hinrich foundation
advancing sustainable global trade

MERICS

DECEMBER 2023

China's data management: Putting the party-state in charge

BY REBECCA ARCESATI AND JEROEN GROENEWEGEN-LAU

About MERICS

The Mercator Institute for China Studies (MERICS) was founded in 2013 by the German Stiftung Mercator to strengthen knowledge and debate about China in Germany and Europe. With international researchers from Europe, the United States and Australia, MERICS is currently the largest European research institute focusing solely on the analysis of contemporary China and its relations with Europe and the wider world. Our specialists have a wide range of expertise on China, scientific qualifications and methodological skills. With its main premises in Berlin, MERICS also operates an office in Brussels.

Contents

Introduction

Both security and growth imperatives have persuaded China's leaders that the market alone cannot handle data safely and efficiently; the party-state is firmly in charge of all key levers of policy and society in China.

Tight restrictions on cross-border data flows, coupled with vague legal stipulations that empower Chinese officials to request access to company data, are making China less attractive to foreign businesses. European industry associations and government delegations alike have repeatedly sounded the message to China's government that its data laws are driving a costly economic decoupling.[1] With China accounting for as much as 23% of transnational data flows,[2] and data-driven technologies such as artificial intelligence (AI) increasingly transforming traditional economic sectors and business models, Beijing's stringent data localization requirements have sweeping implications for global trade, investment, and innovation.

Chinese policymakers and regulators appear to be listening.[3] Amid a dire outlook for the domestic economy, the Cyberspace Administration of China (CAC) in October issued a major set of draft rules which, if implemented, would walk back key aspects of its security-first approach to cross-border data management.[4] It is too soon to evaluate the extent, impact, or longevity of this policy reversal. Implementation will be key. It is instead paramount to place it within a wider context. Both security and growth imperatives have persuaded China's leaders that the market alone cannot handle data safely and efficiently; the party-state is firmly in charge of all key levers of policy and society in China.

In fact, China's data governance regime is undergoing a shift toward a more decisively top-down management of data resources. Also in October, China launched its National Data Administration (国家数据局, NDA), tasked with

Tight restrictions on cross-border data flows and vague legal stipulations that empower officials to request access to company data are making China less attractive to foreign firms. (Image: AP)

promoting data utilization, development, and circulation.[5] This institutionalizes regulations for a more centralized state management of data that the Chinese Communist Party (CCP) Central Committee and the State Council issued in December 2022.[6] After repeated and largely unsuccessful attempts at tearing down so-called data islands, or silos, many of which sit within government departments and state-owned utility firms, Beijing is trying again—this time with greater resolve.

The regulatory and institutional overhaul of China's data governance framework over the past six years frames Beijing's efforts to harness data as a national resource and a factor of production. Beijing issued several laws and regulations, most notably the 2017 Cybersecurity Law as well as the Data Security Law (DSL) and Personal Information Protection Law (PIPL) of 2021. Although this regulatory edifice is now more or less in place, a lot of key details remain unclear. China also traditionally has a gap between regulations and their implementation.[7] This paper seeks to shed light on this gap by considering both regulations and institution-building at the national level and in specific sectors: the emerging mechanics of China's data management.

Overall, Beijing has considerably strengthened its control and visibility over China's data flows through party and state agencies like the Cyber Administration of China (CAC) and the National Development and Reform Commission (NDRC), as well as through a range of data exchanges, platforms, and clearinghouses that sit in strategic positions in China's financial, economic, industrial, and social structures. Campaigns and investigations show how regulations and institutions come together to correct any divergence, as perceived by Beijing, from progress towards a Cyber Great Power (网络强国) and a Digital China (数字中国). Increasingly, privately owned Chinese and foreign firms alike must navigate intrusive party-state control over data transfers, both within China and across borders.

The regulatory and institutional overhaul of China's data governance framework over the past six years frames Beijing's efforts to harness data as a national resource. (Image: Reuters)

State-controlled actors provide visibility and control

In healthcare and education, the government issued regulations to empower state-controlled actors at the expense of privately owned platforms for remote healthcare and digital education services.

A key component of Beijing's efforts to control data flows is that it installs actors that it has control over at strategic positions in the digital ecosystem.

