

The Digital Productivity Foundation of Cross-Border Data Flow Policies in RCEP Member Countries and Their Impacts: A Postprint Referencing the Digital Convergence Index

Authors: Huang Gui, Tao Ru

Date: 2023-08-23T00:00:00+00:00

Abstract

The article systematically reviews the recent legislation and policies of Regional Comprehensive Economic Partnership (RCEP) member states concerning cross-border data flows, categorizing them according to data transmission prohibition, data localization, licensing systems, standard-based regimes, and other circumstances. With reference to the pillar indices and their standardized evaluation metrics from the ASEAN Digital Integration Index report, it examines the subject and object elements of digital productivity and the current state of the digital economy among RCEP member states. The article introduces data value chain theory to elaborate on the decisive influence of subject elements of digital productivity on cross-border data flow policy formulation; cites data discourse power theory to explain that object elements constitute the foundation of policy formulation; and based on “data colonialism” theory, explains the non-linear relationship between the digital economy and the “degree of freedom” in policies. Finally, the article proposes recommendations for promoting the free flow of cross-border data among RCEP member states.

Full Text

On the Digital Productivity Base of Policies for Cross-Border Data Flows Between RCEP Parties and Its Influences—Taking the Digital Integration Index as a Reference

HUANG Gui^{1,2*}, TAO Ru¹

¹ Law School, Yunnan University, Kunming 650500, China

² Faculty of Law, University of Fribourg, Fribourg CH1700, Switzerland

Abstract

This study reviews the newest legislation and policies of Regional Comprehensive Economic Partnership (RCEP) participating countries on cross-border data flows, categorizing them according to prohibitions on data transfer, local data storage requirements, permission-based systems, standards-based systems, and other circumstances. Using the pillar indexes and standardized evaluation indicators from the *ASEAN Digital Integration Index* report as a reference, the subject and object elements of digital productivity in RCEP parties are systematically analyzed alongside the current state of their digital economies. By introducing data value chain theory, this article expounds on the decisive influence of digital productivity's subject elements on policy formulation for cross-border data flows. It invokes data discourse power theory to explain how object elements constitute the foundation of policy making, and employs "data colonization" theory to elucidate the non-linear relationship between digital economy development and policy "freedom." Finally, the article proposes recommendations for promoting free cross-border data flows among RCEP parties.

Keywords: RCEP, cross-border data flows, digital productivity, digital economy

In the process of the Fourth Industrial Revolution, data has emerged as the fifth crucial element transcending traditional cross-border trade, following goods, labor, services, and capital [1]. Cross-border data flow policies serve as essential tools for countries to protect their national data interests [2]. Against the backdrop of the World Trade Organization (WTO) lacking systematic rules to coordinate national governance of cross-border data flows [1], regional economic and trade agreements have become critical arenas for balancing divergent national positions on cross-border data governance. On June 2, 2023, as the Regional Comprehensive Economic Partnership (RCEP) formally entered into force for the Philippines, RCEP achieved comprehensive implementation across all ten Association of Southeast Asian Nations (ASEAN) members and five non-ASEAN countries¹. The activation of RCEP's cross-border data provisions represents a negotiated compromise among developed, developing, and least-developed countries in the Asia-Pacific region regarding complex data governance positions². Using the relevant pillar indexes and standardized evaluation indicators from the *ASEAN Digital Integration Index* report released in August 2021 as a reference framework, this study examines the digital productivity and digital economy status of RCEP parties, and subsequently analyzes how digital productivity influences cross-border data flow policy formulation. Finally, it proposes recommendations for advancing free cross-border data flows among RCEP parties.

1. Policy Review of Cross-Border Data Flows in RCEP Countries

Kapland et al. [4] researched and summarized types of cross-border data flow policies, identifying four categories ranked by degree of policy freedom: prohibition of data transfer, local data storage, permission-based systems, and standards-based systems. Since Cambodia, Brunei, and Myanmar have not yet enacted specific laws or policies on cross-border data flows, a fifth category—“other circumstances”—is added.

