UNSW SYDNEY

CIBEL Working Paper Series

Digital Industrial Policy through Data Security? – China's Approach and Security Exceptions under Trade Agreements

Xiaomeng Qu & Weihuan Zhou

[2025] CIBELWPS 7
Manuscript Date: 27 February 2025

UNSW SYDNEY | China International Business & Economic Law (CIBEL) Centre 法

About CIBEL

UNSW Law & Justice's China International Business and Economic Law (CIBEL) Centre is the world's largest centre outside China for the research and teaching of international business and economic law issues focusing on the impact of China domestically, in Asia Pacific and internationally. Established in 2015, CIBEL membership boasts the largest number of Chinese scholars of international business and economic law in any law school outside China, alongside pre-eminent Australian experts in CIBEL issues.

CIBEL research provides essential objective insights into China and its impact. China is Australia's largest trade partner and its influence on the country, within the region and internationally is growing. Current political difficulties do not change these facts. In fact, they make the study of China in the context of international business and economic law more critically important for business, policy makers and other stakeholders than it was previously.

About CIBEL Working Paper Series

The CIBEL Working Paper Series provides a world's leading platform for the publication and promotion of quality research-in-progress on the most fundamental and cutting-edge issues relating to China, the Asia-Pacific region and the global economy in the fields of international business and economic law. It features work by established and early career academics and commentators worldwide and welcomes submissions accordingly.

Working Paper Website: https://www.cibel.unsw.edu.au/research/CIBEL-working-paper-series

Digital Industrial Policy through Data Security? – China's Approach and Security Exceptions under Trade Agreements

Xiaomeng Qu* & Weihuan Zhou**

ABSTRACT

As industrial policy and national security become increasingly integrated, the extent to which national security may be abused to foster select economic sectors requires more dedicated studies. We make two major contributions in this paper. First, we offer a critical analysis of China's digital industrial policy focusing on data security regulation and practices. We show that China has maintained a reasonably balanced approach towards data liberalization and protection without evidence to suggest abuses of national security to bolster its data sector. Yet, major loopholes remain in China's regulatory framework leaving room for discretion and abuse in deploying data security measures. As geopolitical tensions and strategic rivalries intensify, a data trade war in the name of national security is not a remote possibility. Second, we argue that the security exceptions under existing trade or digital economy agreements can hardly strike a desirable balance between data liberalization and security. Governments should join forces to modernize these exceptions, ideally via multilateral venues, by deliberating on data security goals and regulatory practices to build transparency and trust and lay the groundwork for negotiating more detailed exceptions for data security.

Keywords: WTO; FTAs; Digital economy agreements; China; Industrial policy; Data flows; Data localization; National Security.

I. INTRODUCTION

Industrial policy is not new. For decades, governments have deployed policies to foster the development of selected economic sectors or entities through a wide array of instruments.[1] Yet, no consensus exists in relation to the rationale and efficacy of industrial policies. For example, leading economists in this space have maintained that industrial policies are legitimate and effective so that the critical question is not whether such policies should be employed but how to make them better.[2] A recent report of the Organisation for Economic Co-operation and

* Lecturer, Member of the China-ASEAN Legal Research Center, School of International Law, Southwest University of Political Science & Law. Email: qxmmsr@gmail.com.

** Professor, Co-Director of the China International Business and Economic Law (CIBEL) Centre, Faculty of Law and Justice, UNSW Sydney. Email: weihuan.zhou@unsw.edu.au (corresponding author).

[1] See generally Dani Rodrik, 'Industrial Policy for the Twenty-First Century', September 2004, 1-56; Todd Tucker, 'Industrial Policy and Planning: What it is and How to Do It Better', Roosevelt Institute, July 2019, 1-49, https://rooseveltinstitute.org/wp-content/uploads/2020/07/RI_Industrial-Policy-and-Planning-201707.pdf.

[2] Réka Juhász, Nathan Lane, and Dani Rodrik, 'The New Economics of Industrial Policy', National Bureau of Economic Research Working Paper 31538 (August 2023) 1-48, https://www.nber.org/papers/w31538.

Development (OECD) also advocated for the important role that industrial policy can play in the pursuit of strategic goals and put forward a framework for better designing such policies.[3] In contrast, the classic criticisms of industrial policy remain influential, concerning misallocation of resources, economic inefficiency, and significant spillovers which adversely affect trading partners and generate trade tensions.[4] Moreover, while the success of leading East Asian and Latin American economies in pursuing industrialization and economic growth has presented a strong narrative in favour of industrial policy,[5] some have cautioned that empirical evidence remains limited to support "an activist government policy".[6]

Today, industrial policy is ubiquitous regardless of the ongoing debate over its rationale and utility. As Nobel laureate Professor Michael Spence has observed,

> "At a time of rising geopolitical tensions and supply-chain fragmentation – when national-security considerations are shaping economic policy, and the risks of war seem to be intensifying – industrial policy is all but inevitable. The question is how to do it well."[7]

Indeed, the rise of contemporary challenges concerning national security, supply chain resilience, sustainability, technological supremacy etc. has been widely perceived as justifications for the use of industrial policy.[8] That is, the current development of industrial policy is no longer confined to consideration of economic competitiveness or efficiency but embraces broader strategic, societal, and political goals. In this context, industrial policy that shapes business decisions and practices or creates national champions and global behemoths is on the rise,[9] although the West has long criticized and fought against such policies by state-led economies like China for concerns about market distortions and unfair trade practices.[10] Here, empirical studies have shown that

---

3 Chiara Criscuolo et al., 'An Industrial Policy Framework for OECD Countries: Old Debates, New Perspectives', OECD Policy Papers No. 127 (May 2022), https://www.oecd.org/en/publications/an-industrial-policy-framework-for-oecd-countries_0002217c-en.html.

4 See eg. Simon Evenett et al, 'The Return of Industrial Policy in Data', IMF Working Paper No. 2024/001 (January 2024), https://www.imf.org/en/Publications/WP/Issues/2023/12/23/The-Return-of-Industrial-Policy-in-Data-542828; Douglas Irwin, 'The Return of Industrial Policy', IMF Finance & Development Magazine (June 2023), https://www.imf.org/en/Publications/fandd/issues/2023/06/the-return-of-industrial-policy-douglas-irwin; IMF, OECD, World Bank and WTO, Subsidies, Trade, and International Cooperation, Analytical Notes No 2022/001 (April 2022), https://www.imf.org/en/Publications/analytical-notes/Issues/2022/04/22/Subsidies-Trade-and-International-Cooperation-516660.

5 See eg. above n 1, Rodrik, at 15; Tucker, at 13-16.

6 Howard Pack and Kamal Saggi, 'Is There a Case for Industrial Policy? A Critical Survey', (2006)21(2) *The World Bank Research Observer* 267-297.

7 Michael Spence, 'In Defense of Industrial Policy', Project Syndicate (5 May 2023), https://www.project-syndicate.org/commentary/industrial-policy-us-chips-and-science-act-debate-by-michael-spence-2023-05.

8 Ibid. See also above n 3, Criscuolo et al.

9 See eg. Ruchir Agarwal, 'Industrial Policy and the Growth Strategy Trilemma', IMF Finance & Development Magazine (September 2023), https://www.imf.org/en/Publications/fandd/issues/Series/Analytical-Series/industrial-policy-and-the-growth-strategy-trilemma-ruchir-agarwal; Willy C. Shih, 'The New Era of Industrial Policy Is Here', Harvard Business Review (September-October 2023), https://hbr.org/2023/09/the-new-era-of-industrial-policy-is-here; Anshu Siripurapu and Noah Berman, 'Is Industrial Policy Making a Comeback?', Council on Foreign Relations (18 September 2023), https://www.cfr.org/backgrounder/industrial-policy-making-comeback.

10 See Henry Gao and Weihuan Zhou, *Between Market Economy and State Capitalism: China's State-Owned Enterprises and The World Trading System* (Cambridge: Cambridge University Press, 2022) Ch 1-3. For a recent joint critique of China's economic system and policies by G7 countries, see The White House, 'G7 Hiroshima Leaders' Communiqué', 20 May 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-hiroshima-leaders-communique/.

industrial policies have been increasingly introduced by advanced economies to foster specific economic sectors or firms which are already powerful players in global markets.[11] In line with rapidly-expanding policy goals, governments have also repurposed and expanded their policy tools and practices by shifting from inward-oriented protectionist instruments such as tariffs to outward-oriented ones such as subsidies and export-related measures.[12] Consequently, while the new generation of industrial policies may be designed for certain legitimate policy objectives, they are more likely to spill across national borders.[13] However, in deploying these policies, governments tend to prioritize their own national interests without paying sufficient attention to the policies' global implications.[14]

Against this backdrop, this paper explores the so-called 'digital industrial policy' by focusing on data-related policies and regulation. As the world navigates the digital age, data regulation has proliferated and rapidly fragmented. Governments have introduced and continue to experiment a variety of regulatory approaches in pursuit of diverse and oftentimes competing policy goals. These range from promoting free flows of data for e-commerce, global business connectivity and supply chains to protecting privacy and cybersecurity, fostering national digital capabilities, and pursuing strategic competition for technological leadership.

To contribute to the already voluminous literature on data policies and regulation at domestic and international levels, this paper focuses on examining the growing interaction between digital industrial policy and national security, using China as a case study. As observed in Section II, digital industrial policies in major economies have been designed increasingly through a security lens. This trend generates concerns about the extent to which national security may be abused for protecting or advancing digital industries at home at the cost of foreign competitors. Here, China offers a good case study given its longstanding reliance on ambitious industrial policies to foster economic growth and global leadership, especially in the digital space in recent times. Therefore, Section III conducts a detailed study on the evolution of China's digital industrial policy with a focus on data policies and regulation. After a critical analysis of China's data security laws and practices, particularly those relating to cross-border data transfers and data localization, we find no compelling evidence to suggest that China has used security-based measures to bolster its data sector. Rather, we show that China has sought to maintain a balanced approach towards data security by ensuring that data restrictive measures target genuine security risks and do not cause unnecessary burdens on business operations. However, the existence of major ambiguities in China's data security laws, the well-known lack of transparency in China's regulatory practices, etc. may provide room for abuse of national security as industrial policy. To address the systemic challenges posed by the increasingly blurry line between (digital) industrial policy and national security, Section IV discusses the inadequacies of security exceptions in existing trade or digital economy agreements in dealing with data security, focusing on the Comprehensive and

---

[11] Réka Juhász et al., 'The Who, What, When, and How of Industrial Policy: A Text-Based Approach', Structural Transformation and Economic Growth WP050 (12 January 2023), https://steg.cepr.org/publications/who-what-when-and-how-industrial-policy-text-based-approach.

