BANCA D'ITALIA

EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Chinese data governance and trade policy: from cyber sovereignty to the quest for digital hegemony?

by Oscar Borgogno and Michele Savini Zangrandi

April 2023

Number 759

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Chinese data governance and trade policy: from cyber sovereignty to the quest for digital hegemony?

by Oscar Borgogno and Michele Savini Zangrandi

Number 759 – April 2023

The series Occasional Papers *presents studies and documents on issues pertaining to the institutional tasks of the Bank of Italy and the Eurosystem. The* Occasional Papers *appear alongside the* Working Papers *series which are specifically aimed at providing original contributions to economic research.*

The Occasional Papers *include studies conducted within the Bank of Italy, sometimes in cooperation with the Eurosystem or other institutions. The views expressed in the studies are those of the authors and do not involve the responsibility of the institutions to which they belong.*

The series is available online at www.bancaditalia.it .

ISSN 1972-6643 (online)

Designed by the Printing and Publishing Division of the Bank of Italy

CHINESE DATA GOVERNANCE AND TRADE POLICY: FROM CYBER SOVEREIGNTY TO THE QUEST FOR DIGITAL HEGEMONY?

by Oscar Borgogno* and Michele Savini Zangrandi*

Abstract

The paper provides an up-to-date overview of the data governance framework developed by the People's Republic of China. The work investigates whether and how the domestic legal framework on data governance has influenced Chinese trade policy with reference to cross-border data flows and e-commerce issues (at the WTO and G20 level). This study shows that Chinese data governance features a two-pronged legal architecture in which the Cyberspace Administration of China plays a prominent role. By prioritizing the need to maintain party-state domestic control across the digital economy, China has proved to be extremely averse to any international agreement that could undermine its domestic data governance framework.

JEL Classification: K20, K33, O33, P33, P37.
Keywords: data governance, digital infrastructure, China, data sovereignty, digital trade.
DOI: 10.32057/0.QEF.2023.0759

Contents

* Bank of Italy, Directorate General Economics, Statistics and Research.

1. Introduction. Data governance: the case of China[1]

Digital integration is shaping the dynamics of the global economy. Data-enabled technologies lower barriers to firms' internationalisation, foster innovation and open new routes for trade in goods and services. In this context, the People's Republic of China (China or PRC) is at the forefront of the global race for primacy in the digital domain, both in terms of domestic control and influence over developing countries.

The impact of digitalization on trade flows goes through multiple and reinforcing channels. The impact on trade in services is straightforward: digital connectivity provides direct support to trade in services that are produced and consumed in different countries. Digital connectivity however also fosters merchandise trade via digital marketplaces and via increased demand for digital devices and infrastructure. Finally, the rise of the Internet of Things, creates a powerful connection between merchandise trade and cross-border services. This new wave goes beyond smart consumer devices as it involves the systemic use of sensors for industrial applications, spanning from remote monitoring of equipment to factory automation and healthcare services.[2] Global IoT revenue is projected to increase by EUR 301.5 billion by 2030, with almost 8 billion interconnected devices.[3]

Alas, international digital trade remains a blurred field due to the lack of clearly defined global rules and definitions, meaning that there is no coherent set of laws or guidelines for countries to ensure free flows of digital trade internationally.[4] The last major round of WTO negotiations, the Uruguay Round, predates the rise of digital trade, and, no diplomatic initiatives have succeeded in updating this international legal framework since.

Against this backdrop, looms large the issue of cross border data flows, absent which, digital and digitally-enabled trade would grind to halt.[5] Data governance – which shapes cross-border data flows – can be broadly defined as the set of rules and enforcement mechanisms that discipline collection, access, storage and processing of third party data.[6] Each jurisdiction's legal framework determines whether data can freely flow across borders thereby allowing cross-border digital services, how and under what circumstances businesses can make use of users' data as well as how much individuals can rely on the trustworthy functioning of digital markets.

Developing an adequate data governance framework requires policy makers to strike a balance between conflicting policy objectives (Figure 1).[7] Thus, it should not come as a surprise if several jurisdictions developed different approaches to data governance over the last five years. Some countries prioritize the need to safeguard the privacy of their citizens. For instance, in the European Union (EU), Canada, and Japan personal data protection is ensured by means of comprehensive regulatory frameworks. Therefore, the treatment of personal information by firms is allowed under

[1] The authors wishe to thank Riccardo Cristadoro, Giovanni Veronese, Alessandro Borin, Michele Graziadei, and Marina Timoteo for their constructive criticisms which lent form and substance.