The CAC, which drafts most data-related regulations, was established in 2011. In 2016, China's central bank, the People's Bank of China (PBoC), approved the establishment of Wanglian (网联) and required all digital payments to be routed through this clearinghouse. Ostensibly prompted by concerns over systemic risks from financial technology, the central bank extended this approach to an attempt at crafting a national system of individual credit ratings. Several years after announcing individual credit rating services would need to obtain permits to operate, the PBoC made this requirement official in October 2021.[8]

Because only the state-controlled firms Baihang (百行征信) and Pudao (朴道征信) have been able to obtain such a permit, the policy forces the micro-lending sector to run through state-controlled entities. It outlawed financial platform Ant Group's lending services which had been based on scores from Sesame Credit, the private credit rating agency owned by Ant Group. The data that this credit score is based on, such as Alibaba's e-commerce and Ant Group's payment data, is now to be submitted to China's two official personal credit rating agencies Baihang and Pudao.[9]

This is part of a larger trend. China's Ministry of Transportation wants a nationally integrated "data brain" to be basically in place by 2025, according to its Digital Transportation Five-Year Plan (2021-2025).[10] To make China a transportation power and improve government administration, the plan calls for real-time data on public roads, railways, airlines, and waterways to be integrated into a national information platform, and for a large network of supporting data centers. Progress at the national level is slow, but several major cities have built platforms to integrate this data, most notably Shanghai, Guangzhou, and Chongqing.

Didi Chuxing, China's leading ride-hailing service, has initiated collaboration with several of these projects. However, Didi's ambition to be the driving force behind developing smart transportation services was eviscerated when in June 2022 Chinese regulators forced the company to delist from the New York Stock Exchange, after it allegedly endangered China's data security and mishandled personal information.[11] Like Ant Group, Didi had in the past irked Chinese authorities by refusing to share its consumer data, specifically in the context of criminal investigations.[12] Moreover, Didi was deemed a critical information infrastructure operator (CIIO), indicating that Beijing regarded the company's vast data troves as a matter of national security.[13]

In healthcare and education, the state similarly issued regulations to empower state-controlled actors at the expense of privately owned platforms for remote healthcare and digital education services. The National Health Commission in 2018 required all digital healthcare services to work with physical hospitals, curtailing the advance of platform companies.[14] These examples show that the transfer of power over data flows from private to state control pre-dates the regulatory and enforcement campaign that amplified Beijing's dominance over China's tech sector

in 2020-2022, and should therefore be seen as a long-term systemic feature of Beijing's data governance model.

State-controlled data clearinghouses and similar entities are hybrid in nature and best understood as trusted actors. Their loyalty to the state goes before anything else, but to be effective they also need to remain at least somewhat responsive to market demands. Although government policy for financial technology, transportation, digital healthcare, and education is often framed as promoting innovation, Beijing is aware that state-affiliated institutions struggle to deliver on this account. As a result, trusted actors tend to be spun-out subsidiaries of semi-public organizations (banks, public transport operators, utility companies, hospitals, public universities) and/or private firms with close government ties as indicated by company leadership and ownership structures.

In the case of individual credit ratings, the two officially accredited firms, Baihang and Pudao, are not straightforward subsidiaries of the central bank or any other state institution. But both organizations are led by former PBoC officials and majority-owned by state-owned investors.[15] Private interests can hold only minority stakes in these entities. This attempt to co-opt private ownership has not led to a straightforward success. Baihang and Pudao have not been able to improve upon credit rating services previously provided by private tech firms, as these are much better integrated in their financial and related services. Private firms have been reluctant to share data with the state that supports some of their core products.

In remote healthcare, the 2018 regulations led to a fragmentation of digital healthcare services. Prior to the rule, tech firms were gaining bargaining power over doctors and hospital administrators, especially in smaller cities, which raised concerns in Beijing. But innovation in this space is now led by hospitals, for which telemedicine is not a top priority. This has slowed progress in digital healthcare: though 1,600 e-hospitals were set up by 2021, 90% are not being used.[16]

These examples show how the state struggles to promote innovation even as it frames its measures within this rubric. Since 2014, Beijing has consistently pursued both cybersecurity (网络安全) and informatization (信息化) as two pillars of China's top leader Xi Jinping's vision for China as a Cyber Great Power.[17] However, for Beijing, security comes first. Cybersecurity is interpreted extensively to encompass any harm posed to the country's security—with the regime's political security at the top—through networks, data, or information. Nevertheless, within these parameters, government agencies are promoting data trading and the digital economy more generally to develop China's economy. The National Data Administration, which embodies this effort, sits at the pinnacle of a wider set of institutions.

