

China's Evolving Data Governance Regime

With China's ambitions to become a leader in the digital economy by 2025 and a "cyber superpower," data governance has been a top priority for Chinese policymakers.¹ Beijing sees that sustaining economic growth and leading in global innovation requires expanding and protecting China's digital capabilities, both for digitally-enabled trade in goods and provision of digital services, which account for an increasing proportion of overall economic activity. In addition to the economic benefits of a secure digital economy, maintaining "cybersovereignty" is important for Chinese policymakers in carving out new legal and regulatory systems. Contrary to the U.S. vision of a free and open internet, upholding cybersovereignty means that cyberspace, data, and networks are regarded as sovereign territory subject to local laws of individual countries.² This concept is critical to the Chinese Communist Party's (CCP) strategy to maintain information control, political stability, and limitations on expression of popular dissent.

While some of China's protections on data appear similar to those in other countries, they are generally more restrictive. Since the passage of China's Cybersecurity Law in 2017, the Chinese government has been creating an expansive thicket of laws, regulations, and technical standards related to the collection, sharing, commercialization, and protection of data. The Chinese government is developing more specific regulations and standards in sectors of particular concern, such as finance and transportation. China has also implemented more restrictive data protection and cybersecurity rules for government and national-security related data.

China's development of its data governance regime is also part of a broader CCP strategy to influence global data governance norms. Many of China's data-related measures encourage China's "formulation of international rules and standards."³ In September 2020, Chinese Foreign Minister Wang Yi presented a Global Initiative on Data Security, which Foreign Ministry spokesman Zhao Lijian characterized as "contributing China's wisdom to international rules-making" for data.⁴ The initiative has since been endorsed by leaders from Tanzania, the Philippines, Russia, and Ecuador. In March 2021, China signed a "Cooperation Initiative on Data Security" with the Arab League.⁵ The initiative urges countries not to weaponize the use of data while also encouraging cybersovereignty and local data storage—policies that have raised concerns among human rights experts as well as U.S. tech firms.⁶ Authoritarian or illiberal governments are increasingly interested in these types of cybersovereignty-based policies, as they can be used to seize data and computing equipment for vaguely-defined "national security" purposes, jeopardizing the protection of civil and intellectual property rights.⁷

China's data governance regime stands to increase fragmentation of global data policies and the digital economy. Running counter to the free flow of data approach favored by the United States and many democratic countries, Chinese policy positions clearly appeal to certain governments around the world. Vietnam's cybersecurity law, adopted in 2019, mirrors the 2017 Chinese law. Similarly, the military junta in Myanmar has recently proposed a draft cybersecurity law that has clearly drawn from its Chinese counterpart.⁸ While China's approach to data has influenced some of its closest neighbors, it has also produced friction in regional forums. China has historically refused to sign onto the Asia Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules, which it claims is a U.S.-led initiative to hoard data, and subsequently has hampered consensus-

* The Arab League consists of 22 members: Algeria, Bahrain, Comoros, Djibouti, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Mauritania, Morocco, Oman, Palestine, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, the United Arab Emirates, and Yemen. Syria's membership is currently suspended while Brazil, Eritrea, India, and Venezuela are observer countries. Imad K. Harb, "Syria's Return to the Arab League Is Imminent," *Arab Center Washington DC*, October 5, 2021. <https://arabcenterdc.org/resource/syrias-return-to-the-arab-league-is-imminent/>; Museum with No Frontiers, "About the League of Arab States | Member States." <https://www.museumwnf.org/league-of-arab-states/?page=LAS-member-states.php>.

building within APEC on other digital economy work.⁹ Under the Regional Comprehensive Economic Partnership (RCEP), China's insistence against explicit prohibitions on data transfer restriction and protections on source code was a key contention with the governments of Japan and Singapore, which have enshrined protections on source code and free flows of data in other agreements.¹⁰ As a result of this difference, RCEP includes both a broad principle on protecting the free flow of data and a broad exception for governments to create restrictions where a member may deem it "necessary to achieve a legitimate public policy objective."¹¹ China's membership in RCEP and growing trade relationships in the region may lend it greater influence in the coming years as ASEAN builds out a data governance regime.