[12] Ibid. See also above n 3, Criscuolo et al.

[13] See above n 9, Shih.

[14] See the references in FN 4, and above n 9, Siripurapu and Berman. See also Bernard Hoekman, Petros Mavroidis and Douglas Nelson, *Non-Economic Objectives, Globalisation and Multilateral Trade Cooperation* (Paris & London: CEPR Press, 2023), https://cepr.org/publications/books-and-reports/non-economic-objectives-globalisation-and-multilateral-trade.

Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States–Mexico–Canada Agreement (USMCA), the Digital Economy Partnership Agreement (DEPA), the Regional Comprehensive Economic Partnership (RCEP) and the Joint Statement Initiative on E-commerce (JSI) under the World Trade Organization (WTO). We then propose ways to move forward negotiations of data security issues with an aim to modernizing the security exceptions to strike a proper balance between data liberalization and security. Section V concludes.

II. Digital Industrial Policy Via A Security Lens

As reported by Evenett and Fritz, "[p]olicymakers are flying blind as they shape and nurture the digital domain", with a better part of this fast-evolving, global regulatory developments driven primarily by fostering selected, domestic digital sectors.[15] While governments have different policy priorities, a common area of regulatory effort has been data[16] due to the pivotal role data plays in digital transformation. Various forms of regulatory interventions have been introduced to build data-related capabilities such as subsidizing R&D, digital start-ups and the establishment of data infrastructures, and enhancing enabling regulatory frameworks for data-based digital businesses.[17] Such interventions have also been used to foster the competitiveness of national tech companies through mobilizing local data collection, restricting cross-border data flows, mandating data localization, promoting outbound foreign investment, etc.[18] More broadly, the growing claim for data sovereignty can potentially become an all-encompassing policy that enables the deployment of industrial policy for a diverse range of economic and non-economic goals.[19]

Our key inquiry in this paper is "to what extent national security influences digital industrial policy especially in data regulation?" Recent studies have expounded the contrasting models that major economies have adopted in digital/data regulation, with the U.S. model focused on the protection of firms, the EU model on the protection of individuals, and the Chinese model on the protection of the state.[20] While this distinction captures the essence of the respective regulatory priorities, it does not offer sufficient insight of the intricacies associated with the

---

15 Simon Evenett and Johannes Fritz, *Emergent Digital Fragmentation: The Perils of Unilateralism* (London: CEPR Press, 2022) at 5, 14-15, https://www.hinrichfoundation.com/research/wp/digital/emergent-digital-fragmentation-the-perils-of-unilateralism/.

16 Ibid., at 21.

17 See generally Parminder Jeet Singh, 'Digital Industrialisation in Developing Countries — A Review of the Business and Policy Landscape', IT for Change Research Paper (December 2017), https://itforchange.net/sites/default/files/1468/Digital-industrialisation-May-2018.pdf.

18 Ibid. For a comprehensive discussion of digital policies and transformation in the US, China and the EU, see generally Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (New York: Oxford University Press, 2023).

19 See generally Melody Musoni, et al., 'Global Approaches to Digital Sovereignty: Competing Definitions and Contrasting Policy', ECDPM Discussion Paper No. 344 (May 2023), https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf; Anupam Chander and Haochen Sun, 'Sovereignty 2.0' in Anupam Chander & Haochen Sun (eds) Data Sovereignty: From the Digital Silk Road to the return of the State (New York: Oxford University Press, 2023) ch 1.

20 See generally above n 18, Bradford; Henry Gao, 'Digital or Trade? The Contrasting Approaches of China and US to Digital Trade', (2018)21(2) Journal of International Economic Law 297; Henry Gao, 'Data Sovereignty and Trade Agreements: Three Digital Kingdoms' in Anupam Chander & Haochen Sun (eds) Data Sovereignty: From the Digital Silk Road to the return of the State (New York: Oxford University Press, 2023) ch 9.

growing intersection of economic and security matters including in the digital domain. The anticipated escalation of geopolitical tensions and strategic competition between global powers, especially the US and China under the second Trump Administration, is leading to further expansion of security interests and growing influence of such interests on the development of industrial policy.

There is already abundant evidence to show strengthened regulatory linkages between digital industrial policy and national security. One major example concerns the ongoing shift of the US's pro-innovation, market-driven digital policy [21] to one that involves increasing regulatory interventions to restore American leadership in digital transformation and rulemaking. This shift can be viewed as one major dimension of the surge of U.S. industrial policy in recent times to promote U.S. global competitiveness in critical sectors, technologies, and manufacturing capabilities.[22] These industrial policies, officially labelled as the "modern American industrial strategy", have been developing noticeably through a security lens which may involve all matters related to economic prosperity and opportunity, democratic values, U.S. global leadership, and strategic and geopolitical competition with China.[23] To remain the world leader in critical and frontier technologies, the U.S. industrial strategy is determined to promote advanced manufacturing where data is the backbone of many targeted sectors.[24] To preserve policy space at home, the US recently withdrew its longstanding position on cross-border data flows and data localization in the WTO e-commerce negotiations and suspended digital trade talks in the Indo-Pacific Economic Framework for Prosperity (IPEF).[25] This was followed by an Executive Order of former President Biden to constrain outbound data transfers to certain countries of concern which may use the data to develop strategic advantages over the U.S., threatening U.S. national

---

[21] See generally Ashley Johnson, 'Restoring US Leadership on Digital Policy', ITIF (July 2023), https://www2.itif.org/2023-us-digital-policy-leadership.pdf.

[22] See generally Scott Lincicome, 'Made in America: The Boom in U.S. Manufacturing Investment', Testimony to the Joint Economic Committee of the United States Congress (12 June 2024), https://www.cato.org/testimony/made-america-boom-us-manufacturing-investment; above n 9, Siripurapu and Berman.

[23] See generally The White House, *National Security Strategy* (October 2022), https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf; The White House, 'Remarks on Executing a Modern American Industrial Strategy by NEC Director Brian Deese' (13 October 2022), https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-on-executing-a-modern-american-industrial-strategy-by-nec-director-brian-deese/; The White House, 'Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution' (27 April 2023), https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution/; U.S. Department of the Treasury, 'Remarks by Secretary of the Treasury Janet L. Yellen on the U.S. - China Economic Relationship at Johns Hopkins School of Advanced International Studies' (20 April 2023), https://home.treasury.gov/news/press-releases/jy1425; Andres B. Schwarzenberg, 'Industrial Policy and International Trade', U.S. Congressional Research Service (9 August 2024), https://crsreports.congress.gov/product/pdf/IF/IF12119.

[24] See generally National Science and Technology Council, *National Strategy for Advanced Manufacturing*, Report by the Subcommittee on Advanced Manufacturing and Committee on Technology (October 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Strategy-for-Advanced-Manufacturing-10072022.pdf.

[25] The Aspen Institute, 'Fireside Chat with Katherine Tai' (8 December 2023), https://www.youtube.com/watch?v=nwT5GfbxTMY; Danielle M. Trachtenberg, 'Digital Trade and Data Policy: Key Issues Facing Congress', U.S. Congressional Research Service (30 April 2024), https://crsreports.congress.gov/product/pdf/IF/IF12347/6.

security and foreign policy.[26] While this restriction on data flows to selected countries is apparently driven by security concerns, the US government recognizes that data protection can serve multiple goals such as protecting U.S. leadership and competitiveness.[27] A good example of recent legislative practices is the CHIPS and Science Act of 2022 which essentially adopts a subsidy-based industrial policy to advance U.S. global leadership in semiconductors, technologies of the future and the relevant supply chains, while this leadership is also seen crucial for protecting U.S. national security.[28] Another case in point concerns the regulatory development on artificial intelligence (AI). The Biden Administration already committed unwaveringly to advancing U.S. global leadership in AI technologies, infrastructure and capabilities as a matter of national security significance.[29] While abandoning AI policies under the Biden Administration, President Trump became even more committed to "enhance[ing] America's global AI dominance to promote ... economic competitiveness, and national security."[30] Given the importance of data for the training of AI, the recent development of U.S. AI policies sends a signal that more regulation may be introduced to tighten control over data.[31]

Similar regulatory developments where industrial policy and national security become increasingly integrated are also underway in other major economies. For example, faced with geopolitical shocks and uncertainties, the EU's "New Industrial Strategy" becomes inevitably multi-purpose with an emphasis on strengthening its "strategic autonomy".[32] When it comes to

---

[26] The White House, 'Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern' (28 February 2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

[27] National Science and Technology Council, *National Strategy for Advanced Manufacturing*, Report by the Subcommittee on Advanced Manufacturing and Committee on Technology (October 2022) at 8.

[28] The White House, 'FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China' (9 August 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/; The White House, 'FACT SHEET: Two Years after the CHIPS and Science Act, Biden-Harris Administration Celebrates Historic Achievements in Bringing Semiconductor Supply Chains Home, Creating Jobs, Supporting Innovation, and Protecting National Security' (9 August 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/08/09/fact-sheet-two-years-after-the-chips-and-science-act-biden-%e2%81%a0harris-administration-celebrates-historic-achievements-in-bringing-semiconductor-supply-chains-home-creating-jobs-supporting-inn/.

[29] The White House, 'Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence' (24 October 2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/.

[30] The White House, 'Fact Sheet: President Donald J. Trump Takes Action to Enhance America's AI Leadership' (23 January 2025), https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-takes-action-to-enhance-americas-ai-leadership/.

[31] For an interesting discussion of how the development of AI policies may increase the pursuit of digital/data sovereignty via industrial policy, see generally Andrew Keane Woods, 'Digital Sovereignty + Artificial Intelligence' in Anupam Chander & Haochen Sun (eds) *Data Sovereignty: From the Digital Silk Road to the return of the State* (New York: Oxford University Press, 2023) ch 5.

