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. 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. 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.” 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. 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.* 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. 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.

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. 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-

building within APEC on other digital economy work. 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. 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.” 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. Similarly, the Biden Administration’s Indo-Pacific Economic Framework includes negotiations on the digital economy as well as digital and emerging technologies. 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. 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.

---


Table: Key Chinese Measures and Norms on Data Governance

<table>
<thead>
<tr>
<th>Title</th>
<th>Purpose</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Law</td>
<td>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.</td>
<td>Effective June 2017</td>
</tr>
<tr>
<td>Measures for the Administration of Scientific Data</td>
<td>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.</td>
<td>Effective March 2018</td>
</tr>
<tr>
<td>E-Commerce Law</td>
<td>Establishes a registration system for e-commerce platforms, third-party sellers, and individual sellers; provides consumers the option to decline targeted marking and search options.</td>
<td>Effective January 2019</td>
</tr>
<tr>
<td>Encryption Law</td>
<td>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.</td>
<td>Effective January 2020</td>
</tr>
<tr>
<td>Opinions on Strictly Cracking Down on Illegal Securities-Related Activity in Accordance with Law§</td>
<td>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.</td>
<td>Published July 2021</td>
</tr>
<tr>
<td>Several Provisions on the Management of Automobile Data Security (Trial)</td>
<td>Outlines obligations for organizations on the collection, protection, sharing, and use of data collected by automobiles.</td>
<td>Effective August through October 2021</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Data Security Law</strong></th>
<th>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.</th>
<th>Effective September 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Information Protection Law</strong></td>
<td>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.</td>
<td>Effective November 2021</td>
</tr>
<tr>
<td><strong>Cybersecurity Review Measures</strong></td>
<td>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.</td>
<td>Revision effective February 2022</td>
</tr>
<tr>
<td><strong>Internet Information Service Algorithmic Recommendation Management Provisions</strong></td>
<td>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.</td>
<td>Effective March 2022</td>
</tr>
<tr>
<td><strong>Security Assessment Measures on the Cross-Border Transfer of Data</strong></td>
<td>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.</td>
<td>Effective September 2022</td>
</tr>
</tbody>
</table>

*Source: Compiled by Commission Staff.*


†† 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


