthorized copying and distribution. However, they can be bypassed, and critics argue they may restrict legitimate use, such as educational sharing. Detection algorithms, including AI-based content recognition, flag potentially infringing content by comparing it to copyright databases. While effective in some cases, these methods are limited by high costs and cannot address all instances of piracy, especially when infringers continually alter content or location to evade detection. See eg Jamil Afzal, *Implementation of Digital Law as a Legal Tool in the Current Digital Era* (Springer Singapore 2024).

84 Hiroki Habuka, 'Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency' (CSIS, 14 February 2023) <https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-02/230214_Habuka_Japan_AIRegulations.pdf?VersionId=BnLSQRRq0O9jQ8u1RW3SGKOA0i8DBc4Q> accessed 29 April 2025.

85 Both Japan and Korea are actively involved in international IP agreements and have robust enforcement mechanisms to combat digital piracy and infringements. See Copyright Act, Act No 48 of 1970, as amended Act No 52 of 2021 (JPN); Patent Act, Act No 950 of 1961, later amended by Act No 20322 of 2024 (ROK).

86 Imam Hanafi and Arief Fahmi Lubis, 'Protection of Privacy and Intellectual Property Rights in Digital Data Management in Indonesia' (2023) 2 Easta Journal Law and Human Rights 33.

3.4 *Taxing the Digital: Between Fiscal Autonomy and Coordination*

The rapid growth of digital businesses has exposed significant gaps in existing tax frameworks, particularly in capturing value from companies operating without a physical presence. The lack of physical economic presence in the country where the digital activity is carried out has resulted in governments (i) introducing unilateral rules – such as digital service tax, withholding tax, equalization levy, digital permanent establishment, significant economic presence, as well as (ii) putting forward international proposals to tax highly digitalized business – above all under the OECD Pillar One and Pillar Two initiatives.[87] Pillar One aims to tax the income of highly digitalized businesses operating in countries without a physical presence, whereas Pillar Two aims to reduce tax competition, by introducing a global minimum tax of 15%. Both initiatives will have an effect on digitalized business with respect to trade (Pillar One) and investment (Pillar Two).[88] In a nutshell, these initiatives aim to reallocate taxing rights and implement a global minimum tax to counter base erosion and profit shifting, directly impacting trade and investment flows in digital economies.

The objective of these regulatory efforts is twofold: to improve conditions for trade and investment, and to ensure that digital businesses contribute a fair portion of tax revenues in the jurisdictions where economic value is generated. However, while Pillar Two rules are being implemented, discussions regarding the introduction of the Pillar One rules are still ongoing. At the time of writing, several Indo-Pacific countries have adopted unilateral measures to ensure the fair taxation of digitalized business in the absence of a physical economic presence, such as digital services taxes, withholding tax, equalization levy, and significant economic presence. Examples include India, Malaysia, Japan, Indonesia, Vietnam, New Zealand, and Thailand.[89]

---

87 See Irma Johanna Mosquera Valderrama, 'Trade Digitalization and Taxation' in Julien Chaisse and Cristián Rodríguez-Chiffelle (eds), *Elgar Companion to the World Trade Organization* (Edward Elgar 2023).

88 Tibor Hanappi and Ana Cinta González Cabral, 'The Impact of the Pillar One and Pillar Two Proposals on MNE's Investment Costs: An Analysis Using Forward-Looking Effective Tax Rates' (2020) OECD Taxation Working Papers 50 <https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/the-impact-of-the-pillar-one-and-pillar-two-proposals-on-mne-s-investment-costs_93c19699/b0876dcf-en.pdf> accessed 29 April 2025.

89 See Era Dable-Norris and others, 'Digitalization and Taxation in Asia' (2021) International Monetary Fund Departmental Papers 2021/017 <https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/09/13/Digitalization-and-Taxation-in-Asia-460120> accessed 29 April 2025; Bruno da Silva and Rolando Avendano, 'Trade in Digital Services and International Taxation: Implication for Development Asia' in Jong

Notwithstanding the above, one of the conditions of the Political Statement (2021 and 2023) endorsing the Pillar One and Pillar Two Initiatives is for countries to refrain from introducing Digital Service Tax and other relevant similar unilateral measures.[90] This statement has been endorsed by 142 tax jurisdictions, including the tax jurisdictions that have introduced unilateral measures above. The question that arises is how countries will reconcile these multilateral (political) commitments with the unilateral measures already in place. These developments in taxation go beyond e-commerce and affect the broader digital economy in the Indo-Pacific.[91]

In addition, the lack of precedent on how to regulate digital economic activity, which is inherently cross-border, often leads to frictions.[92] For example, the interaction between trade and some of the above-mentioned unilateral rules for taxing digitalized businesses has led countries like the United States to initiate trade investigations against nations implementing a digital services tax or equalization levy.[93] These investigations are currently suspended while awaiting the taxation of highly digitalized business rules (Pillar One), which include the negotiation of a Multilateral Convention to Implement

---

Woo Kang and others (eds), *Unlocking the Potential of Digital Services Trade in Asia and the Pacific* (Asian Development Bank 2022).

90 OECD, 'Outcome Statement on the Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy' (11 July 2023) para 9 <https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/beps/outcome-statement-on-the-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-july-2023.pdf> accessed 29 April 2025.

91 See Julien Chaisse, 'Taxing the Digital Economy: Cross-Border Data and Trade Policies in Asia' in *The Role and Future of Digital Economy Agreements in Developing Asia and the Pacific* (Asian Development Bank 2025) 137 <https://www.adb.org/publications/digital-economy-agreements-asia-pacific> accessed 29 April 2025. See also Nella Hendriyetty and others (eds), *Taxation in the Digital Economy: New Models in Asia and the Pacific* (Routledge 2022).

92 See generally Georgios Dimitropoulos, 'Law and Digital Globalization' (2022) 44 University of Pennsylvania Journal of International Law 41.

93 One example in the Indo-Pacific is Indonesia; see Office of the United States Trade Representative Press Release, 'Section 301 Investigations Status Update on Digital Services Tax Investigations of Brazil, the Czech Republic, the European Union, and Indonesia' (13 January 2021) <https://ustr.gov/sites/default/files/files/Press/Releases/StatusUpdate301InvestigationsBEUIndCR.pdf> accessed 29 April 2025; see also Ichwan Sukardi and Sophia Jiaqian She, 'Taxing the Digital Economy in Indonesia' (*International Tax Review*, 22 September 2022) <https://www.internationaltaxreview.com/article/2a6a6s9xb79f62ftcu41s/taxing-the-digital-economy-in-indonesia> accessed 29 April 2025.