(1) Prohibition of Data Transfer: This category prohibits the cross-border transfer of data and its copies. For example, South Korea prohibits the cross-border transfer of medical and health data [5]; Indonesia’s Regulation No. 71 of 2019 forbids cross-border data transfers by public sector entities [6]; and Australia’s *Personally Controlled Electronic Health Records Act 2012* prohibits the cross-border transfer of personal medical health records [7].

(2) Local Data Storage: This approach permits cross-border transfer of data copies while requiring that copies be stored within national territory. New Zealand’s *Tax Administration Act 1994* and *Goods and Services Tax Act 1985* require business information and goods information to be stored domestically via paper or data storage devices [8,9]. Vietnam’s 2018 *Cybersecurity Law* (Article 26, Clause 3) mandates that network service providers store data within the country [10]. Thailand’s *Personal Data Protection Act 2019* (Article 27, Clause 3) stipulates that relevant data information not requiring data subject consent must be stored domestically during cross-border transfers [11].

(3) Permission-Based System: This requires obtaining permission from data subjects or relevant authorities for cross-border data transfers. South Korea’s *Personal Information Protection Act* (Article 17, Clauses 3 and 4) establishes a permission system with exceptions [12], while its *Regulation on Data Processing by Financial Institutions and Authorization for Other Businesses* (Article 4) creates an authorization-based permission system [13]. Indonesia’s *Ministerial Regulation on Personal Data Protection in Electronic Systems* (Article 22, Clause 1) establishes a permission system [14]. Japan’s amended *Act on the Protection of Personal Information 2021* (Article 27, Clause 1) requires data subject consent for personal data cross-border transfers [15]. Thailand’s *Personal Data Protection Act 2019* (Article 28, Clause 1) clarifies three exception scenarios to establish a permission system [11]. Laos’ *Electronic Data Protection Law* also establishes a permission system³. The Philippines’ *Data Privacy Act 2012* (Article 12, Item a) requires obtaining data subject authorization or consent as a prerequisite for cross-border data transfers [16]. Australia’s *Privacy Act 1988* “Privacy Principles” (Article 8, Clause 2, Items b-e) specifies four permission scenarios [17]. Malaysia’s *Personal Data Protection Act 2010* (Article 129, Clause 3) establishes a permission system through exception clauses [18].

(4) Standards-Based System: This requires meeting national security standards for data security before cross-border transfer is permitted. Singapore’s

Personal Data Protection Act 2012 (Article 26) establishes a standards-based system for cross-border data transfers [19], with detailed provisions in Articles 9 and 10 of its *Personal Data Protection Regulations 2021* [20]. Japan's *Act on the Protection of Personal Information* (Article 28) specifies three types of standards-based cross-border data transfer mechanisms: the recipient jurisdiction must guarantee equivalent protection levels to Japan, comply with Japanese legal provisions, or conform to relevant international standards for cross-border data transfers [15]. Australia's *Privacy Act 1988* "Privacy Principles" (Article 8, Clause 2, Item a) establishes a standards-based system requiring protection levels similar to Australia's own [17]. New Zealand's *Privacy Act 2020* (Article 193, Clause 1) establishes an authorization-based standards system [21]. Thailand's *Personal Data Protection Act 2019* (Article 28, Clause 1) provides for a generally applicable standards-based system [11], and has compiled a list of countries with inadequate personal data protection levels [22]. Malaysia's *Personal Data Protection Act 2010* (Articles 129, Clauses 1 and 2) requires cross-border data transfers to have protection levels recognized as equivalent by the Malaysian government [18]. The Philippines' *Data Privacy Act 2012* (Article 21, Item a) adopts a standards-based system through contracts or other mechanisms providing equivalent protection [16].

(5) Other Circumstances: Cambodia has not enacted dedicated data protection legislation, with rules on cross-border data flows scattered throughout its *E-Commerce Law* passed in November 20194. Brunei and Myanmar have not yet established regulations on cross-border data transfers [22].

RCEP parties' data flow policies are not absolute; neither absolutely prohibiting nor absolutely permitting free cross-border data flows exist. Instead, each country establishes different control standards and procedures according to its own digital productivity level. Restricting free cross-border data flows is not an end in itself, but rather a means to protect the value generated by cross-border data flows.