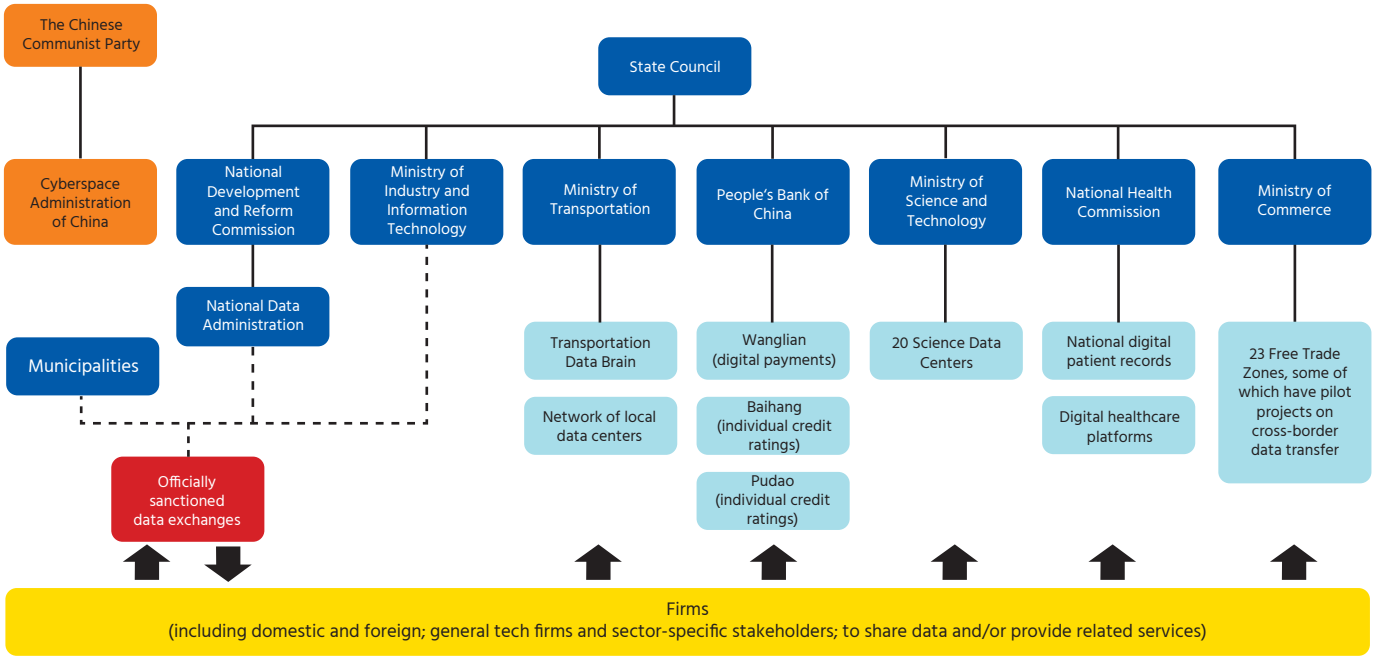
Beijing's control of data trade

In a growing number of sectors, domestic and foreign firms must interact with state agencies and their trusted actors on issues relating to data storage, sharing, trading, and use. Data security is the main focus of this interaction, but promoting data circulation is gaining importance in official discourse. The Data Security Law (DSL) makes it clear that non-sensitive data is to circulate freely in a "data exchange market" to make domestic governance more efficient and the economy more productive.[18] By devoting almost equal space to data development and security, the DSL codifies President Xi Jinping's vision that "cybersecurity and informatization are two wings of a single body and two wheels of a single drive."[19]

Since the Fourth Plenum of the 19th CCP Central Committee in 2019 designated data a "factor of production" alongside land, labor, capital, and technology, a number of top-level policies have called for a better integrated and more efficient data market in China.[20] These include the 14th Five-Year Plan for China's socioeconomic development, as well as sectoral plans for national informatization, the digital economy, and Big Data development.[21] By 2025, the digital economy is to account for 10% of national gross domestic product, up from 7.8% in 2020, while a functional data trading system shall be in place, the plan says.[22]

Such growth requires building out China's data circulation institutions and wider ecology (see Figure 1). Next to the trusted actors outlined in the previous section,

Figure 1 – Schematic overview of China's emerging data circulation ecology



Source: MERICS

By devoting almost equal space to data development and security, the Data Security Law codifies President Xi's vision that "cybersecurity and informatization are two wheels of a single drive."

data exchanges will play a key facilitating role. These operate like marketplaces where data and related products can be queried, developed through third-party services, or traded like commodities. Mindful of a graveyard filled with predecessor institutions, the current slate of exchanges in Beijing, Shanghai, Guizhou, and Shenzhen since 2021 all operate under tight government supervision and coordination. For instance, the Guiyang Big Data Exchange was a frontrunner when it was set up as a private enterprise in 2015. However, it was restructured in 2021, becoming 100% state-owned.[23]

Beijing says firmer state control is aimed at addressing the mishandling of personal information and security-sensitive data, as well as China's rampant data black market. But it is also a manifestation of Beijing's impatience with private data-collecting monopolies and lack of supervision, which policymakers believe are preventing data flows from upgrading traditional sectors such as manufacturing. Nearly every data-related policy announcement urges companies to "properly handle the relationship between the government and the market, give full play to the decisive role of the market in resource allocation, and optimize the [supporting] role of government guidance and regulation."[24]