Amount A of Pillar One (Multilateral Convention).[94] It is not yet certain that Pillar One rules, including the Multilateral Convention, will be adopted by all countries.[95] The Indo-Pacific's diverse economies now confront strategic decisions about how to reconcile fiscal sovereignty with the need to generate revenue from digital business under emerging international tax arrangements. These decisions will affect the direction and depth of regional integration in the digital economy.[96]

Regarding Pillar Two, the use of incentives to attract digital manufacturing and enhance technological innovation may need to be reconsidered in light of the potential introduction of a global minimum tax rate. Currently, 139 tax jurisdictions have endorsed the October 2021 Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalization of the Economy. A majority of Indo-Pacific countries have endorsed this statement. Bangladesh, Bhutan, Cambodia, Nepal, Myanmar, the Pacific Island countries, Pakistan, Sri Lanka, Taiwan, and Timor Leste have not endorsed it.[97] Countries in the Indo-Pacific are in the process of drafting legislation to implement the Pillar Two rules (for example, Thailand, Australia) or have already adopted these rules (for example, Japan, South Korea, Vietnam, Malaysia, and New Zealand).[98] While introducing these rules, countries need to consider how to keep providing incentives to digitalized businesses, which may be difficult with the global minimum tax rate. This may lead to differing approaches among countries, affecting the integration of the digital economy across the Indo-Pacific region.

94 OECD Press Release, 'Statement by the Co-Chairs of the OECD/G20 Inclusive Framework on BEPS' (30 May 2024) <https://www.oecd.org/en/about/news/announcements/2024/05/statement-by-the-co-chairs-of-the-oecdg20-inclusive-framework-on-beps.html> accessed 29 April 2025.

95 David Lawder, 'US, India Extend Digital Tax Truce to Sunday as Deadline Approaches' (*Reuters*, 29 June 2024) <https://www.reuters.com/world/india/us-india-extend-digital-tax-truce-sunday-deadline-approaches-2024-06-28/> accessed 29 April 2025.

96 Julien Chaisse, 'Tax, Trade, and Investment Conundrum in Asia-Pacific Regionalism' (2023) 31 Asia Pacific Law Review 535.

97 See OECD, 'Members of the OECD/G20 Inclusive Framework on BEPS Joining the Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy as of 9 June 2023' <https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/beps/oecd-g20-inclusive-framework-members-joining-statement-on-two-pillar-solution-to-address-tax-challenges-arising-from-digitalisation-october-2021.pdf> accessed 29 April 2025.

98 For an overview of the implementation of Pillar Two rules see KPMG, 'BEPS 2.0 Pillar Two State of Play – Global Developments Summary' (17 May 2024) <https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/beps2-state-of-play-summary.pdf> accessed 29 April 2025.

In addition to the taxation of digitalized business, taxation is also relevant in other areas, for instance regarding digital transformation of tax administrations to ensure domestic resource mobilization,[99] the use of AI in tax analytics to prevent fraud and tax evasion,[100] as well as the introduction of cybersecurity measures to prevent leaks of taxpayer's information and to guarantee the protection of privacy and confidentiality of taxpayer's information.[101]

Overall, the Indo-Pacific's diverse tax strategies reveal a tension between fiscal autonomy and the need for regulatory cohesion in digital markets. As countries implement and adapt to global tax standards, inconsistencies risk creating trade barriers, potentially slowing digital integration. A balanced approach that respects national interests while promoting interoperability in tax policy could prevent fragmentation, ensuring that digital businesses operate within a stable, predictable framework across the Indo-Pacific. Regulatory coordination is critical for sustaining regional competitiveness in an increasingly digital global economy.

3.5 *Coordination Without Unification: The Emerging Indo-Pacific Legal Grammar*

Efforts to coordinate digital regulation in the Indo-Pacific have produced a range of international agreements, reflecting different legal forms, institutional strategies, and substantive ambitions. These agreements can be grouped into four broad categories: regional trade agreements with digital provisions, stand-alone digital economy agreements, sectoral and/or informal coordination mechanisms, and plurilateral frameworks.[102] These instruments do not operate in isolation. Many states in the region are parties to multiple overlapping commitments, which may function in parallel or, at times, come into conflict depending on the regulatory domain. In this context, regulatory

99 Ehtisham Ahmad and Aekapol Chongvilaivan, *Digital Transformation of Multilevel Tax Policies and Administration for Resilience and Sustainable Growth* (Asian Development Bank 2024).

100 Mohammad Hassan Shakil and Mashiyat Tasnia, 'Intelligence and Tax Administration in Asia and the Pacific' in Hendriyetty and others (n 81). More recently, see also Joshua Aslett and others, 'Understanding Artificial Intelligence in Tax and Customs Administration' (2024) 2024 *Technical Notes and Manuals* 1 <https://www.elibrary.imf.org/view/journals/005/2024/006/005.2024.issue-006-en.xml> accessed 29 April 2025.

101 Mosquera Valderrama (n 53).

102 The agreements analyzed in this section, and throughout the special issue, can be readily located within the TAPED dataset. This comprehensive resource maps digital trade provisions in PTAs since 2000, covering over 465 agreements. It includes 130 coded items spanning digital trade, IP, services, government procurement, trade in goods, exceptions, and emerging issues. See Burri, Vásquez Callo-Müller and Kugler (n 28).

coordination depends less on uniform legal standards than on the ability to align instruments and practices across jurisdictions with divergent institutional preferences and capacities. While the four categories discussed below capture the region's primary legal strategies for digital integration, one notable omission across nearly all of them is the lack of robust dispute resolution mechanisms. Most existing agreements include only soft commitments to dialogue or cooperation. This reflects an effort to balance an open digital economy with respect for digital sovereignty.

3.5.1 Trade Agreements: Thin Commitments, Structural Limits

Firstly, PTAs in the broader Indo-Pacific, including the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership (RCEP), offer frameworks for regulatory cooperation and the establishment of regional standards. While these are traditional PTAs aimed at reducing trade barriers, they also include dedicated chapters on electronic commerce. CPTPP's Chapter 14 on electronic commerce, sets minimum standards for data protection, electronic authentication, and paperless trading. The same largely applies to RCEP and its Chapter 12 on electronic commerce, despite the more digital sovereignty-oriented provisions. Yet, the commitments undertaken in each agreement differ in scope and depth. CPTPP contains a standalone chapter on regulatory coherence (Chapter 25), encouraging transparency, impact assessments, and institutional coordination. RCEP, by contrast, takes a more cautious approach; both the broader framework, and its e-commerce chapter stop short of imposing such obligations.[103] These divergences indicate differing visions of digital economy governance and may pose regulatory dilemmas for economies simultaneously bound by both treaties. Despite divergencies, these agreements can help mitigate regulatory fragmentation by aligning standards and thereby fostering a more cohesive digital economy.