2. Digital Productivity of RCEP Parties Based on the Digital Integration Index

Digital productivity represents the digital integration of the subject elements (workers) and object elements (means of production and objects of labor) of productivity [23]. This study selects the five pillar indexes and their standardized evaluation indicators from the *ASEAN Digital Integration Index* report—digital technology and talent, data protection and cybersecurity, digital payments and identity, institutional and infrastructure readiness, and digital trade and logistics—to reflect and analyze digital productivity and its application and transformation capabilities from the perspectives of subject and object elements.

(1) Subject Elements of Digital Productivity Determine Development Levels. The subject elements of digital productivity consist of workers who, through education and training, possess digital technology literacy and applica-

tion skills [23]. Their status can be reflected through the “digital technology and talent” and “data protection and cybersecurity” pillar indexes and their standardized evaluation indicators. First, the “digital technology and talent” pillar serves as an important reflection of labor force conditions. Compared with other pillar indexes, RCEP parties exhibit their lowest average in this pillar at only 49.19. Among its standardized evaluation indicators, the proportion of graduates in science, technology, engineering, and mathematics fields registers a mere 5.82, the proportion of knowledge-intensive service workers stands at only 4.48, while the proportion of individuals with digital skills reaches 13.11, the proportion of people engaged in digital technology-related businesses is 12.67, and the indicator for digital technology research and development cooperation is 12.13. Based on these figures, RCEP parties have a limited digital workforce, and their digital technology literacy, application, and transformation capabilities require further enhancement. Second, the “data protection and cybersecurity” pillar reflects digital technology literacy and application capacity from another perspective. Overall, RCEP parties perform well on this pillar with an average index of 70.65, though substantial room for improvement remains. Among its standardized evaluation indicators, cybersecurity technical capabilities (10.96), institutional cybersecurity capacity (12.96), and national cooperation on cybersecurity (11.88) require strengthening. Specific RCEP parties such as Laos (32.58), Cambodia (24.76), and Myanmar (20.41) demonstrate unsatisfactory performance on this pillar and need to enhance data and cybersecurity construction across multiple dimensions.

(2) Object Elements of Digital Productivity Form the Important Foundation for Development. Digital productivity’s object elements comprise digitalized means of production and objects of labor. Means of production manifest as digital technology equipment and tools, while objects of labor appear as data, commercial software, and natural materials upon which production acts [23]. The “digital payments and identity” and “institutional and infrastructure readiness” pillar indexes and their standardized evaluation indicators reflect these object elements. First, the “digital payments and identity” pillar represents an important manifestation of means of production. Regarding this pillar index, the RCEP parties’ average (67.21) exceeds the ASEAN index value (58.84), primarily because some non-ASEAN developed countries show relatively high values: New Zealand (90.33), Australia (88.00), Japan (82.00), and South Korea (81.42). This demonstrates that these developed countries possess relatively superior object elements of productivity. Examining the pillar’s standardized evaluation indicators, most countries show relatively high configuration rates for identity recognition systems and 普及率 (popularization rates) for identity systems at 14.76 and 14.48 respectively. However, the standardized evaluation indicator for the proportion of people using digital payment methods or digital devices is very low at only 2.64, while for other financial transactions this indicator is merely 7.6. Second, the “institutional and infrastructure readiness” pillar reflects the status of objects of labor. ASEAN’s index value for this pillar is 62.85, with the proportion of active mobile broadband users (14.76)

being the highest among standardized evaluation indicators, the proportion of IoT users (11.59) the lowest, and the standardized evaluation indicator for government digital service availability and usability at 12.44. The RCEP parties' average is slightly lower than ASEAN's at 61.67. Country-specific performance varies significantly, with Singapore showing the highest pillar index (90.36) and Laos the lowest (38.27). This indicates that most RCEP parties exhibit unbalanced development in the means of production and objects of labor for digital productivity. On one hand, means of production are somewhat deficient with substantial room for improvement; on the other hand, the volume of data and its related elements as objects of labor is relatively large, constituting important data resources.