[32] See generally Simone Tagliapietra and Reinhilde Veugelers, 'Industrial Policy in Europe: Past and Future' in Simone Tagliapietra and Reinhilde Veugelers (eds) *Sparking Europe's New Industrial Revolution: A Policy for Net Zero, Growth and Resilience* (Belgium: Bruegel Blueprint Series, 2023) ch 1; The European Parliament, 'General Principles of EU Industrial Policy', Fact Sheets on the European Union (undated), https://www.europarl.europa.eu/factsheets/en/sheet/61/general-principles-of-eu-industrial-policy.

the digital domain, the Digital Agenda for Europe is currently focused on fulfilling the EU's technological and geopolitical goals by prioritizing critical and emerging technologies such as semiconductors, quantum computing as well as security-related interests such as cybersecurity and digital sovereignty.[33] As such, the EU's digital industrial policy treats digital capabilities and competitiveness as essential security interests.[34] The EU's data strategy, in particular, while maintaining a focus on the protection of individuals, sets forth a comprehensive blueprint for enhancing EU's data-related technologies, infrastructures and capabilities as a crucial way to safeguard its fundamental values, rights and digital sovereignty.[35]

In addition, digital industrial policy has also gained popularity in developing economies. While these policies are aimed at advancing domestic digital sectors including the data industry, they are also driven by non-economic goals particularly national security and (data) sovereignty.[36] Consequently, a set of policy tools, such as data blocking and localization, are put in place to serve both economic and non-economic goals, demonstrating growing linkages between industrial policy and national security.[37] Here, India has presented a more proactive case given the comprehensiveness and accomplishments of India's digital industrial policy in enabling regulatory environment and mobilizing diverse resources to foster the development of its digital firms and data-related infrastructures and capabilities.[38] At the same time, India's digital industrialization has also relied on a range of laws and regulations to protect digital security currently focusing on data security and sovereignty.[39] Thus, data control measures, such as localization requirements, are employed not only as a protectionist instrument but also a security instrument under India's overarching digital industrial policy.[40]

In short, as the global race for digital transformation intensifies, digital industrial policy has risen to an unprecedented scale underpinned by both economic and security considerations.[41]

---

[33] See The European Parliament, 'Digital Agenda for Europe', Fact Sheets on the European Union (undated), https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe.

[34] See The European Commission, 'European Industrial Strategy' (undated), https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en; The European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions', COM(2020)102 final (10 March 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0102.

[35] The European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions', COM(2020)66 final (19 February 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066; Macmillan Keck, 'The Role of Cross-Border Data Flows in the Digital Economy', UNCDF (Jul. 2022) at 11-12, https://policyaccelerator.uncdf.org/all/brief-cross-border-data-flows#:~:text=In%20a%20digital%20economy%2C%20cross,transfer%20of%20goods%20or%20services.

[36] See Christopher Foster & Shamel Azmeh, 'Latecomer Economies and National Digital Policy: An Industrial Policy Perspective', (2020)56(7) Journal of Development Studies 1247, 1257; Sanghyun Han, 'Data and Statecraft: Why and How States Localize Data', (2024)26(2) *Business and Politics* 263, 273-80.

[37] Ibid.

[38] See above n 17, Singh, at 35-56. For a more comprehensive discussion of India's digital strategy, see Li Zhang and Dayi Hu, 'National Digital Development Strategy and Its Practice in India' in Guang Yang et al. (eds) Countries and Regions: Dynamic Interconnectivity (Singapore: Palgrave Macmillan, 2024) 137-181.

[39] International Trade Administration of India, 'Digital Economy' (updated 18 September 2024), https://www.trade.gov/country-commercial-guides/india-digital-economy; above n 38, Zhang and Hu, at 165.

[40] See Kaushambi Bagchi, Gangesh Varma and Sashank Kapilavai, 'Data Flows and Data Localisation: An Economic Analysis', Indian Council for Research on International Economic Relations (June 2020) ii-iv, https://icrier.org/pdf/Data_Flows_and_Data_Localisation.pdf; Rudra Chaudhuri and Arjun Kang Joseph, 'Living in a Fragmented World: India's Data Way', (2024)23(2) India Review 154, 156-57.

[41] See above n 15, Evenett and Fritz.

This emerging trend in the development of digital industrial policy requires a more detailed study to demystify how such policies now interact with and are influenced by national security.

III. The Evolution Of China's Data Regulation: National Security As Industrial Policy?

China offers a good case study for at least two reasons: (1) China's economic growth has relied heavily on industrial policies for decades, and (2) the ambitious and fast-developing digital industrial policy in China has prioritized economic and security goals. Through a careful review and analysis of China's data-related policies and regulation, we seek to expound the extent to which the development of these policies has been shaped by security concerns and how national security may be (ab)used as a disguised protectionist tool to advance China's global leadership in digital industrialization. For this purpose, we adopt so-called process-tracing methodology by tracing the evolution of China's data regulatory regime based on primary sources.[42]

1. China's Digital Industrial Policy in a Nutshell

A brief review of the evolution of China's overarching digital industrial policy provides an important context for understanding its regulatory framework for data. This evolution dates to the 1990s and covers at least three main phases. In the first phase up to 2005, China's primary goal was to foster the infant information industry, particularly manufacturing capabilities of electronics and information products.[43] A well-known example concerns the growth of the semiconductor sector based on a wide array of subsidies and regulatory support, such as R&D and other grants, tax preferences, export promotion, and government procurement.[44] More broadly, through similar supportive schemes at both central and local levels, the information industry developed rapidly to become a key pillar of the national economy by 2005.[45]

The second phase (2006-2015) witnessed a shift of policy priorities from building an infant domestic industry to developing China's indigenous innovation and competitiveness in critical

---

[42] This methodology has proven effective and reliable in demystifying complex regulatory frameworks in the digital space. See eg. Rogier Creemers, 'China's Emerging Data Protection Framework', (2022)8(1) Journal of Cybersecurity 1; Han, above n 36.

[43] 《中华人民共和国国民经济和社会发展十年规划和第八个五年计划纲要》[Ten-Year Plan and the Eighth Five-Year Plan for Economic and Social Development of the People's Republic of China (1991–1995)], issued in April 1991, https://www.ndrc.gov.cn/fggz/fzzlgh/gjfzgh/200709/P020191029595681819982.pdf; 《中华人民共和国国民经济和社会发展"九五"计划和 2010 年远景目标纲要》[Ninth Five-Year Plan for Economic and Social Development of the People's Republic of China and the Outlines of Objectives in Perspective of the Year 2010 (1996–2000)], issued on 17 March 1996, https://www.ndrc.gov.cn/fggz/fzzlgh/gjfzgh/200709/P020191029595686994247.pdf; Feitao Jiang et al., 'China's Industrial Policy in the Digital Economy Era' [数字经济时代的中国产业政策], (2024) 6 *Study& Exploration* 168, 169–174.

[44] 《国务院关于印发鼓励软件产业和集成电路产业发展若干政策的通知》[Several Policies to Encourage the Development of the Software Industry and Integrated Circuit Industry], issued by the State Council on 24 June 2000, https://www.gov.cn/gongbao/content/2000/content_60310.htm; Alex He, 'China's Techno-Industrial Development: A Case Study of the Semiconductor Industry' (CIGI Papers No.252, May 2021) at 15, https://www.cigionline.org/static/documents/documents/no.252%20web.pdf.

[45] 《中华人民共和国国民经济和社会发展第十个五年计划纲要》[Tenth Five-Year Plan for Economic and Social Development of the People's Republic of China (2001–2005)], issued on 5 March 2001, www.gov.cn/gongbao/content/2001/content_60699.htm; '"十五"期间信息化建设成效显著' [Achievements in Informatization Development during the Tenth Five-Year Period] (1 January 2006), https://www.gov.cn/ztzl/2006-01/01/content_145195.htm.

technologies.[46] In light of its technology-and-innovation-oriented development model, China deployed massive resources to advance R&D and innovation in frontier information technologies[47] and develop supportive digital infrastructures.[48] These policies enabled China to process the world's largest broadband network infrastructure within a short period as well as the world's largest internet user base which produces a tremendous amount of data.[49] In 2015, the Chinese government recognized data as a "basic strategic resource" and since then has placed growing emphasis on the development and application of data in traditional and emerging industries to advance digital transformation.[50] At the same time, however, the rapid and widespread adoption of digital technologies, such as the internet, generated significant security-related challenges. Thus, since the early 2010s, the Chinese government has taken steps to strengthen security safeguard capabilities by enhancing digital security infrastructure,[51] tightening data protection,[52] amongst other means. As China's overarching economic policies continued to prioritize development and growth, data regulation in this phase remained piecemeal largely confined to consumer protection.[53] Nevertheless, these efforts laid the groundwork for the development of a comprehensive regulatory framework to address security concerns in the following decade.

---

[46] 《2006-2020年国家信息化发展战略》[The National Informatization Development Strategy for 2006-2020], issued by the General Office of the Central Committee of Communist Party of China and the General Office of the State Council on 19 March 2006, https://www.gov.cn/gongbao/content/2006/content_315999.htm.

[47] 《信息产业"十一五"规划》[Eleventh Five-Year Plan for Information Industry], issued by the Ministry of Industry and Information Technology and Information on 1 March 2007, https://www.ndrc.gov.cn/fggz/fzzlgh/gjjzxgh/200709/P020191104623156010398.pdf;《关于印发国家十二五科学和技术发展规划的通知》[Development Plan of Science and Technology for the Twelfth Five-Year Plan], issued by the Ministry of Science and Technology on 4 July 2011, https://www.most.gov.cn/xxgk/xinxifenlei/fdzdgknr/qtwj/qtwj2011/201107/t20110713_88228.html.

[48] 《中华人民共和国国民经济和社会发展第十一个五年规划纲要》[Eleventh Five-Year Plan for Economic and Social Development of the People's Republic of China (2006-2010)], issued on 14 March 2006, https://www.gov.cn/gongbao/content/2006/content_268766.htm; 《中华人民共和国国民经济和社会发展第十二个五年规划纲要》[Twelfth Five-Year Plan for Economic and Social Development of the People's Republic of China (2010-2015)], issued on 14 March 2011, https://www.gov.cn/2011lh/content_1825838.htm.

[49] '"十二五"期间宽带运营业发展回顾' [Review of the Development of Broadband Operation Industry during the Twelfth Five-Year Period] (2 August 2017), https://www.ndrc.gov.cn/xwdt/gdzt/xyqqd/201708/t20170802_1197809_ext.html.