Within ASEAN, the digital sector has experienced substantial growth, driven by the widespread adoption of digital technologies across various industries.[104] The responsibilities of ASEAN's Information and Communications Technology (ICT) ministries have broadened beyond traditional ICT infrastructure

103 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (entered into force 30 December 2018) ch 25; Regional Comprehensive Economic Partnership (entered into force 1 January 2022) ch 12.

104 Saif ur Rehman, Abid Rashid Gill and Minhaj Ali, 'Information and Communication Technology, Institutional Quality and Environmental Sustainability in ASEAN Countries' (2023) Environmental Science and Pollution Research <https://link.springer.com/content/pdf/10.1007/s11356-023-27219-3.pdf> accessed 29 April 2025.

and telecommunications oversight to include digital data governance, cybersecurity, and the regulation of online platforms.[105] These expanded duties aim to create a secure and innovative digital environment, facilitating ASEAN's transformation into a digitally integrated society and economy.

ASEAN has introduced several strategic frameworks to support this integration. The ASEAN Digital Integration Framework and its Action Plan (DIFAP), for example, function as comprehensive roadmaps for digital integration, covering priorities, such as trade facilitation, data flows, electronic payments, and entrepreneurship.[106] DIFAP's adaptability allows it to address the diverse needs of ASEAN's digital ecosystem through both rule-based mechanisms and thematic partnerships.[107] Another notable initiative is the Bandar Seri Begawan Roadmap, introduced in 2021 to accelerate digital transformation in the wake of the COVID-19 pandemic.[108] This multi-year plan seeks to enhance ASEAN's digital connectivity, with a significant milestone being the start of negotiations for an ASEAN DEFA by 2025.[109]

105 Recent initiatives include the ASEAN Framework on Digital Data Governance and the establishment of regional Computer Emergency Response Teams, aimed at enhancing cross-border cybersecurity capabilities and harmonizing data governance standards; see ASEAN, 'ASEAN Framework on Digital Data Governance' (September 2020) <https://cil.nus.edu.sg/wp-content/uploads/2020/09/2018-Framework-Digital-Data-Governance.pdf>; see also ASEAN, 'Singapore Declaration' (February 2024) <https://asean.org/wp-content/uploads/2024/02/ENDORSED-Singapore-Declaration_30-Jan-2024-CLN.pdf> both accessed 29 April 2025, outlining regional data governance and cybersecurity initiatives under the ASEAN Digital Masterplan 2025, the ASEAN Framework on Digital Data Governance, and the ASEAN Digital Economy Framework Agreement (DEFA).

106 Ikumo Isono and Hilmy Prilliadi, 'ASEAN's Digital Integration: Evolution of Framework Documents' (ERIA 2023) <https://www.eria.org/uploads/media/Books/2023-ASEAN-Digital/ASEAN-Digital-Integration-ERIA-23Aug.pdf>. See also Lili Yan Ing and others, 'ASEAN Digital Community 2045' (2023) ERIA Discussion Paper Series 487 <https://www.eria.org/uploads/ASEAN-Digital-Community-2045-DP.pdf> both accessed 29 April 2025.

107 Neha Mishra and Ana Maria Palacio Valencia, 'Digital Services and Digital Trade in the Asia Pacific: An Alternative Model for Digital Integration?' (2023) 31(2) Asia Pacific Law Review 489 <https://doi.org/10.1080/10192557.2023.2216058> accessed 29 April 2025 (arguing that Asia-led agreements like RCEP and the ASEAN e-commerce frameworks pursue digital integration through deliberately narrow commitments that sidestep controversial regulatory issues while still advancing coordination on trade facilitation and digital trust).

108 Paul Cheung and Taojun Xie (eds), *The ASEAN Digital Economy: Towards an Integrated Regional Framework* (Routledge 2023).

109 Initiated in 2023, the DEFA builds on earlier efforts, focusing on digital trade facilitation, payment system integration, and the development of common standards, while also addressing emerging technologies, such as AI. See Mukhamad Zulianto, 'ASEAN Digital

Although ASEAN's agreements (such as the 2018 e-commerce treaty and the Digital Integration Framework) signal certain progress, their impact often depends on voluntary compliance and informal coordination.[110] Moreover, these initiatives work in synergy with broader trade agreements – and their e-commerce chapters, such as RCEP and the updated ASEAN-Australia-New Zealand Free Trade Agreement. ASEAN's regulatory model reflects an implicit trade-off: it preserves sovereignty by avoiding binding obligations while encouraging convergence through best practices and soft templates.[111] This model works within the region's political realities, but its limits must be acknowledged.

3.5.2 Digital Economy Agreements: Modularity as Legal Technique

Second, the region has 'invented' a new form of agreement for digital trade and the digital economy, the DEAs. Singapore has spearheaded this approach.[112] The Digital Economy Partnership Agreement (DEPA) signed in June 2020 is the first agreement of this kind. DEPA was initially signed by Singapore, New Zealand, and Chile,[113] and expanded its membership to include South Korea, which joined in 2023, further strengthening the agreement's role as a platform for digital trade integration and cooperation across the Indo-Pacific. Other countries, both from the Indo-Pacific, such as China and the United Arab Emirates, as well as outside, such as Canada, have expressed interest in joining DEPA, signalling its growing influence in shaping the global digital economy.

Economy Framework Agreement (DEFA): Opportunities and Challenges for Vietnam' (2024) 10 Asia-Pacific Journal of Public Policy 53.

110 Lurong Chen, 'ASEAN in the Digital Era: Enabling Cross-Border E-Commerce' in Lurong Chen and Fukunari Kimura (eds) *Developing the Digital Economy in ASEAN* (Routledge 2019).

111 See Shintaro Hamanaka, 'ASEAN's Approach to Regional Economic Integration: Flexible, Political, and Gradual' (2021) 48 JCMS 1235.

112 Ministry of Trade and Industry Singapore, 'Digital Economy Agreements' (31 January 2025) <https://www.mti.gov.sg/Trade/Digital-Economy-Agreements> accessed 29 April 2025. See also Jason Grant Allen and Qiu Xu Martin Liao, 'Digital Economy Innovation and Implementation in the Indo-Pacific: Towards a "Singapore Effect"?' 26(4) JWIT 680–711 in this Special Issue.

113 DEPA is a legally binding digital trade agreement under public international law. It entered into force in 2020 between Singapore and New Zealand, with Chile following in 2021. Digital Economy Partnership Agreement (entered into force 7 January 2021); see <https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/> accessed 29 April 2025.