(3) Digital Economy as an Important Manifestation of Digital Productivity Application and Transformation. The digital economy represents activities or economic forms where productivity subjects organically integrate digital technology with productivity elements to create value in digital products and other goods [23]. Digital economy development levels can be reflected through the “digital trade and logistics” pillar index and its standardized evaluation indicators. The RCEP parties' average on this pillar is 66.97, with non-ASEAN developed countries such as Japan, New Zealand, and Australia all exceeding 90, followed by South Korea, China, Thailand, and Singapore, all surpassing 80—far exceeding the ASEAN index value (55.27). By contrast, Laos (23.22), Cambodia (33.91), and Myanmar (18.51) show lower pillar indexes. Examining standardized evaluation indicators, the indicator for digital technology adoption in cross-border trade and government customs is slightly low at 11.20, while indicators for digital authentication and electronic signature usage (12.00) and logistics service competitiveness and quality (12.07) are somewhat higher. Overall, the gap in digital productivity application and transformation capabilities between developed and least-developed countries is substantial, even showing polarization.

3. Impact of Digital Productivity on RCEP Parties' Cross-Border Data Flow Policies

3.1 Decisive Influence of Digital Productivity's Subject Elements

Digital productivity's subject elements play a decisive role in determining policy scale and implementation methods. Subject elements constitute the core of data sources and value formation. Data sources and their value jointly determine a country's position in the global data value chain. The data value chain is crucial for estimating data value, representing the process through which raw data is collected, analyzed, and processed into digital intelligence that can be used for commercial purposes with economic value or serve social objectives with social value potential. Creating and capturing value requires both raw data and the capability to transform data into digital intelligence. In essence, the data value chain represents a new form of digital divide resulting from data becoming a re-

source and the value effects created by its cross-border flows. In this new digital divide, global digital enterprises based in developed countries gather top talent and control core technologies for data value transformation, placing developed countries at the apex of the data value chain and enabling them to lead digital intelligence development. In contrast, developing and least-developed countries, while possessing the vast majority of raw data, lack core digital technologies and thus can only serve as raw data providers and consumers of digital intelligence products, placing them in subordinate positions within the data value chain [24]. Consequently, policymakers must acknowledge their position and its effects within the data value chain when formulating cross-border data flow policies, thereby making choices regarding policy scale and implementation methods. For instance, the United States hosts major global high-tech digital platform enterprises and talent, commands cutting-edge digital technologies, and dominates global digital intelligence products and services. Only by enabling its platform enterprises to obtain maximum raw data globally can the United States ensure the frontier nature and innovativeness of its digital intelligence products and maintain its position at the data value chain's apex, which explains its advocacy for liberal cross-border data flow policies [25]. Compared with the United States, although the European Union also possesses top high-tech enterprises and talent, it lacks digital platform enterprises capable of influencing global digital intelligence markets, meaning its mastery of global digital technologies and talent reserves is relatively weak, and its data value transformation capabilities are limited. Consequently, the EU inevitably becomes a raw data provider, resulting in relatively conservative cross-border data flow policies [24].

3.2 Object Elements as the Foundation of Policy Formulation

Digital productivity's object elements constitute both the foundation of productivity and the basis for policymakers to determine policy scale and implementation. Object elements include not only the data subject to policy adjustment but also the foundational tools ensuring policy implementation. The "digital payments and identity" pillar reflects the volume of "data" as an object of labor, demonstrating the current state of policy regulation objects, while the "institutional and infrastructure readiness" pillar reflects hard indicators of digital infrastructure as means of production. Data volume and digital technology infrastructure constitute the objective foundation for policy scale choices in cross-border data flows.