At the national level, several institutions shape the overall policy framework. Overseeing this work is the newly created National Data Administration (NDA) under the authority of China's top planning agency, the National Development and Reform Commission (NDRC). While the Cyberspace Administration of China remains firmly in charge of security and data protection (in collaboration with other organs), the NDA is responsible for tasks such as planning and coordinating the digital transformation of public services, society, and the economy as well as managing China's data resources to promote their use and circulation.[25] This ostensibly formalizes a division of labor between security- and development-focused data governance.

The creation of the NDA is also a response to the regional fragmentation that has long hampered China's efforts to make use of its rich data resources, especially those that sit unused within government departments and state-owned enterprises. Prior to the reform, responsibility was fragmented over about 15 local administrations, with limited coordination.[26] However, this is unlikely to end the turf wars that are common in China's policymaking. The DSL requires sectoral regulators to issue catalogs of 'important' and 'core' data—the backbone of a hierarchical, risk-based data classification regime which aims to set strict boundaries for domestic and cross-border data circulation. This leads to an in-built competition between 'protect' and 'promote' imperatives, as well as a patchwork of interlocking and sometimes overlapping regulations and bureaucratic interests.

For example, companies in the industrial, telecommunications, and radio sectors that handle data must answer to the Ministry of Industry and Information Technology (MIIT). They need to set up cumbersome structures and processes to secure data throughout its lifecycle, including detailed requirements for filing, data security monitoring, risk assessment, and emergency management.[27] On top of its security-related responsibilities, the MIIT is also backing some of the officially sanctioned data exchanges, such as the Shanghai Data Exchange. This leads to competition with both the CAC and the NDRC, adding to confusion for companies. Another powerful agency is the Ministry of Science and Technology (MOST), which oversees data management and cross-border transfer in important areas such as scientific research results and human genetic resources data from clinical trials in China.

Cross-border data flows viewed as security threat by default

As a national asset and a key production factor in China's "socialist market economy", in Beijing's view, data should above all support the economic development strategy of internal (domestic) "circulation". This strategy prioritizes economic security and self-reliance to minimize the country's exposure to external shocks.[28] As a result, sweeping yet vague localization requirements have been in place since the Cybersecurity Law (CSL) came into force in 2017—and even prior to that in some sectors—compelling multinationals from Apple to Tesla to set up local storage facilities and fueling a de-facto decoupling in data operations.[29] But until recently, these requirements were not consistently enforced. Now that most implementing regulations and standards are in place, companies need to navigate a more predictable but also increasingly rigid data management regime.

This comes as China's regulators are obscuring from foreign eyes more and more national data, ranging from shipping data and corporate registries to academic literature and economic statistics.[30] China's Ministry of State Security investigated 3,000 meteorological stations in 2023 for sending data overseas.[31] Behind this trend is a securitized approach to data and information, which was applied in the Didi case, when regulators revised the Cybersecurity Review Measures and explicitly linked overseas listings with the risk of data being accessed, controlled, or manipulated by foreign governments.[32] This security-centric approach has also led the CAC to drag its feet on or deny most requests for data export permits, seeing any cross-border data transfer as an unnecessary risk best avoided.

In Beijing's view, data should above all support the economic strategy of domestic "circulation", which prioritizes self-reliance to minimize the country's exposure to external shocks. (Image: ImagineChina)

In Beijing's view, data should foremost support the economic development strategy of internal (domestic) "circulation". As a result, sweeping yet vague data localization requirements have been put in place.

The intricacy of regulatory approvals for outbound data transfer goes back to the principle of data classification: The DSL creates a comprehensive architecture of systems for securing all of China's data, centered on a graded, hierarchical categorization according to the risk data could pose to China's national security, socioeconomic development, and public interest when leaked, falsified, destroyed, mishandled, or illegally appropriated. Overseen by the National Security Commission of the CCP Central Committee, this is the security shield of China's digital sphere. Cross-border flows of personal information, sensitive personal information, and so-called important and core data are only permissible under certain circumstances.

In terms of personal information, the PIPL governs not only the power relations between data handlers and the individuals whose data they collect and process—for example by limiting internet platforms' ability to engage in algorithmic micro-targeting of users—but also how Chinese and foreign actors may transfer personal information out of the country. Several mechanisms are legally possible: an international agreement with another jurisdiction (though China has yet to sign any), certification by a licensed institution, and Standard Contracts, the latter resembling in part a mechanism under the European Union's General Data Protection Regulation (GDPR).[33] In other cases, a security review by the CAC is necessary.