Thematically, DEPA focuses on the cross-border digital economy based on free data flows and non-discrimination principles for digital products.[114] DEPA is structured around multiple modules that address key aspects of the digital economy, including CBDFs, privacy protection, AI ethics, digital trade facilitation, and consumer trust. The modular approach allows countries to adopt specific provisions at their own pace, reflecting their unique digital development goals and regulatory frameworks. Another innovative feature of DEPA is its focus on emerging technologies, such as blockchain, paperless trade, and AI, making it adaptable to future advancements. Finally, the agreement emphasizes inclusive participation, ensuring that SMEs can access the benefits of the digital economy.

DEPA serves as a blueprint for digital trade agreements, offering a flexible and scalable framework that aligns with WTO principles, on the one side, while addressing the unique challenges of the digital economy as well as accommodating the interests and needs of individual signatories.[115] Its modular structure allows states to opt into specific commitments, reducing entry barriers and enhancing appeal to a diverse set of economies. This also encourages experimentation in an evolving area of regulation. Still, this same flexibility may weaken enforceability or dilute legal certainty if key members backtrack or apply modules inconsistently. In periods of geopolitical instability, such as during shifts in US trade policy or regional disputes, DEPA's resilience will depend on whether its informal design can withstand political pressures without fracturing the regime.[116]

Another example, bilateral this time, is the collaboration between Singapore and Australia on the Singapore-Australia DEA signed in December 2020. It includes provisions for e-invoicing, paperless trading, and digital identities, ensuring secure engagement for both businesses and consumers in the global

114 Deborah Elms, 'Unpacking the Digital Economy Partnership Agreement (DEPA)' (Asian Trade Center, 28 January 2020) <http://asiantradecentre.org/talkingtrade/unpacking-the-digital-economy-partnership-agreement-depa> accessed 29 April 2025; see also Julien Chaisse, '"The Black Pit:" Power and Pitfalls of Digital FDI and Cross-Border Data Flows' (2023) 22 WTR 73, 86 (explaining the importance of DEPA in attracting FDI to the digital economy).

115 Surendar Singh, 'Digital Economy Partnership Agreement and the Quest for the Global Digital Trade Rule-Making: Indian Perspective' (2025) Asia Pacific Law Review <https://doi.org/10.1080/10192557.2025.2478395> accessed 29 April 2025 (arguing that DEPA's modular and opt-in architecture, inspired by CPTPP and SADEA, enables legal experimentation and gradual convergence, making it a functional template for plurilateral digital rule-making beyond WTO deadlock).

116 Meredith Kolsky Lewis, 'International Trade Agreements: Laboratories of Innovation or Propellers of Fragmentation?' (2023) 26(1) JIEL 110-223.

digital economy. The agreement also focuses on areas, such as data protection, CBDFs, and digital trade facilitation, thus providing a model for other countries to emulate.

3.5.3 Informal Cooperation: Governance Through Flexibility

A third type of agreement emerging in the Indo-Pacific digital economy is characterized by a less formal and often sectoral approach to transnational collaboration. One example is the ASEAN Smart Cities Network (ASCN), which brings together members with a view to promoting sustainable urban development through digital technologies.[117] This initiative underscores the potential of regional partnerships to drive digital innovation and address shared challenges in urban planning and infrastructure.

Similarly, the APEC CBPR system offers a framework to facilitate secure and CBDFs while ensuring robust personal data protection. This system is particularly relevant in the Indo-Pacific, where digital trade and cross-border data transfers are vital for economic integration and growth. The CBPR system allows businesses to transfer personal data across APEC economies by adhering to a uniform set of data privacy standards, reducing the complexities and costs associated with complying with diverse national privacy regulations. Although participation in the CBPR is voluntary, economies and businesses that opt in commit to upholding high data privacy standards. The framework bridges differences between national data protection laws by offering a standardized yet flexible approach to data governance. Companies that participate are certified by accountability agents, ensuring their data practices align with APEC's privacy standards. This certification enhances trust in cross-border data exchanges, thereby fostering digital trade while protecting consumer privacy.

The CBPR system complements other regional digital integration efforts, such as the ASCN, which focuses on employing digital technologies for sustainable urban growth. Together, both initiatives reflect the Indo-Pacific region's commitment to regional cooperation and innovation in the digital sphere. They illustrate a concerted effort to build a cohesive digital economy that balances technological advancement with stringent data governance and privacy protections.

117 'ASEAN Smart Cities Network' (2024) <https://asean.org/our-communities/asean-smart-cities-network/> accessed 29 April 2025.

3.5.4 Plurilateralism: Selective Integration Without Consensus

Plurilateral frameworks represent a fourth category of emerging agreements.[118] Plurilateral framework agreements are focused on more targeted cooperation and facilitate separate sector-specific (that is plurilateral) agreements within a smaller group of countries from within the original membership.[119] Already DEPA has an open membership structure since it allows accepting members beyond the original membership; it moreover allows the development of individual modules by its members as discussed above.[120] The Indo-Pacific Economic Framework for Prosperity (IPEF) is the first agreement of this kind.[121] It is a regional initiative and the first international agreement that uses the term 'Indo-Pacific'. Its current membership includes 13 Indo-Pacific countries and the US, which has led the initiative. An overarching agreement now serves as its foundation.[122] Three agreements have so far been signed under the IPEF: the Supply Chain Agreement under its Pillar II,[123] the Clean Economy

118 Georgios Dimitropoulos, Richard C Chen and Julien Chaisse, 'Plurilateralism: A New Form of International Economic Ordering?' (2025) 26 JWIT 1; Dimitropoulos (n 3).

119 Dimitropoulos, Chen and Chaisse (n 122).

120 Michelle Warren and Ziyang Fan, 'Digital Economy Agreements are a New Frontier for Trade – Here's Why' (World Economic Forum, 24 August 2022) <https://www.weforum.org/agenda/2022/08/digital-economy-agreements-trade/> accessed 29 April 2025.

121 Briefing Room, 'FACT SHEET: In Asia, President Biden and a Dozen Indo-Pacific Partners Launch the Indo-Pacific Economic Framework for Prosperity' (The White House, 23 May 2022) <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-in-asia-president-biden-and-a-dozen-indo-pacific-partners-launch-the-indo-pacific-economic-framework-for-prosperity/> accessed 29 April 2025; see Julien Chaisse and Pasha L Hsieh, 'Rethinking Asia-Pacific Regionalism and New Economic Agreements' (2023) 31 Asia Pacific Law Review 451 (highlighting that the IPEF strongly emphasizes promoting inclusive economic growth and sustainable development, alongside fostering innovation in the digital economy. The authors further explain that these priorities are crucial to the broader objectives of strengthening economic ties and strategically exerting influence while carefully navigating the economic strategies employed by China); Georgios Dimitropoulos, 'Industrial Policy and the New Internationalism: After the Liberal International Order' (forthcoming) Cornell International Law Journal (explaining that the IPEF – and similar plurilateral initiatives in the Indo-Pacific and beyond – are the result of domestic industrial strategies pursued in the US and elsewhere).