The policy logic based on object elements concerns how policymakers maintain their data discourse power. As previously discussed, most developing and least-developed countries serve as primary sources of raw data and major data exporters but occupy marginal or bottom positions in the data value chain [24]. Conversely, some developed countries are major data importers that utilize their digital technologies and massive data for innovation, creating high value-added data products and positioning themselves at the center or apex of the data value chain. Disparities in data value chain positions lead to unequal data dis-

course power. From policymakers' perspectives, unequal data discourse power will, on one hand, cause political discourse inequality that places international relations in passive positions, and on the other hand, create economic inequality that squeezes out or eliminates domestic enterprises. Consequently, many developing country policymakers view unequal data discourse power as legitimate justification for strategic intervention in cross-border data flows through policies or legislation [24]. Thus, most RCEP parties promote policy interventions on cross-border data flows by enacting legislation or policies to enhance national data governance and cybersecurity capabilities and advance institutional and infrastructure development. For example, in November 2020, Singapore amended its *Personal Data Protection Act 2012* and *Spam Control Act 2007* to fully protect consumer rights in the digital age and ensure capacity to keep pace with technological development and new business models, while balancing consumer demand for innovation with related rights protection and risk prevention [3]. As data exporters with massive raw data but lacking digital technology infrastructure and application capabilities, Cambodia, Laos, Myanmar, and Vietnam advocate that relevant cross-border data flows should not yet be subject to RCEP provisions.

3.3 Non-Linear Relationship with Digital Economy

From policymakers' perspectives, strong digital economy performance does not necessarily justify relaxed controls on cross-border data flows. The digital economy represents activities where productivity subjects integrate digital technology with productivity elements to create value. Data serves as an important object of labor in digital economic activities, making the digital economy fundamentally based on digital technology and data. While free cross-border data flows can promote digital technology innovation, development, and application, as well as drive digital economy growth, policymakers must ensure that digitalized production relations adapt to digital productivity development. Cross-border data flow policies must be built upon national productivity development levels to maximize the effectiveness of digital technology and data resources, rather than blindly pursuing digital economy development at the risk of becoming "data colonies." Therefore, digital economy development does not necessarily correlate positively with policy "freedom."

Specifically, the "digital trade and logistics" pillar index primarily examines digital technologies and supporting infrastructure available for cross-border trade [3]. Its standardized evaluation indicators constitute important foundations for digital economy development. Although RCEP parties demonstrate excellent performance on the "digital trade and logistics" pillar, their cross-border data flow policies are not necessarily liberal. For instance, Japan shows optimal performance on this pillar index but employs a "dual-track" system combining permission-based and standards-based regulations. New Zealand follows closely behind Japan but requires copies of business information, goods, and service records to be stored domestically, simultaneously implementing a "dual-track"

system of local storage and standards-based regulation. Australia’s policy is even more stringent, employing a “triple-track” system that prohibits data exports while parallel implementing permission-based and standards-based regulations.

In the digital economy, markets continue to follow self-reinforcing dynamics of “winner-take-all,” where only a few commercial entities capture the vast majority of benefits and power in their relationships with end-data owners [26]. Consequently, when balancing digital economy development against overall domestic interests, policymakers inevitably tend to avoid dependence on digital technology powerhouses like the United States⁵. India, though not an RCEP party, provides a typical example: to safeguard the development of its domestic digital technology capabilities, India adopts cross-border data flow policies that maximize its national data economic and social interests to promote domestic digital economy development while preventing data economic benefits from flowing to digitally advanced countries and regions. The philosophy underlying such policies is to prevent India from becoming a “data colony” of other economically developed nations—that is, to prevent developed countries from extracting benefits from India’s cross-border data flows and harming India’s national interests [26]. Therefore, India requires that data within its territory should be prioritized for use by domestic emerging enterprises and prevented from flowing to developed countries’ technology companies, thereby avoiding victimization by “data colonialism” [27].

4. Conclusions and Recommendations

4.1 Conclusions

Cross-border data flows are not entirely free and even exhibit de facto data protectionism, representing the outcome of digital productivity competition. The advocacy for free cross-border data flows possesses a certain degree of geopolitical and discursive characteristics, primarily emanating from developed countries’ theories, while arguments for restricting cross-border data flows mostly originate from competing nations seeking to maintain competitive advantages [28].

RCEP parties’ cross-border data flow policies can be classified into five types, with most employing “multi-track” parallel or overlapping systems, while some adopt “single-track” systems. Additionally, a few countries have yet to introduce policies or legislation on cross-border data flows.