The United States is leading a digital agenda with allies and partners to incorporate a broad set of economic and security concerns. Under the U.S.-EU Trade and Technology Council, both sides are moving forward with specific working groups on technology standards cooperation and data governance and technology platforms.[†]¹² Similarly, the Biden Administration's Indo-Pacific Economic Framework includes negotiations on the digital economy as well as digital and emerging technologies.¹³ The United States has already cemented certain policies on cybersecurity capacity building, cross-border data flows, and online consumer and data privacy protections through commitments in the U.S.-Mexico-Canada Agreement, in the U.S.-Japan Digital Trade Agreement, and under the Trans-Atlantic Data Privacy Framework signed with the European Commission.[‡]¹⁴ The United States is also a strong supporter of APEC's Cross-Border Privacy Rules and several initiatives at the WTO aimed at reducing barriers to digital trade and e-commerce.

[†] Seven of the ten working groups under the U.S.-EU Trade and Technology Council center on rules and norms of digital technologies and digital trade: (1) tech standards, (2) information and communications technology and services (ICTS) security and competitiveness, (3) data governance and tech platform regulation, (4) misuse of technology threatening security and human rights, (5) export controls, (6) promoting SME access to and use of digital technologies, and (7) global trade challenges. Chad P. Bown and Cecilia Malmström, "What is the U.S.-EU Trade and Technology Council? Five Things You Need to Know," *Peterson Institute for International Economics*, September 24, 2021. <https://www.piie.com/blogs/trade-and-investment-policy-watch/what-us-eu-trade-and-technology-council-five-things-you-need>.

[‡] Signed with the European Commission in March 2022, the Trans-Atlantic Data Privacy Framework replaces the earlier Privacy Shield Framework and more closely adheres to EU legal standards stemming from its General Data Protection Regulation. White House, "FACT SHEET: United States and European Commission Agree on Trans-Atlantic Data Privacy Framework," March 25, 2022. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/>.

Table: Key Chinese Measures and Norms on Data Governance

Title	Purpose	Date
Cybersecurity Law	Establishes general security practices and authorities over cybersecurity matters; security process requirements and reviews for all organizations in China, including broad liabilities; restrictions on cross-border data transfer; and a framework for implementing regulations specific to critical sectors and information. ¹⁵	Effective June 2017
Measures for the Administration of Scientific Data	Restricts overseas access to scientific data by foreign investors in China; limits joint research by Chinese and foreign partners; and requires government review for cross-border transfer of scientific data. Scientific data such as basic and applied research generated through government funding must be reported directly to government entities. ¹⁶	Effective March 2018
E-Commerce Law	Establishes a registration system for e-commerce platforms, third-party sellers, and individual sellers; provides consumers the option to decline targeted marketing and search options. ¹⁷	Effective January 2019
Encryption Law	Establishes three encryption categories with different levels of protection and use; a testing and certification system for encryption, some of which must go through an accredited body; and an import licensing system and export controls for national security-related commercial encryption. ¹⁸	Effective January 2020
Opinions on Strictly Cracking Down on Illegal Securities-Related Activity in Accordance with Law [§]	Calls for stronger supervision and enforcement of cross-border listings, including improvement of laws and regulations related to data security, transfer, and management involved in such listings. ¹⁹	Published July 2021
Several Provisions on the Management of Automobile Data Security (Trial)	Outlines obligations for organizations on the collection, protection, sharing, and use of data collected by automobiles. ²⁰	Effective August through October 2021

[§] “Opinions” and “Guiding opinions” are policy circulars issued by the CCP Central Committee, State Council, their general offices, or State Council line ministries and ministry-level agencies that outline central government guidance and objectives, but are not legally binding. In practice, however, Opinions have become a primary mechanism for mobilizing Chinese government agencies and subnational governments. State Council of the People’s Republic of China, *Measures for the Disposal of Official Documents of State Administrative Organs* (国家行政机关公文处理办法), August 24, 2000. http://webcache.googleusercontent.com/search?q=cache:pND7Ysmp05gJ:www.gov.cn/gongbao/content/2000/content_60454.htm+&cd=1&hl=en&ct=clnk&gl=us.