122 United States Department of Commerce, 'Agreement on the Indo-Pacific Economic Framework for Prosperity' (March 2024) <https://www.commerce.gov/sites/default/files/2024-03/IPEF-Overarching-Agreement.pdf> accessed 29 April 2025.

123 United States Department of Commerce, 'Indo-Pacific Economic Framework for Prosperity Supply Chain Agreement' (7 September 2023) <https://www.commerce.gov/sites/default/files/2023-09/2023-09-07-IPEF-Pillar-II-Final-Text-Public-Release.pdf> accessed 29 April 2025.

Agreement under Pillar III,[124] and the Fair Economy Agreement under Pillar IV.[125] While they do have certain implications for digital trade, these agreements do not operate under the trade pillar.[126] Initially, IPEF prioritized digital trade. Its first pillar was dedicated to the 'connected economy'.[127] Pillar I is now referred to as the ' Fair and Resilient Trade' pillar.[128] India has opted out of this pillar.[129] Moreover, some Southeast Asian states are said to be reevaluating their involvement in the pillar if it fails to go beyond commitments in PTAs, such as by including market access in the digital economy sector.[130]

4 Trade and Investment Law in the Indo-Pacific's Digital Economy

The digital economy has become a core component of economic development strategies across the Indo-Pacific. Countries such as Singapore and South Korea have demonstrated that targeted legal reforms, combined with

124 United States Department of Commerce, 'Indo-Pacific Economic Framework for Prosperity Agreement Relating to a Clean Economy' (March 2024) <https://www.commerce.gov/sites/default/files/2024-03/IPEF-PIII-Clean-Economy-Agreement.pdf> accessed 29 April 2025.

125 United States Department of Commerce, 'Indo-Pacific Economic Framework for Prosperity Agreement Relating to a Fair Economy' (March 2024) <https://www.commerce.gov/sites/default/files/2024-03/IPEF-PIV-Fair-Economy-Agreement.pdf> accessed 29 April 2025.

126 See United States Trade Representative, 'Ministerial Text for Trade Pillar of the Indo-Pacific Economic Framework for Prosperity' (September 2019) <https://ustr.gov/sites/default/files/2022-09/IPEF%20Pillar%201%20Ministerial%20Text%20(Trade%20Pillar)_FOR%20PUBLIC%20RELEASE%20(1).pdf>; Briefing Room, 'FACT SHEET: In San Francisco, President Biden and 13 Partners Announce Key Outcomes to Fuel Inclusive, Sustainable Growth as Part of the Indo-Pacific Economic Framework for Prosperity' (The White House, 16 November 2023) <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/11/16/fact-sheet-in-san-francisco-president-biden-and-13-partners-announce-key-outcomes-to-fuel-inclusive-sustainable-growth-as-part-of-the-indo-pacific-economic-framework-for-prosperity/> both accessed 29 April 2025.

127 Briefing Room (n 105).

128 See United States Department of Commerce, 'Pillar I – Fair and Resilient Trade' <https://www.commerce.gov/ipef/pillar-i> accessed 29 April 2025; see also United States Trade Representative (n 110).

129 India's fears are not related to the digital economy, but rather potential issues with environmental and labour rights; see 'The United States Launches the Indo-Pacific Economic Framework for Prosperity and the Americas Partnership for Economic Prosperity' (2022) 116 AJIL 868, 871.

130 Andreyka Natalegawa and Gregory B Poling, 'The Indo-Pacific Economic Framework and Digital Trade in Southeast Asia' (CSIS, 5 May 2022) <https://www.csis.org/analysis/indo-pacific-economic-framework-and-digital-trade-southeast-asia> accessed 29 April 2025.

sustained investment in infrastructure, can generate measurable gains in competitiveness and cross-border connectivity. Yet these successes remain unevenly distributed. Many economies in the region continue to face structural and regulatory constraints that limit the broader diffusion of digital trade and investment. This section examines how regional cooperation could reduce these disparities. It considers the legal and policy tools available to improve coordination, identifies gaps in infrastructure investment that constrain integration, and explores the role of interoperability as an alternative to formal legal harmonization. These developments matter not only for the region's internal cohesion, but also for its capacity to influence the future direction of the global digital economy.

4.1 *Functional Convergence Over Normative Uniformity*

The digital economy plays a central role in driving economic growth across the Indo-Pacific. The question arises as to the optimal level of coordination and collaboration within the Indo-Pacific as well as between the Indo-Pacific – and its nations – and other regions – and nations – outside the region. Consistent regulatory standards reduce legal barriers, streamline compliance, enhance regulatory predictability, and foster a climate conducive to both investment and innovation. Efforts to establish consistent regulations must prioritize the key areas identified above: data protection, cybersecurity, IP and taxation laws. Both economic and geopolitical factors suggest that, in the Indo-Pacific, coordination should primarily occur within the region and amongst its nations.

By drawing on the strengths and expertise of various countries, cooperative efforts can accelerate technological progress, enhance regulatory frameworks, and ensure inclusive growth. Such cooperation facilitates the exchange of knowledge, enabling nations to benefit from each other's experiences in implementing digital policies, developing infrastructure, and nurturing innovation ecosystems that are key to digital economic development. For instance, advanced economies like Japan and South Korea, with their technological expertise, can offer valuable insights into building robust digital infrastructure and promoting digital literacy. Meanwhile, emerging markets, such as India and Indonesia, provide important lessons on scaling digital services and promoting widespread adoption. Knowledge exchange will allow countries to avoid common mistakes, adopt effective strategies, and accelerate their digital transformation processes. A major advantage of regional collaboration lies in its potential to enhance innovation. Collaborative research and development efforts can pool resources and expertise from multiple nations, driving advancements in cutting-edge technologies.

Geopolitical dynamics are playing an increasingly pivotal role in shaping the expansion and integration of the digital economy in the Indo-Pacific. Trade disagreements, territorial disputes, and divergent political ideologies present substantial obstacles to collaboration, often being responsible for the fragmentation within the digital sector. This fragmentation typically manifests through countries aligning with differing technological standards and ecosystems, which obstruct the seamless exchange of data, capital, and digital services.[131] Consequently, regional cooperation is not merely advantageous but essential in mitigating the disruptive effects of these geopolitical challenges. The relationship between the digital economy and geopolitics underscores the importance of strategic initiatives aimed at conflict resolution and regulatory coordination. Regional organizations, such as APEC and ASEAN, play a crucial role in facilitating dialogue, fostering trust, and developing mechanisms to address conflicts. In this context, regional collaboration extends beyond mere economic integration, aiding in the development of a resilient digital ecosystem capable of enduring external pressures. Enhancing collective efforts, particularly in data protection, cybersecurity, IP, and tax, as well as digital trade facilitation, can enable the Indo-Pacific region to address geopolitical complexities while advancing a more unified and competitive digital economy.