[50] 《国务院关于积极推进"互联网+"行动的指导意见》[Guiding Opinions on Promoting the 'Internet Plus' Action Plan], issued by the State Council on 1 July 2015, https://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm; 《国务院关于印发促进大数据发展行动纲要的通知》[Action Outline for Promoting the Development of Big Data], issued by the State Council on 31 August 2015, https://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm.

[51] 《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》 [Several Opinions on Promoting the Development of Informatization and Effectively Ensuring Information Security], issued by the State Council on 28 June 2012, effective on 17 July 2012, https://www.gov.cn/zhengce/content/2012-07/17/content_5906.htm. In 2015, the Chinese government implemented 96 special projects for national information security. See《国家信息安全专项及下一代互联网技术研发、产业化和规模商用专项项目清单》[List of Projects for National Information Security, Next-Generation Internet Technology R&D, Industrialization, and Large-Scale Commercial Application], issued by the National Development and Reform Commission on 16 February 2015, https://zfxxgk.ndrc.gov.cn/web/iteminfo.jsp?id=3331.

[52] See above n 51, Several Opinions. For specific regulations, see Kemeng Cai, 'Jurisdictional Report: The People's Republic of China' in Clarisse Girot (eds), *Regulation of Cross-border Transfers of Personal Data in Asia*, ABLI Legal Convergence Series (May 2018) at 67-72, https://abli.asia/abli-publications/regulation-of-cross-border-transfers-of-personal-data-in-asia-softcover/.

[53] See above n 42, Creemers, at 4.

Balancing development and security interests has been at the centre of China's digital industrial policy in the third phase (2016-current). When it comes to data, the Thirteenth Five-Year Plan (2016-2020) reaffirmed the vital role of data in the digital transformation and stressed the need for the openness and sharing of government data, the development of infrastructure such as data platforms and centres, the advancement of data-related technologies, etc.[54] On the other hand, the Plan mandated the integration of data security into digital development by establishing a comprehensive regulatory framework for strengthening data protection across the entire data lifecycle.[55] The first major milestone in this balancing act was the enactment of the Cybersecurity Law (CSL)[56] in 2016, which becomes the cornerstone of China's digital security legislation.[57] As will be further discussed in Section III.2, this law introduced a classification of data and requirements on data localization and cross-border data flows, apart from other cybersecurity-related measures. Under the current fourteenth five-year period (2021–2025), the balancing act has continued to evolve through new policy priorities and regulatory interventions on both sides of the equation.

The "development" side has focused on broadening and deepening digital industrialization in both traditional and emerging sectors (e.g. communication equipment, core electronic components, and critical software vs. AI, big data, blockchain, and cloud computing).[58] Data is regarded as a "core engine" to drive the digital industrialization so that a national data market is needed to establish a comprehensive data-related supply chain involving the R&D, creation, collection, transfer, application, and storage of data.[59] For instance, new approaches have been introduced to facilitate the opening of business data by leading digital and internet platforms and promote cross-industry data interconnectivity and sharing through trusted data spaces collaboratively built by enterprises, research institutions, and industry organizations.[60] One of the

---

[54] 《中华人民共和国国民经济和社会发展第十三个五年规划纲要》[Thirteenth Five-Year Plan for National Economic and Social Development of the People's Republic of China (2016–2020)], issued on 17 March 2016, https://www.gov.cn/xinwen/2016-03/17/content_5054992.htm;《国务院关于印发"十三五"国家信息化规划的通知》[National Informatization Plan for the Thirteenth Five-Year Period], issued by the State Council on 15 December 2016, https://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm.

[55] Ibid.

[56] 《中华人民共和国网络安全法》[Cybersecurity Law of the People's Republic of China 2016] [hereinafter 'CSL'], promulgated by the Standing Committee of the National People's Congress on 7 November 2016, effective on 1 June 2017, http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm.

[57] See above n 42, Creemers, at 4.

[58] 《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》[Outline of the Fourteenth Five-Year Plan for the National Economic and Social Development and the 2035 Long Term Goals (2021–2025)], issued on 12 March 2021, https://www.gov.cn/xinwen/2021-03/13/content_5592681.htm.

[59] 《国务院关于印发"十四五"数字经济发展规划的通知》[Digital Economy Development Plan for the Fourteenth Five-year Period], issued by the State Council on 12 December 2021, https://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm.

[60] 《关于促进数据产业高质量发展的指导意见》[Guiding Opinions on Promoting the High-Quality Development of the Data Industry], issued jointly by six State ministries and departments on 28 December 2024, https://www.gov.cn/zhengce/zhengceku/202412/content_6995430.htm. For detailed policies on the opening and sharing of public and enterprise data, see 《关于加快公共数据资源开发利用的意见》[Opinions on Accelerating the Development and Utilization of Public Data Resources], issued by the General Office of the Central Committee of Communist Party of China and the General Office of the State Council on 21 September 2024, https://www.gov.cn/zhengce/202410/content_6978911.htm; 《关于促进企业数据资源开发利用的意见》[Opinions on Promoting the Development and Utilization of Enterprise Data Resources], issued by five State ministries and departments on 20 December 2024, https://www.gov.cn/zhengce/zhengceku/202412/content_6994570.htm.

latest developments was the establishment of China's first state-owned enterprise specializing in data integration and technology, which aims to build a platform for data sharing among highways, railways, waterways, aviation and ports, thereby creating a more competitive and innovative servicing ecosystem.[61]

On the "security" side, the Data Security Law[62] (DSL) and the Personal Information Protection Law[63] (PIPL) were enacted at the outset of the five-year period to provide detailed rules in specific areas of digital security and cumulatively to create a comprehensive regulatory framework for safeguarding the digital ecosystem. These were followed by the promulgation of a series of implementing regulations setting forth in detail the standards and procedures of existing and new security-related measures, such as security review, standard data security contract, and personal information protection certification,[64] which are further discussed in the section below.

A raft of criticisms have been levelled at China's digital industrial policy especially the security-related measures. For example, the CSL provoked an intense debate at the WTO with major players such as the US, the EU and Japan criticizing the law for creating protectionist and trade-restrictive instruments in the guise of cybersecurity.[65] Commentators have similarly criticized China's security-related data localization requirements and restrictions on cross-border data flows as digital protectionism aiming to boost Chinese tech firms at the cost of foreign competitors.[66] Has China used security-related measures to foster its digital industrialization? To answer this question, a more detailed assessment of China's balancing act in data regulation is warranted.

2. Balancing Development and Security in Data Regulation

As mentioned, the CSL, DSL and PIPL have consolidated and strengthened China's data protection mechanisms. While some elements of the mechanisms can be further clarified and

---

[61] Kandy Wong, 'How China manages big data is changing, as new state-owned firm takes the helm', SCMP (20 December 2024), https://www.scmp.com/economy/china-economy/article/3291731/how-china-manages-big-data-changing-new-state-owned-firm-takes-helm.

[62] 《中华人民共和国数据安全法》[Data Security Law of the People's Republic of China] [hereinafter 'DSL'], promulgated by the Standing Committee of the National People's Congress on 10 June 2021, effective on 1 September 2021, http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html.

[63] 《中华人民共和国个人信息保护法》 [Personal Information Protection Law of the People's Republic of China] [hereinafter 'PIPL'], promulgated by the Standing Committee of the National People's Congress on 20 August 2021, effective on 1 November 2021, https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm.

[64] 《数据出境安全评估办法》 [Measures for Security Assessment of Outbound Data Transfer 2022] [hereinafter 'Security Assessment Measures'], issued by the Cyberspace Administration of China on 7 July 2022, effective on 1 September 2022, https://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm; 《个人信息出境标准合同办法》[Measures on Standard Contract for Outbound Transfers of Personal Information] [hereinafter 'Standard Contract Measures'], issued by the Cyberspace Administration of China on 22 February 2023, effective on 1 June 2023, https://www.gov.cn/zhengce/202311/content_6917770.htm; 《关于实施个人信息保护认证的公告》[Announcement on the Implementation of Personal Information Protection Certification], issued by the State Administration for Market Regulation and the Cyberspace Administration of China on 4 November 2022, https://www.samr.gov.cn/rzjgs/zcfg/art/2022/art_e7cf688ac2944d84b641008252e31db8.html.

[65] See eg. WTO, Committee on Technical Barriers to Trade, 'Minutes of the Meeting of 29-30 March 2017', G/TBT/M/71 (2 June 2017) 3-6.

[66] Council on Foreign Relations, 'The Rise of Digital Protectionism' (18 October 2017), https://www.cfr.org/report/rise-digital-protectionism. For detailed discussions of digital protectionism, see eg. Susan Ariel Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?', (2019) 18(4) *World Trade Review* 541.

refined, we argue that these mechanisms have been designed cautiously in balanced ways to pursue genuine security interests. To expound this balanced approach, we focus on analyzing the security measures related to data localization and cross-border data flows below.

In general, the legislation above has established a tiered risk management system for protecting data security based on the importance of data, operators and security interests. This system does not impose a blanket restriction on the cross-border flow or localization of data. Rather, it adopts different levels of regulatory checks and requirements commensurate to the severity of security risks and impacts, thereby developing a proportionate and targeted approach towards data security. More specifically, the CSL has not only unified the fragmented rules on data localization and cross-border transfer scattered in different prior regulations.[67] It has also reduced the relevant restrictions by requiring data localization only in certain circumstances and permitting cross-border data transfers when prescribed conditions are met, a more balanced approach subsequently reaffirmed in the DSL and PIPL.[68]

(a) Data Localization

Data localization is required in three major circumstances. The first circumstance concerns personal information and "important data" collected and generated by critical information infrastructure operators (CIIOs).[69] As further clarified in the relevant implementing regulations, "critical information infrastructure" refers to "important network infrastructure and information systems in important industries and sectors, including telecommunications, information services, energy, transportation, hydraulic engineering and water utilities, finance, public services, e-government services, national defense science and technology, and others that once damaged or suffer a data leakage, could severely harm national security, the economy, livelihoods, or the public interest."[70] "Important data" covers "data that can endanger national security, economic operations, social stability, or public health and safety if manipulated, destroyed, leaked or illegally obtained or used."[71] To provide better clarity and certainty, the DSL mandates competent authorities to formulate "important data" catalogues which specify the scope of important data in specific sectors.[72] As remarked by President Xi, the localization requirement under this circumstance targets data generated by industries of the highest economic and social importance and likely to attract the most advanced attacks.[73] Since CIIOs have greater control

---

67 See eg. Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them', Information Technology & Innovation Foundation (19 July 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

68 See above n 56, CSL, art 37; above n 62, DSL, art 31; above n 63, PIPL, art 40. To compare with the previous restrictions, see above n 52, Cai, at 67–72.