Digital productivity elements significantly influence the scale and implementation methods of cross-border data flow policies. Subject elements play a decisive role in policy formulation because they concern the cognition, development, and application capabilities of digital technology, as well as the cognitive and implementation capacities for policy making, thereby determining policy scale and implementation approaches. These subject elements contribute to the “digital divide” between developed, developing, and least-developed countries. In con-

trast, object elements of digital productivity, comprising means of production and objects of labor, concern fundamental issues of data discourse power and constitute an important foundation for policy formulation. Although the digital economy falls outside the scope of digital productivity per se, it represents a crucial manifestation of productivity application and transformation. From a digital economy perspective, cross-border data flow policies must balance national digital economy development with various productivity elements, avoiding the pursuit of economic development at the cost of becoming “data colonies.”

4.2 Policy Recommendations

From the perspective of digital productivity, RCEP parties should undertake efforts in the following three areas to promote the free cross-border data flows advocated by RCEP:

(1) Strengthen Digital Talent Cultivation. Digital technology talent constitutes the core and key driver of cross-border data flows and represents the decisive factor in policy formulation and implementation. Therefore, RCEP parties should focus on cultivating and attracting digital talent, enhancing their knowledge literacy and application transformation capabilities to improve national competitiveness in digital human capital.

(2) Increase Investment in Data Infrastructure. RCEP parties should increase investment in digital technology infrastructure construction to enhance security guarantees for cross-border data flow infrastructure. Simultaneously, countries should construct comprehensive institutional guarantee systems for data security and cybersecurity, promoting the internationalization and standardization of institutional development.

(3) Advocate for Equal Data Rights. RCEP parties should advocate for equal data rights and strive to eliminate unequal factors in the data value chain.

References

1. Mitchell A D, Mishra N. Regulation cross-border data flows in a data-driven world: How WTO law can contribute. *Journal of International Economic Law*, 2019, 22(3): 389-415.
2. Hodson S. Applying WTO and FTA disciplines to data localization measures. *World Trade Review*, 2019, 18(4): 631-657.
3. United States Agency for International Development, United States-ASEAN Connect Digital Economy Series, Association of South-East Asian Nations. *ASEAN Digital Integration Index: Measuring Digital Integration to Inform Economic Policies*. Jakarta: Association of South-East Asian Nations, 2021.
4. Kaplan J M, Rowshankish K. Addressing the Impact of Data Location Regulation in Financial Services, Global Commission on Internet Gover-