In this direction, ERIA's Digital Innovation and Sustainable Economy Centre (DISC) has been established to promote digital transformation across ASEAN and East Asian nations.[132] It seeks to modernize traditional business models by offering technical support for digital trade, developing harmonized rules on digital governance and cybersecurity, and fostering innovation among start-ups. Through these efforts, DISC aims to bring together talent in technology, innovation, and sustainability, supporting digital development in the region.

Along the same lines, the DEFA offers a critical opportunity to formulate region-specific regulations for digital economy governance and broader digital transformation. This is to be achieved through agreements on areas, such as digital trade, CBDFs, competition, and digital payments. DEFA is projected to contribute up to USD two trillion to the regional digital economy by 2030, thereby enhancing the region's competitiveness in the global market.[133]

131 See generally Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (OUP 2023).

132 ERIA, 'Centre for Digital Innovation and Sustainable Economy – The Latest News and Updates from ERIA' <https://www.eria.org/news-and-views/category/all/centre-for-digital-innovation-and-sustainable-economy> accessed 29 April 2025.

133 ASEAN, 'Digital Economy Framework Agreement (DEFA): ASEAN to Leap Forward Its Digital Economy and Unlock US$2 Tn by 2030' (19 August 2023) <https://asean

The current preference for regional partnerships suggests that lighter forms of cooperation, whether sector-specific or through plurilateral deals, may offer a more workable path. One example is the APEC CBPR system. It helps countries align their data protection practices in a way that supports cross-border data flows and builds commercial trust, without requiring identical standards. Digital Economy Agreements such as DEPA follow a similar approach. They allow participants to engage in selected areas of cooperation, based on their own priorities and readiness. While Indo-Pacific economies are building regionally grounded frameworks, their legal autonomy remains conditioned by wider geopolitical dependencies; particularly *vis-à-vis* the United States and China. The Indo-Pacific cannot be fully understood as a self-contained regulatory regime; its evolution reflects broader contestation in the global digital order.

At the same time, legal interventions in the digital economy are not universally beneficial. Regulatory efforts, if poorly calibrated, risk entrenching exclusion, undermining innovation, or reinforcing existing geopolitical and economic asymmetries. There is a growing recognition that law can channel digital development along suboptimal paths, creating barriers rather than bridges. As Indo-Pacific states experiment with governance models, sustained attention to the unintended consequences of legal design will be critical to ensuring that regulatory frameworks advance inclusive and sustainable digital growth.

4.2 *Building Legal Capacity Through Investment and Connectivity*

Creating a digital infrastructure is very important in order to enhance digital connectivity and promote broader participation in the digital economy. Investment in digital infrastructure is critical to integrating into the global digital economy as well as tackling the ongoing and emerging digital divide – both within and across nations. For instance, approximately one-third of the total world population does not have access to the Internet – primarily in low-income and rural areas.[134] To address this, targeted investments are

.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/> accessed 29 April 2025.

134 See International Telecommunication Union Press Release, 'Population of Global Offline Continues Steady Decline to 2.6 Billion People in 2023' (12 September 2023) <https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx>; see also ITU, 'Statistics' <https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx>; Simon Kemp, 'Internet Use in 2024' (*DataReportal*, 31 January 2024) <https://datareportal.com/reports/digital-2024-deep-dive-the-state-of-internet-adoption> all accessed 29 April 2025.

required, especially in underserved regions where connectivity is limited or unstable. International efforts, such as the World Economic *Forum's Internet for All* initiative, underscore the need for financial and technical assistance to develop resilient digital infrastructure in emerging countries.[135] Furthermore, integrating SMEs into the digital economy is crucial for fostering inclusive growth. SMEs, which represent 90% of businesses globally, are important drivers of innovation and economic progress.[136] Nevertheless, many encounter significant challenges in adopting digital technologies, particularly in emerging regions.[137]

While digital intra-region integration is relatively advanced compared to other regions – with the exception of Europe, digital infrastructure investment in the Indo-Pacific is essential for further fostering economic growth, reducing inequalities, and eventually supporting digital transformation.[138] The investment gap could potentially be covered through public-private partnerships (PPPs), which are less advanced compared to other regions. PPPs could help bridge divides and boost connectivity across nations, ultimately enabling economic resilience and inclusivity in the digital economy. Examples, such as Made in China 2025 and the Digital India initiative, which aim at integrating PPPs to enhance domestic development of digital technologies, offer insights into how such collaborations can accelerate the development of and investment in digital infrastructure.

Addressing regulatory, legal, and policy issues is essential for creating a supportive environment for digital infrastructure development. Many countries are developing infrastructure laws focused on supporting the creation,

135 World Economic Forum, 'Internet for All: A Project of The World Economic Forum's Digital Economy and Society System' (2017) <https://www3.weforum.org/docs/WEF_Internet_for_All_4_pager.pdf>; see also Heather Johnson, 'About 2.5 Billion People Lack Internet Access: How Connectivity Can Unlock Their Potential' (World Economic Forum, 25 September 2024) <https://www.weforum.org/agenda/2024/09/2-5-billion-people-lack-internet-access-how-connectivity-can-unlock-their-potential/> both accessed 29 April 2025.

136 See eg Jane Fraser, 'Why Supporting SMEs is Critical for Global Trade Stability and a More Inclusive Economy' (World Economic Forum, 16 January 2023) <https://www.weforum.org/agenda/2023/01/why-supporting-smes-is-critical-for-a-global-trade-stability-and-and-a-more-inclusive-economy/> accessed 29 April 2025.

137 Policies, such as those implemented under the European Union's Digital Single Market strategy, provide a framework for reducing these barriers, offering subsidies and incentives to facilitate SMEs' adoption of digital technologies and participation in e-commerce; see EU4Digital, 'EU Digital Strategy' <https://eufordigital.eu/discover-eu/eu-digital-strategy/> accessed 29 April 2025.

138 Asian Development Bank (n 5) 206 ff.

regulation, and management of both existing and new infrastructure. Good examples from the Indo-Pacific are Australia[139] and the Philippines.[140] There are many more examples from the broader region.[141] Policies that incentivize investments in digital infrastructure are integral to a comprehensive strategy of digital transformation in the Indo-Pacific. Tax relief for broadband investments (as in the United States), and regulations on spectrum allocation for 5G deployment (as in the EU), provide good examples. Ensuring cybersecurity and mitigating associated risks, as seen in the coordinated global efforts of the Cybersecurity Tech Accord,[142] also plays a crucial role in facilitating the secure development of digital infrastructure.