69 above n 56, CSL, art 37.

70 《关键信息基础设施安全保护条例》 [Regulation on Security Protection of Critical Information Infrastructure], issued by the State Council on 30 July 2021, effective on 1 September 2021, https://www.gov.cn/gongbao/content/2021/content_5636138.htm, art 2.

71 See above n 64, Security Assessment Measures, art 19.

72 See above n 62, DSL, art 21.

73 '习近平在网络安全和信息化工作座谈会上的讲话' [Xi Jinping's Speech at the Symposium on Cybersecurity and Informatization Work], Xinhua News (26 April 2016) https://www.xinhuanet.com//zgjx/2016-04/26/c_135312437_4.htm.

over data, data localization enables easier monitoring of local servers and faster responses to data leaks and cyberattacks.[74]

The second circumstance requires non-CIIOs to localize "important data".[75] Thus, this localization requirement concerns the importance of data and the interests such data may affect rather than who controls the data. For instance, personal and business data held by private firms can be subject to this requirement if the data falls within the "important" category.[76] As noted above, the development of "important data" catalogues is delegated to competent authorities overseeing specific industries. One example is the automotive industry which possesses increasingly advanced data processing capabilities and generates huge volumes of data.[77] A joint measure issued by five central authorities classifies six types of data as being "important", including geographic data, pedestrian and vehicle flows in sensitive areas (e.g. defense and military administrative zones), data related to certain segments of economic operations (e.g. vehicle flow and logistics), operational data of automobile charging networks, external video and image data (e.g. facial and license information), and other data that may impact national security, public interests and individual rights as decided by the authorities.[78] Therefore, while "important data" may vary among industries, the localization of such data is driven by concerns about security risks associated with the exposure of sensitive information, leakage of key personnel movements, disclosure of critical national targets (e.g. locations of military and defense industrial bases, and government facilities), theft of R&D data, and damage to critical infrastructure, etc.[79]

The third circumstance concerns personal information collected and generated by non-CIIOs that process such information above prescribed thresholds.[80] The current thresholds involve a non-CIIO "cumulatively providing personal information of over 1 million individuals (excluding sensitive personal information) or sensitive personal information of over 10,000 individuals to overseas entities since January 1 of the current year."[81] While the thresholds specifically target the cross-border transfer of data (see below), they would also trigger the localization

---

74 Neha Mishra, 'Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?' (2020), 19(3) *World Trade Review* 341, 355; Jinhe Liu, 'China's data localization', (2020) 13(1) *Chinese Journal of Communication*, 84, 91.

75 See above n 64, Security Assessment Measures, art 4.1; 《促进和规范数据跨境流动规定》[Provisions on Facilitating and Standardizing Cross-Border Data Flow 2024] [hereinafter 'Facilitating and Standardizing Provisions'], issued by the Cyberspace Administration of China on 22 March 2024, https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm, art 7.2.

76 See '数据出境安全评估：保护基础性战略资源的重要一环' [Security Assessment of Outbound Data Transfer: An Important Part of Protecting Basic Strategic Resources], Cyberspace Administration of China (7 August 2017), https://www.cac.gov.cn/2017-08/07/c_1121443948.htm.

77 For example, the daily data generation of an autonomous vehicle is estimated at 4,000 gigabytes, which train the car how to behave in real-life road conditions. See Christopher Foster and Shamel Azmeh, 'Aligning digital and industrial policy to foster future industrialization', Industrial Analytics Platform Insights (May 2023), https://iap.unido.org/articles/aligning-digital-and-industrial-policy-foster-future-industrialization.

78 《汽车数据安全管理若干规定（试行）》[Provisions on the Management of Automobile Data Security (Trial)], issued by five ministries on 16 August 2021, effective on 1 October 2021, https://www.gov.cn/zhengce/zhengceku/2021-09/12/content_5640023.htm, art 3.

79 '智能网联汽车信息安全是国家安全的重要防线' [Information Security of Intelligent Connected Vehicles is a Crucial Defense for National Security] (22 October 2021), https://www.rmzxw.com.cn/c/2021-10-22/2971170.shtml.

80 See above n 63, PIPL, art 40.

81 See above n 75, Facilitating and Standardizing Provisions, art 7.2.

requirement.[82] Major technology firms such as Google, Apple, Alibaba hold a vast amount of user information. As explained by a leading Chinese expert and government advisor, if foreign entities obtain such information, they could combine the data with other datasets, using various algorithms for data mining, to extract information that could potentially threaten China's national security.[83] Thus, this localization requirement is designed to minimize security risks associated with the transmission of personal data at a degree that may pose security risks due to the rapid development of digital firms and technologies.[84]

(b) Cross-border Data Flows

Like its regulatory approach to data localization, China does not prohibit data holders from transferring data abroad. The tiered risk management mechanism consists of two main layers of requirements: (1) security review and (2) standard contract or personal data protection certification. The circumstances that would trigger the security review are essentially those in which the localization requirement applies, namely, (1) the transfer of personal information and "important data" by CIIOs, and (2) the transfer of "important data" or the transfer personal data beyond the above-mentioned thresholds by non-CIIOs.[85] The security review is based on objective criteria to address genuine security risks and balance security concerns with commercial interests by allowing data operators to transfer important data and personal information abroad when necessary for business purposes.[86] The assessment criteria involve, for example, the necessity and legitimacy of a proposed transfer, the importance of data and the scale of the transfer, the situation of cybersecurity protection and the availability of protective measures for business and personal data in the recipient jurisdiction, etc.[87] In other circumstances, a security review is not needed before data can be transferred abroad. Where the transfer of data by non-CIIOs is below the prescribed thresholds but involves non-sensitive personal information of over 100,000 individuals, the transferring entity is asked to conclude a standard contract formulated by the Cyberspace Administration of China (CAC) with the overseas recipient or obtain a personal information protection certification from a third-party accredited institution according to standards and requirements set forth by the CAC.[88] Like the security review criteria, the mandatory contractual clauses and the certification requirements are reasonably focused on addressing potential security risks associated with the transfer of data overseas in accordance with China's cyber/data security law and standards.[89]

---

[82] Jihong Chen et al., '《数据出境安全评估办法》十四个焦点问题的理解' [Understanding the Fourteen Key Issues in the Measures for Security Assessment of Outbound Data Transfer], Zhong Lun Law Firm (8 July 2022), https://www.zhonglun.com/research/articles/9175.html.

[83] Yanqing Hong, 'The Cross-Border Data Flows Security Assessment: An important part of protecting China's basic strategic resources', Yale Law School Paul Tsai China Center Working Paper (20 June 2017), https://law.yale.edu/sites/default/files/area/center/china/document/dataflowssecurity_final.pdf, at 9.

[84] Linghan Zhang, '个人信息跨境流动制度的三重维度' [Three Dimensions of the Cross-Border Flow of Personal Information System] (2021)5 *China Law Review* 37, 41.

[85] See above n 75, Facilitating and Standardizing Provisions, art 7.

[86] '《数据出境安全评估办法》答记者问' [Press Conference: Measures for Security Assessment of Outbound Data Transfer], Cyberspace Administration of China (7 July 2022), https://www.cac.gov.cn/2022-07/07/c_1658811536800962.htm.

[87] See above n 64, Security Assessment Measures, art 8.

[88] See above n 75, Facilitating and Standardizing Provisions, art 8.

[89] See above n 64, Standard Contract Measures, art 5; 《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》[Cybersecurity Standards Practice Guidelines: Security Certification Specifications for

(c) Security as Industrial Policy? – An Appraisal

Our review of China's regulation of data localization and cross-border transfer provides little evidence to suggest an abuse of national security for digital industrialization. Rather, it depicts a carefully-designed, balanced approach in China's pursuit of development and security interests in data regulation. While data localization and cross-border transfer restrictions are widely perceived as major forms of digital protectionism,[90] China's regulatory framework demonstrates a reasonable level of specificity and proportionality aimed at addressing genuine security risks so that the security measures do not unnecessarily impede trade, investment or other business activities.

This observation is supported by facts. For instance, a recent OECD policy paper found that China's data localization requirements fall within a "least restrictive" category among all types of such requirements adopted by a host of economies.[91] A survey conducted by the European Chamber in 2023 showed that a vast majority of European companies (70%) were able to transfer data out of China via the standard contract path without having to undertake a security review.[92] It was also reported that out of the 25 companies that passed data security assessments in 2023, only 10 were Chinese.[93] Thus, as affirmed by the US-China Business Council, China's regulatory requirements on cross-border data transfer are unlikely to significantly benefit Chinese companies *vis-à-vis* foreign investors as these requirements also impact Chinese firms seeking to expand overseas.[94]

China's balancing act becomes even more evident if one considers the continuous effort of the Chinese government to address business concerns about increased operational and compliance costs and difficulties caused by the data security measures.[95] A series of recent foreign investment policies released by the State Council reiterated China's commitment to facilitating "secure, orderly, and free flows of data across borders".[96] Accordingly, the CAC issued an

---

Cross-Border Personal Information Processing Activities], issued by the Secretariat of the National Information Security Standardization Technical Committee on 16 December 2022, https://www.tc260.org.cn/front/postDetail.html?id=20221216161852, art 5.4.

90 For an assessment of the economic costs associated with restrictions on cross-border data flow and data localization requirements, see generally OECD and WTO, *Economic Implications of Data Regulation: Balancing Openness and Trust* (OECD Publishing, Paris, 2025), https://www.wto.org/english/res_e/booksp_e/data_regulation_e.pdf.

91 Chiara Del Giovane et al., 'The Nature, Evolution and Potential Implications of Data Localisation Measures', OECD Trade Policy Paper No. 278 (10 November 2023), https://www.oecd.org/en/publications/the-nature-evolution-and-potential-implications-of-data-localisation-measures_179f718a-en.html, at 8-11; above n 90, OECD and WTO, at 17.

92 European Chamber, 'Flash Survey: the Impact of China's Data Regulations on European Business' (14 November 2023), https://www.europeanchamber.com.cn/en/flash-survey-on-impact-of-china-rsquo-s-data-regulations, at 3.