Data Security Law	Establishes a system of data classification and obligations for organizations handling data, including security requirements and assessments for its protection, collection, use, and transfer domestically and overseas. ²¹	Effective September 2021
Personal Information Protection Law	Similar to the EU’s General Data Protection Regulation, yet more restrictive, the law establishes rights to personal information for all individuals in China and obligations for organizations handling personal information for its protection, collection, use, and transfer domestically and overseas. ^{** 22}	Effective November 2021
Cybersecurity Review Measures	Outlines security review procedures for operators of critical information infrastructure and organizations handling data sensitive to national security, including IPOs and organizations handling data of more than one million users. ²³	Revision effective February 2022 ^{††}
Internet Information Service Algorithmic Recommendation Management Provisions	Establishes new security, privacy, and content management rules for internet services that rely on algorithmic recommendations. Providers allow consumers greater control to enable or disable algorithmic recommendations. ²⁴	Effective March 2022
Security Assessment Measures on the Cross-Border Transfer of Data	Specifies when any organization handling data is required to undergo a security assessment from the national cybersecurity and informatization department to transfer data across Chinese borders, relying first on a self-assessment. ²⁵	Effective September 2022

Source: Compiled by Commission Staff.

^{**} The law also triggered the development of other subordinate regulations, including draft rules for regulations on the management of human genetic resources in March 2022 and draft provisions on standard contracts for the export of personal information in June 2022. The draft provisions are similar to the EU’s standard contractual clauses, which prescribes the design of contracts allowing organizations to transfer information across borders into another jurisdiction. The draft provisions differ from their EU counterparts by placing additional requirements on organizations within China and on foreign receivers of transferred data. Gabriela Kennedy and Joshua T.K. Woo, “(Not So) Standard Contracts? Draft Standard Contracts Finally Released in China,” *Mayer Brown*, July 13, 2022. <https://www.mayerbrown.com/en/perspectives-events/publications/2022/07/not-so-standard-contracts-chinas-draft-standard-contractual-clauses-secs-are-finally-released>.

^{††} The Cybersecurity Administration of China released a new draft of the Cybersecurity Review Measures in July 2021 but added several amendments to the draft later that month, including the one million user threshold.