4.3 *Interoperability as a Governing Principle*

According to the World Economic Forum, when regulation and oversight vary across jurisdictions, the cost of doing business in digital sectors can rise by as much as 30 percent.[143] This is especially true for areas like fintech and e-commerce, where cross-border data flows are essential. Regulatory consistency makes it easier for companies to move into new markets. It helps drive economic growth and lowers the risks that come with navigating different rules. There are several ways to deal with this kind of regulatory fragmentation.

139 *Infrastructure Australia Act 2008* (Cth); see also Infrastructure Australia, 'What We Do' <https://www.infrastructureaustralia.gov.au/what-we-do> accessed 29 April 2025.

140 An Act Facilitating the Acquisition of Right-of-Way Site or Location for National Government Infrastructure Projects 2015 (PHL).

141 Nagesh Kumar (ed), *International Infrastructure Development in East Asia – Towards Balanced Regional Development and Integration* (ERIA 2008) <https://www.eria.org/publications/international-infrastructure-development-in-east-asia---towards-balanced-regional-development-and-integration--> accessed 29 April 2025.

142 The Cybersecurity Tech Accord brings together more than 150 technology companies committed to improving the security of digital infrastructure worldwide. The group supports practices like coordinated vulnerability disclosure and protection of ICT supply chains, which help members share threat information and strengthen defences against both criminal groups and state-backed attackers. Recent efforts by the Accord include working with international bodies and pushing for broader agreement on cybersecurity rules. These actions reflect a growing recognition that cooperative strategies are essential in dealing with increasingly complex cyber threats; see Cybersecurity Tech Accord, 'Cybersecurity Tech Accord: Year 6 Report' (2023) <https://cybertechaccord.org/uploads/prod/Cybersecurity-Tech-Accord-Year-Six-Report.pdf>; see generally Cybersecurity Tech Accord, 'Cybersecurity Tech Accord' <https://cybertechaccord.org/accord/> both accessed 29 April 2025; Kaja Ciglic and John Hering, 'A Multi-Stakeholder Foundation for Peace in Cyberspace' (2021) 6 Journal of Cyber Policy 360.

143 Emina Ajvazoska and others, 'The Future of Global Fintech: Towards Resilient and Inclusive Growth' (World Economic Forum, 18 January 2024) 14 <https://www3.weforum.org/docs/WEF_The_Future_of_Global_Fintech_2024.pdf> accessed 29 April 2025.

A conventional legal view might point to harmonisation through international law. But instead of aiming for full alignment, a more practical route could involve improving the ability of digital systems to work with one another. This kind of interoperability may offer a clearer path to stable and predictable conditions for digital trade and investment.

Regional agreements, such as RCEP,[144] may prove instrumental not only in achieving regulatory convergence but also in achieving system interoperability. As mentioned, the APEC CBPR system exemplifies such initiatives by providing a mechanism for the mutual recognition of data protection standards across APEC economies. Through its standardized approach to privacy regulations, the CBPR system facilitates the smoother transfer of data across borders while maintaining compliance with local requirements. This approach builds trust and alleviates the challenges posed by the multiplicity of privacy laws. For instance, Japan, an early participant in the CBPR system, has successfully aligned its domestic privacy standards with international frameworks, including the EU-Japan Adequacy Agreement, thus enabling more seamless data exchanges with both APEC and non-APEC economies.[145] The ASEAN Framework on Digital Data Governance is another regional initiative that aims to create interoperability across digital policies in Southeast Asia, improving transparency and legal certainty for businesses.[146]

Achieving interoperability and interconnectivity within the Indo-Pacific digital economy necessitates an expansive legal approach that surpasses current frameworks. The objectives of the region could be pursued through regional treaties or agreements aimed at developing mutual recognition frameworks governing data protection – such as the ones mentioned in the previous paragraph, cybersecurity, digital IP, taxation, as well as more broadly

144 Zhai (n 3).

145 The Brookings Institution highlights that the CBPR system has substantially reduced compliance costs for businesses operating in multiple APEC jurisdictions, thereby enhancing digital trade. Joshua P Meltzer, 'The Importance of the Internet and Transatlantic Data Flows for US and EU Trade and Investment' (2014) Brookings Institute Global Economy & Development Working Paper 79 <https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf> accessed 29 April 2025.

146 According to McKinsey & Company, the alignment of digital regulations in Southeast Asia could raise the region's GDP by up to USD 1 trillion by 2030, driven by the growth of digital trade. Oliver Tonby and others, 'Southeast Asia at the Crossroads: Three Paths to Prosperity' (McKinsey & Company, November 2014) <https://www.mckinsey.com/~/media/mckinsey/featured%20insights/asia%20pacific/three%20paths%20to%20sustained%20economic%20growth%20in%20southeast%20asia/southeast_asia_at_the_crossroads_three_paths_to_prosperity_full%20report.pdf> accessed 29 April 2025.

electronic transactions. The adoption of the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce could enable cross-border recognition of electronic contracts and signatures.[147] Mutual recognition agreements may further support this objective by facilitating the acceptance of each nation's regulatory standards, thereby minimizing legal obstacles to trade. Further institutional initiatives should also encompass the formation of joint regulatory entities tasked with monitoring compliance and resolving disputes, thus enhancing legal clarity for businesses operating on a regional scale.

A proactive approach to the formulation of legal instruments that address the specific requirements of digital interoperability and mutual recognition would enable the Indo-Pacific to construct a robust and cohesive digital economy, prepared to accommodate future technological advancements.

5 Conclusion – and Outline of the Special Issue

The Indo-Pacific is an active site of digital experimentation, offering important (though unevenly realized) opportunities to rethink how law can govern and enable digitalization. This transformation is not just a matter of revising old rules. It requires law to work as a forward-planning tool; i.e. one that can respond to ongoing technological changes while managing cross-border economic activity. In this region, law must serve three roles at once: provide legal certainty, enable cooperation, and support new rule-making that takes into account both domestic conditions and regional commitments. However, the capacity of law to guide digital transformation also entails risks. Law can constrain innovation, entrench inequality, or amplify geopolitical divisions if poorly designed or applied without regard to evolving technological and economic conditions. As a stabilizer, it builds trust by ensuring the integrity of data protection with CBDFs, cybersecurity, IP, taxation as well as dispute prevention. As a facilitator, it unlocks the region's economic potential by supporting digital trade, attracting investment, and ensuring fair access to technology. Finally, as a norm creator, it positions the Indo-Pacific as a leader in crafting the global rules for digitalization, balancing the imperatives of sovereignty, interdependence, and inclusivity. This vision is anchored in recognizing law as the foundation for resilience and equity.