93 Yinan Wang, '2023 数据跨境流动年终盘点及未来展望' [2023 Year-End Review and Future Outlook on Cross-Border Data Flows], DeHeng Law Office (2 January 2024), https://www.dehenglaw.com/CN/tansuocontent/0008/029915/7.aspx?MID=0902.

94 The US-China Business Council, 'How American Companies are Approaching China's Data, Privacy, and Cybersecurity Regimes' (13 April 2022), https://www.uschina.org/reports/how-american-companies-are-approaching-china%E2%80%99s-data-privacy-and-cybersecurity-regimes, at 6.

95 See generally above n 92, European Chamber; The American Chamber of Commerce in the People's Republic of China, '2023 American Business in China White Paper' (April 2023), https://www.amchamchina.org/wp-content/uploads/2023/04/AmCham-China-2023-White-Paper.pdf, at 74.

96 《关于进一步优化外商投资环境加大吸引外商投资力度的意见》 [Opinions on Further Optimizing the Foreign Investment Environment and Attracting Foreign Investment 2023], issued by the State Council on 25

implementation measure to streamline the regulatory requirements particularly security reviews with a list of circumstances exempted from such reviews.[97] Significantly, this measure, for the first time, introduced a 'negative list' approach for free trade zones, allowing those areas to develop their own catalogue of data that needs to be subject to the regulatory checks.[98] Foreign observers welcomed these changes as a substantial relaxation of China's data security requirements, thereby reducing compliance burdens for foreign companies.[99] As the CAC confirmed in a recent press conference, since the measure took effect, the streamlined requirements led to a 60% year-on-year decrease in the number of security assessment projects and a 50% drop in the number of standard contract filings for personal information transfers.[100] Only 10% of the notified projects (or 27 out of 285 projects) failed to pass security reviews, with most rejected due to procedural issues and only a few for a lack of necessity to transfer important data abroad or the presence of security risks.[101] Thus, it seems that China has been successful in experimenting new ways to soften security-related checks and requirements and liberalize data-related restrictions incrementally.

China's balanced approach towards data security can be explained by at least four reasons. The first relates to China's ambition to advance digital transformation which requires a market-oriented data sector to stimulate competition, innovation and growth while maintaining government interventions, including security measures, only to the extent necessary.[102] Secondly, a market-based regulatory framework is also aligned with China's long-term opening-up strategy which includes attracting foreign investment by consecutively reducing regulatory restrictions and enhancing protection of foreign investors.[103] Avoiding excessive and discriminatory requirements on data localization and cross-border data flows is key to ensuring the efficacy and attractiveness of China's foreign investment policy in the digital age.[104] Thirdly, a balanced approach is necessary for advancing China's global strategies and engagement, particularly its continued effort to join

---

July 2023, effective on 13 August 2023, https://www.gov.cn/zhengce/content/202308/content_6898048.htm; 《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》[Action Plan on Promoting High-Level Opening Up and Attracting and Utilizing Foreign Investment 2024], issued by the General Office of State Council on 28 February 2024, effective on 19 March 2024, https://www.gov.cn/zhengce/content/202403/content_6940154.htm; 《2025 年稳外资行动方案》[Plans to Stabilize Foreign Investment 2025], issued by the State Council on 17 February 2025, https://www.gov.cn/zhengce/content/202502/content_7004409.htm.

97 See above n 75, Facilitating and Standardizing Provisions, arts 2–5, 7–9, 13. This measure replaced any inconsistent provisions in the older regulations including the Security Assessment Measures (above n 64) and the Standard Contract Measures (above n 64).

98 See above n 75, Facilitating and Standardizing Provisions, art 6.

99 See eg. Reuters, 'China Relaxes Security Review Rules for Some Data Export' (23 March 2024), https://www.reuters.com/technology/cybersecurity/chinas-cyberspace-regulator-issues-rules-facilitate-cross-border-data-flow-2024-03-22/.

100 '国家数据局举行专题新闻发布会，介绍"关于推动数据产业高质量发展和促进企业数据资源开发利用"相关情况'[Press Conference: Promoting High-Quality Development of the Data Industry and Facilitating the Development and Utilization of Enterprises Data"], National Data Administration (31 December 2024), https://www.nda.gov.cn/sjj/swdt/xwfb/1231/20241231172831486110195_pc.html.

101 Ibid.

102 Ibid.

103 For a review of China's foreign investment regime, see Weihuan Zhou, Huiqin Jiang and Qingjiang Kong, 'Technology Transfer under China's Foreign Investment Regime: Does the WTO Provide a Solution?' (2020)54(3) Journal of World Trade 455, 460-69. For China's current foreign investment negative list, see https://www.gov.cn/zhengce/202409/content_6973047.htm.

104 See above n 96.

more advanced trade or digital economy agreements such as the CPTPP and the DEPA.[105] These agreements, and many other free trade agreements (FTAs) concluded in recent times, require the parties to facilitate free flows of data across borders and minimize data localization requirements.[106] Using security measures for digital industrial policy would undermine not only China's effort to join these agreements but also its global reputation more generally as China has long positioned itself as a proponent of the rules-based trading system and an opponent to the abuse of national security.[107] Finally and equally importantly, China does not need to use national security as a tool to promote its digital industrialization. Instead, it remains reliant on traditional policy instruments, such as subsidies, for its digital industrial policy.[108]

While there is no compelling evidence to suggest that China has used security-based measures to bolster its data sector, these measures have continued to attract criticisms about their (potential) asymmetric impact on foreign business. For example, some have argued that the data localization requirements have increased the cost of foreign investors in China and have supported the development of local digital infrastructure particularly data centres.[109] In this regard, it has been reported that global automakers such as BMW, Daimler, Ford and Telsa have set up facilities in China to store data generated by their cars locally, in order to comply with China's data localization rules.[110] In addition, notable ambiguities in the legislation (such as the definitions of "important data" and "CIIOs"), the typical residual category of "other circumstances" which may raise security concerns, and the lack of transparency in China's security reviews still provide room for discretion and abuse when needed.[111] Given the global industrial policy race in the digital domain, a major way to minimise such abuse of national security as industrial policy is for all governments involved to tackle security-based data policies via concerted effort.

---

[105] State Council, 'China to speed up accession to CPTPP', (22 March 2024), https://english.www.gov.cn/news/202403/22/content_WS65fcddf2c6d0868f4e8e555c.html; State Council, 'China to advance efforts to join DEPA: Ministry of Commerce', (21 November 2024), https://english.www.gov.cn/news/202411/21/content_WS673f328bc6d0868f4e8ed4a9.html.

[106] The full text of the CPTPP is accessible here: https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/tpp-text-and-associated-documents, arts 14.11 and 14.13. The full text of the DEPA is accessible here: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources, arts 4.3 and 4.4. For a more comprehensive review of digital trade commitments in recent FTAs, see Mira Burri and Kholofelo Kugler, 'Regulatory Autonomy in Digital Trade Agreements', (2024)27(3) Journal of International Economic Law 397, 400-3.

[107] For a discussion of China's approaches to national security under the global trading system, see Weihuan Zhou, Huiqin Jiang and Zhe Chen, 'Trade vs. Security: Recent Developments of Global Trade Rules and China's Policy and Regulatory Responses from Defensive to Proactive', (2023)22(2) World Trade Review 193.

[108] For a discussion of China's subsidization of its high tech industries and the applicability of WTO rules, see Weihuan Zhou and Meng Fang, 'Subsidizing Technology Competition: China's Evolving Practices and International Trade Regulation', (2021)30(3) Washington International Law Journal 470. For policy documents, see eg. '中共中央 国务院印发《数字中国建设整体布局规划》', 27 February 2023, https://www.gov.cn/zhengce/2023-02/27/content_5743484.htm; '数字经济将迎来多重政策利好', 22 July 2024, http://www.scio.gov.cn/live/2024/34328/xgbd/202407/t20240716_855424.html.

[109] Emily de la Bruyère and Nathan Picarsic, 'China's Quest for Asymmetric Dominance in Data Centers', Hinrich Foundation (25 June 2024), https://www.hinrichfoundation.com/research/wp/tech/china-quest-for-asymmetric-dominance-in-data-centers/, at 8.

[110] Yilei Sun and Tony Munroe, 'As China Plans New Rules, Global Automakers Move to Store Car Data Locally', Reuters (27 May 2021), https://www.reuters.com/business/exclusive-china-plans-new-rules-global-automakers-move-store-car-data-locally-2021-05-27/.

[111] See eg. Raymond Yang Gao, 'A Battle of the Big Three? – Competing Conceptualizations of Personal Data Shaping Transnational Data Flows' (2023), 22(4) *Chinese Journal of International Law* 707, 771; above n 99, Reuters.

IV. MODERNIZING SECURITY EXCEPTIONS IN TRADE AGREEMENTS

As governments continue to liberalize data localization and cross-border data transfer requirements through trade or digital economy agreements, they have also created a range of exceptions and carve-outs for regulatory intervention on privacy, cybersecurity, and other public policy objectives.[112] Whether these exceptions have provided sufficient policy space for data regulation in economies with different conditions and preferences is controversial. While national security has come to the fore of this balancing act between trade and non-trade values, it has generated growing concerns about abuse for strategic and protectionist goals. The lack of clarity about security exceptions in trade agreements remains an existential challenge for governments to confine the use of such exceptions to reasonable parameters.

1. Constraints (or a Lack of Constraints) of Security Exceptions under the WTO & FTAs

The security exception under the WTO was created at the conclusion of the General Agreement on Tariffs and Trade (GATT) in 1947 and remained unchanged today. As of this writing, WTO panels have interpreted and applied this exception, i.e. Article XXI of the GATT, in four disputes, all of which focused on subparagraph (b)(iii).[113] Article XXI reads:[114]

> Nothing in this Agreement shall be construed
> (a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or
> (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests
> (i) relating to fissionable materials or the materials from which they are derived;
> (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;
> (iii) taken in time of war or other emergency in international relations; or
> (c) to prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.

The panels' rulings on three key legal issues for determining the scope of the security exception were consistent. Firstly, whether a security measure that violates WTO rules is justifiable under the exception is not self-judging. Rather, such measures must satisfy certain legal conditions, a matter that is justiciable. In *Russia – Traffic in Transit*, the panel explained that this interpretative approach reflects the intention of the drafters to strike a balance by distinguishing "military and serious security-related conflicts from economic and trade disputes" and genuine security measures from protectionism.[115] In *US – Origin Marking (Hong Kong, China)*, the panel

---

[112] See generally above n 106, Burri and Kugler.