- nance Paper Series No. 14. Waterloo: Centre for International Governance Innovation and Chatham House, 2015.
5. Raghavan A, Demircioglu M A, Tæihagh A. Public health innovation through cloud adoption: A comparative analysis of drivers and barriers in Japan, South Korea, and Singapore. *International Journal of Environmental Research and Public Health*, 2021, 18(1): 334-363.
 6. The Minister of Communication and Informatics of the Republic of Indonesia. *The Regulation of the Minister of Communications & Informatics of Indonesia Regarding the Protection of Personal Data in an Electronic System, No. 20 of 2016*. Jakarta: The Minister of Information and Informatics of the Republic of Indonesia, 2016.
 7. The Parliament of Australia. *Personally Controlled Electronic Health Records Act 2012*, No. 63. Canberra: The Parliament of Australia, 2012.
 8. The Parliamentary Counsel Office of New Zealand. *Tax Administration Act 1994*, Public Act 1994 No. 166. Wellington: The New Zealand Government, 2023.
 9. The Parliament of New Zealand. *Contract and Commercial Law Act 2017*, Public Act 2017 No. 5. Wellington: The New Zealand Government, 2017.
 10. The National Assembly. *The Cybersecurity Law*, Law No. 24/2018/QH14. Hanoi: The National Assembly, 2018.
 11. Personal Data Protection Act, B.E. 2562 (2019). Bangkok: The National Legislative Assembly, 2019.
 12. The National Assembly of the Republic of Korea. *Personal Information Protection Act*, Act No. 16930, 2020. Seoul: Korea Institute of Legal Studies, 2020.
 13. Chung C M. Data location: The causes, evolving international regimes and Korean practices. *Journal of World Trade*, 2018, 52(2): 187-208.
 14. The Minister of Communication and Informatics of the Republic of Indonesia. *The Regulation of the Minister of Communications & Informatics of Indonesia Regarding the Protection of Personal Data in an Electronic System, No. 20 of 2016*. Jakarta: The Minister of Information and Informatics of the Republic of Indonesia, 2016.
 15. The National Diet of Japan. *Act on the Protection of Personal Information*, Act No. 57 of May 30, 2003, Act No. 37 of 2020. Tokyo: The National Diet of Japan, 2020.
 16. Republic of the Philippines Congress of the Philippines Metro Manila Fifteenth Congress Second Regular Session. *Data Privacy Act of 2012*, Republic Act No. 10173. Metro Manila: Republic of the Philippines Congress, 2012.
 17. The Parliament of Australia. *Privacy Act 1988*, No. 119, 1988. Canberra: Federal Register of Legislation of Australian Government, 2021.
 18. The Parliament of Malaysia. *Personal Data Protection Act 2010*, Act 709. Kuala Lumpur: Federal Legislation of Malaysia, 2010.
 19. The Parliament of Republic of Singapore. *Personal Data Protection Act 2012*, Act 26 of 2012. Singapore: Singapore Government Agency, 2021.
 20. The Personal Data Protection Commission, the Minister for Communica-

- tions and Information of Republic of Singapore. *Personal Data Protection Regulation 2021*, No. S63. Singapore: Singapore Government Agency, 2021.
21. The Parliament of New Zealand. *Privacy Act 2020*, No. 31. Wellington: The New Zealand Government, 2020.
 22. Wong B. Data localization and ASEAN economic community. *Asian Journal of International Law*, 2020, 10(1): 158-180.
 23. He Y C, Wang W. The nature and application of digital productivity. *Academic Monthly*, 2021, 53(7): 55-66. (in Chinese)
 24. United Nations. *Digital Economic Report 2021: Cross-border Data Flows and Development: For Whom the Data Flow*. Geneva: United Nation, 2021.
 25. Weber S. Data, development, and growth. *Business and Politics*, 2017, 19(3): 397-423.
 26. Farrell H, Newman A L. Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 2019, 44(1): 42-79.
 27. Srinivas K R. India's emerging data protection regime and its possible impact on the digital economy and trade of India. *New Political Economy*, 2020, 25(5): 813-828.
 28. Dix A, Thüsing G, Traut J, et al. EU data protection reform: Opportunities and concerns. *Intereconomics*, 2013, 48: 268-276.

Notes

1 *Regional Comprehensive Economic Partnership (RCEP) Fully Enters into Force for 15 Signatory Countries* (2023-06-02) [2023-07-04]. http://fta.mofcom.gov.cn/article/rcep/rcepnews/202306/54022_1.html.

RCEP parties include ASEAN 10 countries: Brunei, Myanmar, Cambodia, Philippines, Indonesia, Singapore, Laos, Thailand, Malaysia, and Vietnam; and five non-ASEAN countries: Australia, China, Japan, South Korea, and New Zealand.

2 Digital trade: Is RCEP the WTO's future? (2020-11-23) [2023-01-26]. <https://www.cigionline.org/articles/digital-trade-rcep-wtos-future/>.

3 *Data Protection Laws of the World—Laos* (2022-12-28) [2023-07-17]. <https://www.dlapiperdataprotection.com/index.html?t=law&c=LA>.

4 *Cambodia Enacts a New E-Commerce Law and a Consumer Protection Law* (2019-11-14) [2023-07-21]. <https://www.tilleke.com/insights/cambodia-enacts-new-e-commerce-law-and-consumer-protection-law/>.

5 Is big tech setting Africa back? (2020-11-13) [2023-01-28]. <https://www.tbsnews.net/feature/panorama/big-tech-setting-africa-back-16864>.

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv — Machine translation. Verify with original.