The security review process has been a major concern for foreign firms operating in China since the CSL went into effect in 2017. More clarity on this key piece of the cross-border data transfer puzzle came when the CAC in July 2022 released its Outbound Data Transfer Security Review Measures.[34] The measures, which came into effect in September last year, mandate a risk self-assessment followed by a CAC-led one, in the following cases:[35]

- The data being transferred contains important data;
- A CIIO or an entity handling the personal information of more than a million Chinese citizens seeks to export personal information;
- A data handler has exported the cumulative personal information of more than 100,000 people or the sensitive personal information of more than 10,000 people since January 1 of the previous year.

The CAC may also request a security review whenever it deems necessary, highlighting the typical arbitrariness in the implementation of Chinese laws and regulations. It bears remembering that the CAC is a Party agency rather than a state one, supervised directly by the Central Cyberspace Affairs Commission chaired by Xi.[36]

Companies and other organizations have started testing this mechanism for regulatory approval. An early success case involved clinical trial data exports between Beijing Friendship Hospital, a public institution, and medical research centers at the University of Amsterdam.[37] However, this case is not representative, as its success relied on sponsorship by the National Health Commission, which wanted a poster project for data transfers in the medical and health field.[38] Multinationals have not found the process as smooth. As of July 2023, 11 data exports had received full approval from the CAC's Shanghai department against 530 applications, with 12 partial approvals, four rejections, and the rest still pending.[39]

Meanwhile, the party-state is struggling to push companies to manage cross-border data transfers through trusted clearinghouses. In 2020, the Ministry of Commerce (MOFCOM) tasked free trade zones (FTZs) to experiment with mechanisms for facilitating outbound data transfers.[40] These pilots are underway in the Shanghai Ligang District, Hainan Free Trade Port, and Guangzhou—the latter focuses on economic integration within the Greater Bay Area.[41] In Shenzhen, MOFCOM and the NDRC are encouraging the local data exchange to act as a safe interface for data exports to Hong Kong.[42] Except for Shenzhen, however, most of the pilots do not seem very active beyond building digital infrastructure such as subsea cables, data centers, and industrial parks for Big Data.[43]

CASE STUDY

Autonomous vehicles will drive the centralized collection of transportation data

It will be ambitious to collect all transport and logistics data within a national "Big Data brain," as stipulated by the 14th Five-Year Plan for A Modern and Comprehensive Transport and Logistics Network (2021-2025). Similar goals were part of the previous Five-Year Plan, and so far, there has been limited progress in standardizing and integrating smart city projects, indicating a lack of bottom-up interest.

This may change as more cars get on the roads that need to connect to a vehicle-to-everything (V2X) system for their assisted or autonomous driving capabilities. This is already happening, with 15,000 kilometers of smart roads installed by July 2023, according to MIIT. The ministry recently updated its standards guidelines, covering log keeping, cybersecurity, and data handling.[44] The sector was the first to get dedicated regulations for data security management, issued in 2021.[45] They require companies to store all data in China, obtain official approval for any cross-border data transfer, submit yearly incident reports, and provide Chinese public security, transportation, and industrial planning departments unrestricted access to all data (clause 15). At the same time, it prohibits these state departments from using the submitted information for anything other than security assessment.

Although Tesla insists that it complies with these and other Chinese requirements, Chinese media regularly report that Tesla cars are not allowed to enter Chinese government compounds or park at airports due to cybersecurity concerns, suggesting a lack of trust in foreign data-related entities, and a security-first approach. Meanwhile, local CAC bureaus in Beijing and Shanghai recently started advertising approved applications for outbound data transfers in the auto sector, but they seem the exception rather than the norm.[46]