[113] The four panel decisions are: Panel Report, *Russia – Measures Concerning Traffic in Transit*, WT/DS512/R (adopted 26 April 2019); Panel Report, *Saudi Arabia – Measures concerning the Protection of Intellectual Property Rights*, WT/DS567/R (circulated 16 June 2020); Panel Report, *United States – Certain Measures on Steel and Aluminium Products*, WT/DS544/R (circulated 9 December 2022); Panel Report, *United States – Origin Marking Requirement*, WT/DS597/R (circulated 21 December 2022).

[114] Where data regulation raises issues under the General Agreement on Trade in Services (GATS) or the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs), GATS Article XIV *bis* and TRIPs Article 73(b)(iii) provide for security exceptions identical to GATT Article XXI.

[115] See above n 113, Panel Report, *Russia – Traffic in Transit*, paras. 7.81, 7.98; Panel Report, *US – Steel and Aluminium Products (China)*, paras. 7.105-28.

elaborated that the chapeau and the subparagraphs of Article XXI are not a "single relative clause" but set out separate legal conditions, and that the phrase "which it considers" applies to the chapeau only.[116] This means that whether a contested measure satisfies these conditions is justiciable as these conditions serve to "circumscribe (and limit) the circumstances in which the invoking Member may take action which it considers necessary for the protection of its essential security interests."[117]

Secondly, the scope of "emergency in international relations" is highly restrictive. The panels required "emergency" to involve situations "of the utmost gravity" leading to "a breakdown or near-breakdown" in international relations.[118] In *US – Origin Marking (Hong Kong, China)*, the panel clarified that the term "international relations" "may involve diverse matters, such as political, economic, social, or cultural exchanges."[119] This suggests that the scope of national security may extend beyond military and defence interests to include economic, social and other interests according to the needs of individual governments. However, the panel maintained the strict interpretation of "emergency" which, in its view, must involve an exceptional state of affairs than mere "tensions" or "divergences".[120] Based on the above interpretation, an "emergency in international relations" was found to exist in *Russia – Traffic in Transit* involving armed conflicts between Russia and Ukraine and in *Saudi Arabia – IPRs* involving a heightened and comprehensive diplomatic crise between Saudi Arabia and Qatar. In contrast, in *US – Steel and Aluminium Products (China)*, the panel ruled that global steel overcapacity and its impact on the industries in the US and worldwide did not amount to an emergency in international relations, although it had provoked international concerns and cooperative actions to address the overcapacity.[121] In *US – Origin Marking (Hong Kong, China)*, while the enactment of the Hong Kong (HK) National Security Law provoked some economic and political tensions, the panel held that these did not "meet the requisite level of gravity to constitute an emergency in international relations".[122] In reaching this conclusion, the panel also relied on the fact that the US actions targeted HK only (i.e. not China) and only certain areas of their relations while bilateral trade and cooperation had continued in many other aspects.[123]

Thirdly, Article XXI(b)(iii) imposes an obligation of "good faith" which in turn entails a minimum requirement of "plausibility" between the means and the ends.[124] For the WTO tribunal, this requirement is needed to avoid abuse of "Article XXI as a means to circumvent" GATT obligations.[125] However, the evidentiary standard on "plausibility" is significantly lower than that on "emergency", merely requiring that a contested measure is not "so remote from, or unrelated to" the security interest concerned. By doing so, the tribunal sought to develop a

---

[116] See above n 113, Panel Report, *US – Origin Marking (Hong Kong, China)*, paras. 7.48-88.

[117] Ibid., paras. 7.89, 7.263.

[118] See above n 113, Panel Report, *Russia – Traffic in Transit*, para. 7.136; Panel Report, *Saudi Arabia – IPRs*, paras. 7.257-260; Panel Report, *US – Steel and Aluminium Products (China)*, para. 7.139; Panel Report, *US – Origin Marking (Hong Kong, China)*, paras. 7.289, 7.297-98.

[119] See above n 113, Panel Report, *US – Origin Marking (Hong Kong, China)*, para. 7.280.

[120] Ibid., paras. 7.289, 7.311.

[121] See above n 113, Panel Report, *US – Steel and Aluminium Products (China)*, paras. 7.142-48.

[122] See above n 113, Panel Report, *US – Origin Marking (Hong Kong, China)*, paras. 7.323-53.

[123] Ibid., para. 7.354.

[124] See above n 113, Panel Report, *Russia – Traffic in Transit*, paras. 7.132, 7.138; Panel Report, *Saudi Arabia – IPRs*, paras. 7.283-88.

[125] See above n 113, Panel Report, *Russia – Traffic in Transit*, para. 7.133.

balanced approach to the interpretation and application of the security exception by requiring the security measures to have at least some connection to the claimed objectives.

Thus, the key constraint on policy space under the security exception pertains to the high standard imposed on what situations may amount to an "emergency" in international relations. This constraint stems from the narrowness of the treaty language itself, as intended by the drafters.[126] As such, the security exception provides little room for data security measures precisely because of the requirement that an "emergency in international relations" must be present. Nor would the exception accommodate the need of governments to tackle potential security risks such as cyberattacks as opposed to imminent ones.[127]

In contrast with the constraint on policy space above, Article XXI(a) provides considerable leeway for a government to refrain from "furnish[ing] any information the disclosure of which it considers contrary to its essential security interests". This paragraph operates independently from Article XXI(b) and is not subject to any additional legal requirements as those implicated by the subparagraphs of Article XXI(b). While it would still not permit self-judging, the only applicable condition would be the minimum requirement of plausibility as per the panel's rulings in *Russia – Traffic in Transit* discussed above.[128] Thus, restrictions on transferring data or supplying data in other ways can be justified so long as they are not implausible as measures protective of a chosen security interest. Such a minimum degree of connection between the means and the ends is not hard to establish. Moreover, Article XXI(a) does not limit the coverage of information or entities that provide information but instead allows *any* measures to be taken to address security risks associated with the supply of *any* information by *any* entity. Therefore, when compared to Article XXI(b)(iii), Article XXI(a) almost goes to the other extreme for a lack of any substantive constraint on data security measures, although one may question whether the provision or supply of data also covers data localization requirements or measures limiting access to data.[129]

The WTO's security exception has been further developed in recent trade or digital economy agreements in two major aspects. One is softening the legal conditions to allow more flexibility in invoking security exceptions in general. The other is expanding the scope of the exceptions for data regulation more specifically. For example, Article 32.2 of the USMCA[130] clarified that the disclosure of information includes not only actively transferring or supplying information but also allowing access to information (paragraph 1(a)). The latter is added to close the potential loophole under GATT Article XXI(a) so that the security exception may arguably be applied to all forms of information disclosure.[131] Paragraph 1(b) then removed the subparagraphs of GATT Article XXI(b) while maintaining the chapeau so that the phrase "it considers necessary" is no

---

[126] See Mona Pinchis-Paulsen, 'Trade Multilateralism and U.S. National Security: the Making of the GATT Security Exceptions', (2020)41(1) *Michigan Journal of International Law* 109 (noting that the narrow interpretation of "emergency" is consistent with the drafting record of the security exception).

[127] Joshua Meltzer, 'Cybersecurity, Digital Trade, and Data Flows: Re-thinking a Role for International Trade Rules', Brookings Institution Working Paper 132 (May 2020) at 26, https://www.brookings.edu/wp-content/uploads/2019/11/Cybersecurity-digital-trade-data-flows.pdf. For a more detailed discussion of the limitation of GATS Article XIV*bis*, see Neha Mishra, 'The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance', (2020)54(4) Journal of World Trade 567.

[128] That is, the obligation of "good faith" stems from Article XXI as a whole rather than the sub-paragraphs. See above n 113, Panel Report, *Russia – Traffic in Transit*, paras. 7.132-33, 7.138.

[129] See above n 106, Burri and Kugler, at 420-21.

[130] The full text of the USMCA is accessible here: https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

[131] Ibid.

longer subject to additional legal conditions. As discussed above, while the *Russia – Traffic in Transit* decision would still impose an obligation of "good faith", the resultant minimum requirement of plausibility can be easily satisfied. Thus, the combination of the two developments significantly reduced the rigidity of security exceptions and expanded the scope of justifiable circumstances for data security measures. These developments have also been adopted in digital economy agreements such as the DEPA.[132] The enhanced policy space for data security is a clear response to the more liberal approaches to data flows and localization adopted in these agreements, thereby acting as a classic "safety valve" to enable progressive liberalization or more advanced rules on data.[133]

2. Developing Security Exceptions

While the WTO security exception tends to be overly restrictive on policy space, the recent developments in trade or digital economy agreements discussed above can lead to almost unfettered discretion for the application of data security measures. Neither of the two approaches can strike a desirable balance between trade and security. Faced with the rapid rise of data regulation worldwide and potential abuses of national security for digital industrial policy,[134] there is a pressing need to further develop the security exceptions to ensure legitimate use. Proposals for how to constrain the abuse of national security to protect trade liberalization and a rules-based trading system have flourished since *Russia – Traffic in Transit*.[135] Yet, detailed discussions on how best to design security exceptions for data regulation are developing slowly,[136] although some of the general proposals on security exceptions can also be useful for addressing the growing tensions between trade and data security. Below, we offer some preliminary thoughts on how to move forward negotiations of security exceptions for legitimate data protection.

Negotiation is far better than litigation, as Professor Bacchus rightly suggested.[137] Litigation can provide only certain degree of gap-filling while at the same time carrying the risk of judicial

---

[132] See above n 106, DEPA, art. 15.2.

[133] See WTO, *World Trade Report 2009: Trade Policy Commitments and Contingency Measures* (Geneva: WTO, 2009) 47. Some FTAs, such as the RCEP (art 12.17), also exclude digital trade obligations from dispute settlement, as an additional or alternative approach to safeguarding policy space. See also above n 20, Gao, 'Data Sovereignty and Trade Agreements: Three Digital Kingdoms', at 304-06. The full text of the RCEP is accessible here: https://www.dfat.gov.au/trade/agreements/in-force/rcep/rcep-text.

[134] See above n 90, OECD and WTO, at 14-18.