147 UNCITRAL Model Law on Electronic Commerce (adopted 16 December 1996) (1997) 36 ILM 199.

This Special Issue builds on the analytical architecture developed in this framing article, which positions the Indo-Pacific as a testbed for new approaches to digital economic governance. It advances a shared thesis: the region's legal experimentation is progressively redefining the parameters of international economic law, not through formal multilateralism, but through incremental, modular, and often institutionally hybrid arrangements. Collectively, the contributions examine how Indo-Pacific states are responding to a fragmented legal environment, using strategies of coordination, infrastructure-building, and regulatory interoperability to manage digital trade, data flows, artificial intelligence, IoT and other strategic technologies. Each article extends a core insight of this special issue: that legal capacity in the digital economy does not derive exclusively from formal authority, but also from technical know-how, institutional credibility, and sustained cross-border collaboration.

The article by Anita Prakash, Lurong Chen, and Rashesh Shrestha, titled **"Policy and Economic Imperatives for Participation in and Expansion of the Digital Economy in the Indo-Pacific,"** provides a foundational mapping of the regulatory, economic, and infrastructural conditions required for inclusive digital participation across the region. Through detailed attention to digital public infrastructure, skills development, and investment readiness, the authors present a policy-oriented agenda for integrating Indo-Pacific economies – particularly emerging markets – into global digital value chains. This article establishes the baseline institutional and economic considerations that later contributions build upon.

Tomohiko Kobayashi's article on the **"Role of G7 and G20 for Ensuring Resilient, Trustworthy and Supply Chains for the Digital Economy in the Indo-Pacific"** addresses supply chain coordination and institutional design in the absence of cohesive regional governance. Focusing on Japan's semiconductor strategy, it evaluates how multilateral forums like the G7 and G20 can provide regulatory scaffolding for supply chain resilience, especially when national policies diverge or geopolitical instability limits harmonization. This contribution connects global policy fora to regional legal experimentation, reinforcing the special issue's emphasis on plurilateral and informal institutions as governance alternatives.

In **"Digital Economy Innovation in the Indo-Pacific: Towards a 'Singapore Effect'?,"** Jason Grant Allen and Qiu Xu Martin Liao explore the diffusion of digital economy agreements (DEAs) as tools of regulatory alignment and legal interoperability. The article introduces the concept of the 'Singapore Effect' to describe a model of regulatory entrepreneurship that does not rely on market size but on credibility, institutional agility, and legal pragmatism. Their analysis speaks to a central concern of the special issue: the capacity of middle

powers to influence the digital economy using flexible instruments that function across divergent legal regimes, without relying on formal convergence or binding alignment.

Rostam Neuwirth's article, **"Artificial Intelligence and Related Technologies in the Digital Economy: Multilateral and Regional Legal Challenges from the Perspective of the Indo-Pacific,"** examines the limits of current institutional structures in managing the regulatory demands of artificial intelligence and its associated technologies. The article critiques the fragmented character of global AI governance and argues that the Indo-Pacific could contribute to a more coherent approach, provided that existing institutional silos are overcome. Its core intervention aligns with this special issue's broader claim: that institutional coordination, rather than rule proliferation, is emerging as the key legal currency in the digital economy.

The article by Han-Wei Liu and Ching-Fu Lin titled **"Techno-Geopolitics and Semiconductor Chokepoints: Beyond the US-China WTO Dispute"** focuses on Taiwan and other 'chokepoint economies' whose export control policies and legal autonomy are central to global digital supply chains. The article interrogates how extraterritorial regulatory practices by major powers interact with the fragmented authority of smaller but strategically essential economies. In doing so, it illustrates the strain placed on the WTO-centered trading system and showcases how geopolitical imperatives are restructuring the legal governance of semiconductors and other foundational technologies.

Taken together, these articles show how Indo-Pacific states are developing cooperation approaches that rely less on grand institutional architecture and more on targeted functional mechanisms. Each contribution builds on the central thesis that regional legal innovation (anchored in interoperability, infrastructure, and coordination) is beginning to supply the organizing logic of a post-multilateral order. The Indo-Pacific, in this respect, is not merely adapting to global digital transformation but actively contributing to the redesign of international economic governance. Yet this contribution unfolds in a volatile geopolitical environment. The Trump administration's assertive trade and investment restrictions, coupled with efforts to reconfigure supply chains away from China, introduce exogenous pressures that could fragment Indo-Pacific legal initiatives or force them into defensive, reactive postures.

This collective work began in 2022 with the support of ERIA, culminating in two key events: an online workshop on 18 October 2024, and a conference in November of the same year at Leiden University. The authors and all contributors to this special issue extend their sincere thanks to ERIA for its generous support and to the participants, many of whom provided insightful feedback that significantly enhanced these articles before submission to

the Journal of World Investment & Trade (JWIT). Appreciation is also due to JWIT for its excellent editorial assistance throughout the peer review and publication process.

The Indo-Pacific's digital transformation confirms a central proposition: law can no longer function merely as a reactive instrument. It must anticipate technological developments and provide legal structures capable of managing their economic and institutional consequences. This requires the domestic and international legal order to evolve beyond static rule-making, relying on instruments capable of responding to emerging developments while preserving coherence and enforceability. In a region marked by regulatory diversity, uneven institutional capacity, and heightened interdependence, law operates as the principal mechanism linking innovation with governance, and mediating between sovereign discretion and transnational coordination. The core function of international economic law is not to impose uniformity. Rather, its purpose is to design instruments that facilitate cooperation across jurisdictions, accommodate rapid technological change, and embed principles of equity and predictability. This special issue affirms that the legal design of the digital economy is no less consequential than its technical architecture.

Biographical Note

Julien Chaisse, Professor, School of Law, City University of Hong Kong (Hong Kong SAR) julien.chaisse@cityu.edu.hk; **Georgios Dimitropoulos**, Professor, Hamad Bin Khalifa University (Qatar) gdimitropoulos@hbku.edu.qa; **Irma Mosquera**, Professor, Leiden University (Netherlands) i.j.mosquera.valderrama@law.leidenuniv.nl.

Acknowledgements

The authors are grateful to ERIA for its support and to the workshop and conference participants, many of whom provided feedback that strengthened the contributions prior to submission to the *Journal of World Investment & Trade*. The authors also thank the three anonymous peer reviewers for their detailed and constructive suggestions, Amna Zaman for outstanding research assistance, and the *JWIT* editorial team for its support throughout the review and publication process.