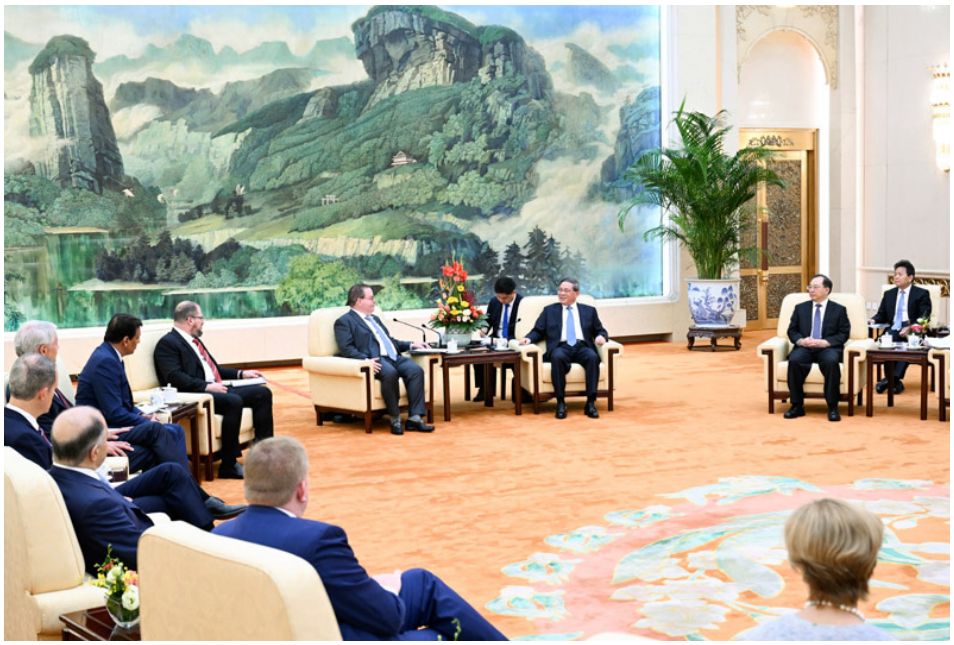
Conclusion: Prepare for Chinese policy that treats all data as a national resource

Forcing foreign firms to submit data to the Chinese state in the interest of innovation would directly go against everything that foreign chambers of commerce are telling Beijing it needs to do to attract foreign investment.

Beijing has methodically increased control over data flows since 2014, building out its regulatory as well as its institutional framework. Harnessing data as a national resource is a clear goal. An important planning document that the State Council issued in February 2023 stipulates "using digitization to drive productivity and reform governance methods, so as to move forward the great rejuvenation of the Chinese nation through Chinese-style modernization."[47]

This, along with emerging policy discussions in China around data ownership and usage rights, fuels concerns among foreign firms over data nationalization. As part of the "new-style whole-of-nation system" (新型举国体制), Xi has repeatedly called for making the most of the socialist system's unique ability to concentrate resources. Because data is seen as a national resource, this could translate into pressure especially on foreign firms in China to contribute data to a national pool in the interest of innovation, supporting China's efforts to break reliance on foreign technology. However, we found no indication in Chinese policies or public debates that the government is considering going beyond security reviews, the empowerment of trusted actors, and voluntary data-sharing platforms, to mandate data transfers.

Forcing foreign firms to submit data to the Chinese state in the interest of innovation would directly go against everything that foreign chambers of commerce are telling Beijing it needs to do to attract foreign investment. Such a move would also radically disrupt the balance between security and development in China's data governance regime. It is still possible that foreign firms eventually



Forcing foreign firms to submit data to the Chinese state in the interest of innovation would be detrimental to Beijing's effort in attracting foreign investment. (Image: Xinhua)

end up in that scenario. To begin with, the legal boundaries of the data that the state has the right to access on national security grounds are not very well defined, which may mean that any interaction with state-affiliated partners could eventually end up supplying some large Chinese database. But a categorical obligation to share data for economic policy reasons would be inconsistent with China's current efforts to attract FDI, including through relaxing rules on cross-border data transfer.

Facing complaints by Chinese and foreign companies alike that the approval process for data exports was unworkable, especially given its low thresholds to trigger security reviews and the persistent lack of clear definitions around concepts like "important" data, in September 2023 the CAC signaled a temporary and partial relaxation. A draft regulation vows to considerably ease the burden on businesses, for example by exempting international trade and transnational manufacturing from the requirement of regulatory pre-approval, or if the proposed transfer of personal information is necessary for fulfilling contractual obligations or managing human resources.[48] The draft also raises the threshold for a CAC-mandated security review and allows FTZs to draw up negative lists of data categories whose export requires approval.

If it materializes, such a relaxation will be welcome news for foreign firms in China that have been lobbying for a reversal of the government-mandated data decoupling. European businesses in sectors ranging from automotive to pharma consistently complain about the opaque and cumbersome security review process for data exports, which authorities seem to view as the go-to mechanism even for routine and non-sensitive data transfers.[49] The proposed regulatory changes would leave it up to companies to determine whether a data transfer is necessary for their operations, rather than allowing security-focused regulators to decide.[50]

Still, multinational corporations will have to live with a regime where multiple and sometimes competing state bureaucracies not only continue to determine the sensitivity of different kinds of data, but also strive to manage their domestic as well as cross-border circulation. In this environment, foreign firms in China may need to face some tradeoffs between protecting their most sensitive information, like trade secrets, from party-state overreach and accessing the data and data pools they need for innovation.[51]

Researcher bio: Rebecca Arcesati and Jeroen Groenewegen-Lau

Rebecca Arcesati's research focuses on China's technology and digital policy as well as Europe-China innovation relations. She covers the global footprint of Chinese tech firms, digital infrastructure and surveillance tools, governance of data and artificial intelligence, technology transfer and research collaboration. Prior to joining MERICS, Rebecca gained experience helping Italian tech startups scale in China and as a research assistant in the UN Women China office.