[135] See eg. Simon Lester and Huan Zhu, 'A Proposal for "Rebalancing" To Deal With "National Security" Trade Restrictions', (2019)42(5) Fordham International Law Journal 1451; Nicolas Lamp, 'At the Vanishing Point of Law: Rebalancing, Non-Violation Claims, and the Role of the Multilateral Trade Regime in the Trade Wars', (2019) 22(4) Journal of International Economic Law 721; James Bacchus, 'The Black Hole of National Security: Striking the Right Balance for the National Security Exception in International Trade', CATO Policy Analysis no. 936 (9 November 2022), https://www.cato.org/sites/cato.org/files/2022-11/policy-analysis-936.pdf; Mona Pinchis-Paulsen, 'Let's Agree to Disagree: A Strategy for Trade Security', (2022)25(4) Journal of International Economic Law 527; Warren Maruyama and Alan W Wolff, 'Saving the WTO from the National Security Exception' (Working Paper No 23-2, Peterson Institute for International Economics, May 2023), https://www.piie.com/publications/working-papers/2023/saving-wto-national-security-exception; Stephen Kho et al., 'The Conundrum of the Essential Security Exception: Can the WTO Resolve the GATT Article XXI Crisis and Save the Dispute Settlement Mechanism?', (2024)40(1) American University International Law Review 127.

[136] See eg. Harlan Grant Cohen, 'Nations and Markets', (2020)23(4) Journal of International Economic Law 793, 814-15; above n 127.

[137] See above n 135, Bacchus, at 11.

overreach.[138] Negotiation is the only way to address the existing legislative deficit and modernize security exceptions in response to contemporary challenges. However, the well-known difficulties in progressing and concluding negotiations on a multilateral basis mean that alternative approaches must be taken. The WTO itself has resorted to plurilateral initiatives for negotiations on emerging issues, including digital trade, to ensure the multilateral trading system stays up to date. Via the JSI, 91 WTO members concluded "a stabilised text" in July 2024[139] with a plan to seek adoption of it as a plurilateral agreement under Annex 4 of the WTO Agreement.[140] As far as data is concerned, the JSI text does not include the more advanced rules on cross-border data transfers and data localization as adopted in the CPTPP (Articles 14.11 & 14.13), the USMCA (Articles 19.11 & 19.12), and the DEPA (Articles 4.3 & 4.4). This outcome reflects the ongoing challenges for achieving more liberalized data-related rules among a significantly larger group of governments.[141] Thus, even plurilateral negotiations will take time and need to be progressed incrementally.

Nevertheless, negotiations on data security can help facilitate data liberalization. To do so, the negotiations need to involve detailed discussions of major security-related issues. One threshold question is whether a categorization of data is required. Not only academic work has proposed ways for data classification,[142] but new generation (digital) trade agreements, including those noted above, have also drawn a distinction between different types of data (e.g. government data, personal data, etc.). What is lacking in the current practice, however, is a dedicated discussion of how such data classifications would help develop exceptions to specifically address data security issues. Another threshold question is whether a classification of data holders or providers is needed,[143] as suggested by China's regulatory approaches relating to CIIOs discussed above. RCEP's security exceptions expanded GATT Article XXI by adding an exception for security measures taken for the protection of critical public infrastructures (Article 17.13(b)(iii)). This exception, however, is currently too broad and hence requires further negotiations to clarify the coverage of critical infrastructures, perhaps with a combination of a general list and country-specific lists to establish a commonly accepted baseline while allowing certain flexibilities for individual economies.

These threshold questions implicate a risk-based approach whereby the central issue concerns the likelihood or gravity of security risks *vis-à-vis* different types of data or data holders. Here, Professor Peng has observed a general trend of governments "moving toward risk-based approaches to protect national security and cybersecurity."[144] Indeed, such approaches have been

---

[138] For detailed discussions of the controversies about judicial overreach by the WTO Appellate Body, see eg. Weihuan Zhou and Henry Gao, ' 'Overreaching' or 'Overreacting'? Reflections on the Judicial Function and Approaches of WTO Appellate Body', (2019)53(6) Journal of World Trade 951.

[139] WTO, 'Joint Statement Initiative on Electronic Commerce', INF/ECOM/87 (26 July 2024).

[140] WTO, 'Information on the Agreement on Electronic Commerce', undated, https://www.wto.org/english/tratop_e/ecom_e/information_on_agreement_ecom.pdf, at 12.

[141] Submissions by JSI participants are accessible here, https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm. See also Nivedita Sen, 'Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?', (2018)21(2) Journal of International Economic Law 323, 339-41.

[142] See above n 141, Sen, at 343-46.

[143] For a detailed discussion of data security challenges associated with critical infrastructure and how to refine security exceptions through a distinction between critical and noncritical infrastructure, see Shin-Yi Peng, *International Economic Law in the Era of Datafication* (Cambridge: Cambridge University Press, 2024) Ch 2.

[144] Ibid., at 73.

incorporated into the USMCA (Article 19.15.2) and the JSI (Article 17.3) to facilitate cooperation on cybersecurity issues. A risk-based approach should also be used to advance negotiations on data security more broadly. At a systemic level, recent studies have suggested that the so-called "targeting rule" derived from the theory of distortions remains applicable to balancing trade and security interests by inquiring about whether a chosen policy instrument addresses a claimed security objective at its source.[145] Accordingly, this inquiry entails two key steps: (1) identifying the policy objective(s) and (2) assessing the appropriateness of the policy instrument(s). The identification of policy objectives necessarily involves an assessment of the security risks and the level of protection that a regulating government seeks to address or achieve. Understanding such risks and objectives provides the basis for evaluating the reasonableness of the chosen means. Where the CPTPP, USMCA and DEPA further liberalized cross-border data transfer and data localization requirements, they also adopted a broad exception to allow measures "necessary to achieve a legitimate public policy objective" as long as they do not cause "arbitrary or unjustifiable discrimination" or impose restrictions on data transfers or localization "greater than are necessary to achieve the objective".[146] Since security exceptions are independent from this exception, one may argue that data security does not fall within the ambit of the undefined "legitimate public policy objective". Nevertheless, the legal conditions contemplated in this exception, particularly the "necessity" and "arbitrary or unjustifiable discrimination" tests, provide a good start point for negotiating how to strengthen the connection between data restrictive measures and security goals beyond a minimum requirement of plausibility. In doing so, the intention is not to restrain the freedom of governments to address any perceived security risks or pursue any chosen security goals. Rather, negotiators should focus on developing mutual understanding of such risks and goals raised by their counterparts as well as reasons for adopting certain data restrictive measures. Despite the controversies over the "necessity" and "arbitrary or unjustifiable discrimination" tests,[147] they have been well developed through a large volume of cases and hence are better understood than any new tests. In our view, the existing case law on these tests is largely compatible with the economic principles derived from the theory of distortions in disciplining the use of protectionist policy instruments while preserving regulatory autonomy.[148] Thus, these tests can be further refined and elaborated to ensure data restrictive measures target security risks and objectives as directly as feasible to minimize abuses for protectionist or other strategic goals. To alleviate concerns about the potential rigidity of the "necessity" test, governments may consider adopting a country-specific negative list of non-conforming measures to accommodate different regulatory preferences, capacity constraints and other considerations.[149]

As negotiations take place, governments should continue to use existing committees and other venues under the WTO to discuss data security and regulatory practices to build transparency

---

[145] See generally Mona Pinchis-Paulsen, Kamal Saggi and Petros Mavroidis, 'The National Security Exception at the WTO: Should It Just Be a Matter of When Members Can Avail of it? What About How?', (2024)23(3) World Trade Review 271.

[146] See above n 106, CPTPP, art. 14.11.3 & 14.13.3; DEPA, art. 4.3.3 & 4.4.3, above n 130, USMCA, art. 19.11.2.

[147] See eg. Magdalena Słok-Wódkowska and Joanna Mazur, 'Between Commodification and Data Protection: Regulatory Models Governing Cross-border Information Transfers in Regional Trade Agreements', (2024)37(1) Leiden Journal of International Law 111, 129-30.

[148] See generally Weihuan Zhou, 'In Defense of the WTO: Why Do We Need A Multilateral Trading System', (2020)47(1) Legal Issues of Economic Integration 9.

[149] For an example of non-conforming measures, see above n 106, CPTPP, Chapter 17-Annex IV.

and trust and manage unilateral actions and potential trade tensions via concerted effort.[150] Enhanced understanding of (data-related) security goals and regulatory tools and increased trust among governments are crucial for modernizing (data) security exceptions. The development of such exceptions would provide legal clarity on the availability of policy space as agreed by all governments involved. To the extent such development adds constraints on governments' discretions in recourse to national security, it would also provide more certainty on the enforceability of data liberalization commitments. It is from such positive spillovers of progressing negotiations on data security that progressive data liberalization may also be attained.

V. CONCLUSION

Industrial policy is no longer confined to economic efficiency or competitiveness but has been increasingly motivated by a mix of economic and non-economic goals particularly national security. This is especially so in the digital domain as governments compete for digital industrialization. While China's digital transformation has embraced ambitious industrial policies and rigorous security protection, our analysis of China's regulatory framework for data has revealed little evidence to suggest that China has (ab)used security measures to foster its data sector at the cost of foreign competitors. Rather, China's approaches to data security are reasonably balanced by targeting genuine security risks and incrementally streamlining regulatory checks and requirements. Yet, major loopholes remain in China's regulatory framework, which provide room for discretion and abuse in data security reviews. Faced with escalating geopolitical tensions and burgeoning security-based trade or investment restrictions, China's recourse to similar restrictions on security grounds is not a remote possibility. A looming data trade war in the name of national security would harm all economies as well as the rules-based global trading system they jointly built. The security exceptions under existing trade or digital economy agreements can hardly strike a proper balance between data liberalization and security. Governments should join forces to modernize these exceptions, ideally via the multilateral forum provided by the WTO for coordinated and inclusive discussions. Such discussions and negotiations would in turn promote progressive data liberalization by bringing about enhanced clarity and certainty on rebalanced rules and exceptions on data security measures. Policy space is essential in this balancing act, but a right balance cannot be achieved with security exceptions that are either overly deferential or excessively restrictive.

[150] For detailed discussions of how WTO committees can be used for governments to deliberate on trade-security issues, see above n 135, Pinchis-Paulsen.

Contact us:

cibel@unsw.edu.au

linkedin.com/showcase/unsw-cibel/

@ CIBELUNSW