Endnotes

- ¹ Rogier Creemers et al., “Translation: 14th Five-Year Plan for National Informationization – Dec. 2021,” *DigiChina*, January 24, 2022. <https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/>.
- ² Justin Sherman, “The Long View of Digital Authoritarianism,” *New America*, June 20, 2019. <https://www.newamerica.org/weekly/long-view-digital-authoritarianism/>.
- ³ Graham Webster, “Translation: Data Security Law of the People’s Republic of China,” *DigiChina*, June 29, 2021. <https://digichina.stanford.edu/news/translation-data-security-law-peoples-republic-china>.
- ⁴ Shannon Tiezzi, “China’s Bid to Write the Global Rules on Data Security,” *Diplomat*, September 10, 2020. <https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/>.
- ⁵ Chaeri Park, “Knowledge Base: China’s ‘Global Data Security Initiative’ 全球数据安全倡议,” *DigiChina*, March 31, 2022. <https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/>.
- ⁶ Shannon Tiezzi, “China’s Bid to Write the Global Rules on Data Security,” *Diplomat*, September 10, 2020.
- ⁷ Adrian Shahbaz and Allie Funk, “The Pandemic’s Digital Shadow,” *Freedom House*, 2020. <https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow>.
- ⁸ Cyber Security Law (Draft) (Myanmar), 2022. https://www.hrw.org/sites/default/files/media_2022/02/220127%20Cyber-Security-Bill-EN.pdf
- ⁹ Nigel Cory, “Writing the Rules: Redefining Norms of Global Digital Governance,” *China’s Digital Ambitions: A Global Strategy to Supplant the Liberal Order*, National Bureau for Asian Research, March 2022, 84. https://www2.itif.org/2022-NBRsr97-china-digital-ambitions.pdf?_ga=2.204751381.480101597.1652729267-2102500758.1652729267#page=79.
- ¹⁰ Oki Nagai, “Japan Teams with RCEP Allies to Push China on Data Free Flow,” *Nikkei Asia*, December 30, 2020. <https://asia.nikkei.com/Economy/Trade/Japan-teams-with-RCEP-allies-to-push-China-on-data-free-flow>.
- ¹¹ Article 12.15, Regional Comprehensive Economic Partnership. <https://rcepsec.org/wp-content/uploads/2020/11/Chapter-12.pdf>.
- ¹² U.S. Department of State, “U.S.-EU Trade and Technology Council.” <https://www.state.gov/u-s-eu-trade-and-technology-council-ttc/>.
- ¹³ U.S. Department of Commerce, “Request for Comments on the Indo-Pacific Framework,” *Federal Register* 87:13971 (March 11, 2022). <https://www.federalregister.gov/documents/2022/03/11/2022-05206/request-for-comments-on-the-indo-pacific-economic-framework>; Office of the U.S. Trade Representative, “Request for Comments on the Proposed Fair and Resilient Trade Pillar of an Indo-Pacific Economic Framework,” *Federal Register* 87:13789 (March 10, 2022). <https://www.federalregister.gov/documents/2022/03/10/2022-05044/request-for-comments-on-the-proposed-fair-and-resilient-trade-pillar-of-an-indo-pacific-economic>.
- ¹⁴ White House, “FACT SHEET: United States and European Commission Agree on Trans-Atlantic Data Privacy Framework,” March 25, 2022. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/>.
- ¹⁵ Rogier Creemers, Graham Webster, and Paul Triolo. “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017),” *DigiChina*, June 29, 2018. <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>.
- ¹⁶ Lester Ross, Kenneth Zhou, and Tao Xu, “China Expands Access to Scientific Data Domestically, Imposes Restrictions on Export of Scientific Data,” *Wilmer Hale*, April 20, 2018. <https://www.wilmerhale.com/en/insights/client-alerts/2018-04-26-china-expands-access-to-scientific-data-domestically-imposes-restrictions-on-export-of-scientific-data>.
- ¹⁷ IP Key, *E-Commerce Law of the People’s Republic of China*, 2018, https://ipkey.eu/sites/default/files/documents/resources/PRC_E-Commerce_Law.pdf.
- ¹⁸ Adam Segal, “The Encryption Debate in China: 2021 Update,” *Carnegie Endowment for International Peace*, March 31, 2021. <https://carnegieendowment.org/2021/03/31/encryption-debate-in-china-2021-update-pub-84218#:~:text=As%20the%20country's%20first%20law,in%20China%20as%20state%20secrets..>

-
- ¹⁹ The General Office of the Central Committee of the Communist Party of China and the General Office of the State Council, *Opinions on Strictly Crackdown on Securities Illegal Activities in accordance with the Law* (关于依法从严打击证券违法活动的意见), July 2021. Translation. http://www.gov.cn/zhengce/2021-07/06/content_5622763.htm.
- ²⁰ Cyberspace Administration of China, *Several Provisions on Car Data Security Management (Trial)* (汽车数据安全若干规定 (试行)), August 20, 2021. Translation. http://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm.
- ²¹ Graham Webster, “Translation: Data Security Law of the People’s Republic of China,” *DigiChina*, June 29, 2021. <https://digichina.stanford.edu/news/translation-data-security-law-peoples-republic-china>.
- ²² Alexander Chipman Koty, “Personal Data Regulation in China: Personal Information Protection Law, Other Rules Amended,” *China Briefing*, May 13, 2021. <https://www.china-briefing.com/news/personal-data-regulation-in-china-personal-information-protection-law-other-rules-amended/>.
- ²³ Rogier Creemers and Graham Webster. “Translation: Cybersecurity Review Measures (Revised) – Effective Feb. 15, 2022,” *DigiChina*, January 10, 2022. <https://digichina.stanford.edu/work/translation-cybersecurity-review-measures-revised-effective-feb-15-2022/>.
- ²⁴ Rogier Creemers, Graham Webster, and Helen Toner, “Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022,” *DigiChina*, January 10, 2022. <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/>.
- ²⁵ Rogier Creemers et al., “Translation: Outbound Data Transfer Security Assessment Measures – Effective Sept. 1, 2022,” *DigiChina*, July 8, 2022. <https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022>.