She holds an LL.M. in China Studies (Politics and International Relations) from Peking University, where she was a Yenching Scholar. Rebecca received an MA degree in International Studies from the University of Turin and a BA in Language Mediation and Cross-Cultural Communication from the University of Milan. She has studied and worked in Beijing, Shanghai and Dalian.

Rebecca Arcesati

Lead Analyst,
MERICS

Jeroen Groenewegen-Lau is Head of Program of "Science, Technology and Innovation" at MERICS. Prior to that he worked at "China Policy", a Beijing-based research and advisory company. He set up the section education, science and innovation at China Policy in 2017, and led it until December 2020. Jeroen spent over ten years in China. He holds a master's degree Languages and Cultures of China from Leiden University and wrote about Chinese popular music in his PhD dissertation.

Jeroen Groenewegen-Lau

Head of Program,
MERICS

Endnotes

1. https://merics.org/en/report/decoupling-severed-ties-and-patchwork-globalisation; https://www.fdiintelligence.com/content/interview/china-losing-its-allure-says-president-of-eu-chamber-of-commerce-81019; https://www.europeanchamber.com.cn/en/flash-survey-on-impact-of-china-rsquo-s-data-regulations; https://ec.europa.eu/commission/presscorner/detail/en/statement_23_4613
2. https://asia.nikkei.com/Spotlight/Century-of-Data/China-rises-as-world-s-data-superpower-as-internet-fractures
3. https://www.politico.eu/article/deal-over-dim-sum-china-caves-eu-data-keep-investors-sweet/
4. https://archive.ph/l9VG2
5. https://www.reuters.com/world/china/china-form-national-data-bureau-2023-03-07/; http://www.news.cn/mrdx/2023-10/26/c_1310747463.htm
6. https://www.gov.cn/zhengce/2022-12/21/content_5732906.htm
7. https://onlinelibrary.wiley.com/doi/full/10.1002/eet.2040
8. https://www.gov.cn/zhengce/zhengceku/2021-10/01/content_5640685.htm
9. https://www.kas.de/en/web/politikdialog-asien/digital-asia/detail/-/content/data-sovereignty-in-action; https://www.wsj.com/articles/ant-to-fully-share-consumer-credit-data-with-chinas-government-11632310975; https://www.wsj.com/articles/chinese-regulators-try-to-get-jack-mas-ant-group-to-share-consumer-data-11609878816
10. https://www.mot.gov.cn/xiazaizhongxin/ziliaoxiazai/202112/P020211222586122741056.pdf
11. https://merics.org/en/comment/didi-fine-marks-new-phase-beijings-rectification-tech-sector. During the long investigation, Didi was rumored to have considered leaving its handling of user data to Westone, a state-affiliated agency, but that was never implemented.
12. https://www.csis.org/analysis/what-i-learned-alibabas-data-protection-summit
13. https://www.wsj.com/articles/in-the-new-china-didis-data-becomes-a-problem-11626606002
14. https://www.gov.cn/gongbao/content/2019/content_5358684.htm
15. The National Internet Finance Association of China owns 36 % of Baihang, and Beijing Financial Holdings 35 % of Pudao. Private tech firms own most of the other stakes, with 25 % of Pudao in the hands of e-commerce platform JD.
16. https://m.21jingji.com/article/20220321/herald/1206c99b9cf419e5566e31420363c8f8_ths.html
17. https://academic.oup.com/cybersecurity/article/8/1/tyac011/6674794; http://www.xinhuanet.com//politics/2014-02/27/c_119538788.htm
18. https://merics.org/en/comment/china-activates-data-national-interest; DSL, art. 19, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/#_ftnref8
19. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/
20. https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm; https://merics.org/en/merics-briefs/data-market-foreign-talent-bio-based-materials; https://archive.ph/ly1ba
21. https://en.ndrc.gov.cn/policies/202203/P020220315511326748336.pdf; https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/; https://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm; https://www.gov.cn/zhengce/zhengceku/2021-11/30/5655089/files/d1db3abb2dff4c859ee49850b63b07e2.pdf
22. https://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm

23. He, Alex and Arcesati, Rebecca (2023). "Better Governance to Unleash the Value of Data: China's Practice of Building a Data Trading System". Forthcoming publication with the Center for International Governance Innovation (CIGI).
24. http://www.qstheory.cn/dukan/qs/2023-01/01/c_1129246978.htm
25. https://digichina.stanford.edu/work/translation-establishing-the-national-data-administration-march-2023/
26. https://www.jnexpert.com/article/detail?id=4260
27. https://www.gov.cn/zhengce/zhengceku/2022-12/14/content_5731918.htm
28. https://www.csis.org/analysis/dual-circulation-and-chinas-new-hedged-integration-strategy
29. https://www.ft.com/content/2f52965f-3bdb-4223-891b-e2208ad2e16e; cite also some EUCCC reports
30. https://www.reuters.com/article/china-regulation-cnki-idINL1N3AI0MD/; https://www.wsj.com/articles/china-data-security-law-ships-ports-court-cases-universities-11638803230
31. https://www.bloomberg.com/news/articles/2023-10-31/china-s-spy-agency-vows-crackdown-on-foreign-weather-stations#xj4y7vzkg
32. https://digichina.stanford.edu/work/translation-cybersecurity-review-measures-revised-effective-feb-15-2022/
33. http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm; http://www.cac.gov.cn/2022-11/18/c_1670399936658129.htm
34. https://merics.org/en/merics-briefs/data-transfer-rules-g20-exports
35. https://web.archive.org/web/20220708014822/http:/www.cac.gov.cn/2022-07/07/c_1658811536396503.htm
36. https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/
37. https://www.globaltimes.cn/page/202301/1284015.shtml
38. https://www.sohu.com/a/675118319_121123759
39. https://finance.sina.cn/tech/2023-07-06/detail-imyztyfi1982337.d.html?from=wap
40. http://www.mofcom.gov.cn/article/b/xxfb/202008/20200802992306.shtml; https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/China/Policy-Briefing-Cross-BorderDataTransfer.html
41. https://www.sohu.com/a/652419269_121255906; http://www.chinareform.org.cn/2023/0414/37604.shtml; https://web.archive.org/web/20220429082419/http:/hmo.gd.gov.cn/ns/content/post_3755560.html; https://www.scmp.com/news/china/politics/article/3228754/guangzhou-set-limited-cross-border-internet-scientific-research
42. He, Alex and Arcesati, Rebecca (2023). "Better Governance to Unleash the Value of Data: China's Practice of Building a Data Trading System". Forthcoming publication with the Center for International Governance Innovation (CIGI).
43. Ibid.
44. https://m.in-en.com/article/html/energy-2325109.shtml, https://www.gov.cn/zhengce/zhengceku/202307/P020230727459713380334.pdf
45. https://www.gov.cn/zhengce/zhengceku/2021-09/12/content_5640023.htm
46. https://news.cnstock.com/industry,rdjj-202305-5067112.htm
47. https://digichina.stanford.edu/work/translation-plan-for-the-overall-layout-of-building-a-digital-china/
48. https://merics.org/en/data-export-rules-beijings-silence-hamas-attacks-eu-technology-risk-assessment; https://www.piie.com/blogs/realtime-economics/chinas-new-rules-data-flows-could-signal-shift-away-security-toward-growth
49. See, for example: https://www.europeanchamber.com.cn/en/publications-position-paper
50. https://www.21jingji.com/article/20230929/4b3de75d9185ebfc77ce1c22aff5e36e.html
51. For example, the European Chamber of Commerce stated that initiatives aimed at creating open data pools in support of R&D, for example in the area of industrial big data, are not equally open to foreign-invested enterprises as they are for to domestic competitors. See: https://www.europeanchamber.com.cn/en/publications-position-paper

Cover image: AP

hinrich foundation
advancing sustainable global trade

MERICS

The Hinrich Foundation is a unique Asia-based philanthropic organization that works to advance mutually beneficial and sustainable global trade.

We believe sustainable global trade strengthens relationships between nations and improves people's lives.

We support original research and education programs that build understanding and leadership in global trade. Our approach is independent, fact-based and objective.

CONTACT US

There are many ways you can help advance sustainable global trade. Join our training programs, participate in our events, or partner with us in our programs.

inquiry@hinrichfoundation.com

Receive our latest articles and updates about our programs by subscribing to our newsletter

hinrichfoundation.com

hinrichfdn
hinrich foundation
hinrichfoundation
hinrichfoundation

Disclaimer:

The Hinrich Foundation is a philanthropic organization that works to advance mutually beneficial and sustainable global trade through original research and education programs that build understanding and leadership in global trade. The Foundation does not accept external funding and operates a 501(c)(3) corporation in the US and a company in Singapore exclusively for charitable and educational purposes.
 All statements of fact and the views, conclusions and recommendations expressed in the publications of the Foundation are the sole responsibility of the author(s).