[2] N Fildes, "Battle intensifies to unlock value in the Internet of Things", 2019, Financial Times, 18 June.

[3] Statista, "Transforma Insights: Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by use case (in millions)", 2020.

[4] Claudia Biancotti and Riccardo Cristadoro, "International digital trade: a primer" (2020); WTO, "Adapting to the digital trade era: challenges and opportunities" (Ed. Maarten Smeets), 2021, 218.

[5] United Nations Conference on Trade and Development - UNCTAD, "Digital Economy Report – Cross-border data flows and development: For whom the data flow", (2021) 74.

[6] For an in-depth analysis of data governance, meant as a bundle of data protection, national security, and competition policy concerns, see: Oscar Borgogno, Michele Savini Zangrandi, "Data governance and the regulation of the platform economy", QEF Banca d'Italia n. 652; Oscar Borgogno, Michele Savini Zangrandi, "Data governance: a tale of three subjects", Journal of Law, Market & Innovation n. 2.

[7] Oscar Borgogno, Michele Savini Zangrandi, "Data governance and the regulation of the platform economy", QEF Occasional Papers, n. 652.

strict limits about which data can be collected, which uses it can be put to, who can access it, and how long it can be retained for. Other jurisdictions as the United States (US) do not have a comprehensive federal legislation.[8] Finally, national security and the so called cyber-sovereignty are often cited by other countries to justify restrictions on cross-border data flows as well as data localization requirements, albeit in varying degrees across different countries. A recent example of this approach is the Cybersecurity Law introduced by the People's Republic of China in 2017, which explicitly aims to "safeguard cyber security, protect cyberspace sovereignty and national security".[9]

Figure 1. UNCTAD, Digital Economy Report (2021), 121.

Such divergence in data frameworks across jurisdictions – although justified with the different strategic priorities of national governments as well as their economic, social and cultural values – may result in different data government arrangements not necessarily compatible with each other, raising questions regarding the potential fragmentation of the global digital economy.

Amongst the world's top economies, China is defining a framework for data governance that is very peculiar, and potentially incompatible with those being developed elsewhere in the world.

China's nascent data governance framework is predicated upon security concerns. Since the early stages of the debate on global Internet governance, China has stressed the importance to preserve "cyber sovereignty".[10] The primacy of sovereignty shaped also the Chinese approach towards data governance, leading to the new mantra of "data sovereignty" as a top priority of the Chinese government in international fora. Issues of national security ranked high in the policy agenda of president Xi Jinping over the last five years.[11] This trend is not going to change anytime soon. Indeed, on 16 October 2022, during the 20th Chinese Communist party congress in Beijing, President Xi noted that the "cyber ecology continued to improve" thereby signaling that censorship and data content surveillance would not diminish.[12]

China's domestic framework for data governance determines its position in the many negotiating tables which contribute to the shaping of transnational data governance. Across negotiating tables,

[8] To date, the most relevant state data privacy state legislation within the US is the California Consumer Privacy Act 2018 (CCPA). Signed into law on June 28, 2018, it went into effect on January 1, 2020. The CCPA is cross-sector legislation that provides for broad individual consumer rights and imposes significant duties on entities or individuals that gather personal information about or from a California resident.

[9] Article 1 Cybersecurity Law of the People's Republic of China, adopted 7 November 2016, www.chinalawinfo.com

[10] Adam Segal, "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace", NBR special report n. 87, 2020.

[11] Kevin Rudd, "The World According to Xi Jinping", Foreign Affairs, November/December 2022.

[12] Paul Mozur and John Liu, "On tech, Xi points to self-reliance and state-led initiatives", The New York Times, 1 October 2022.

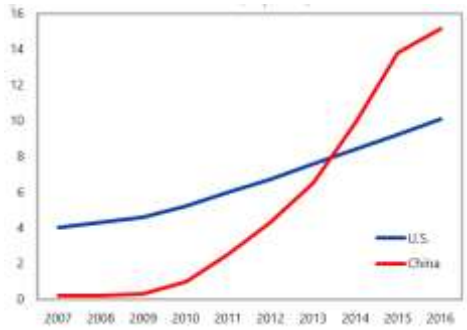
China's position supports free flow of data related to merchandise trade transactions, while restricting all other types of cross-border data flows.

This position is consistent with China's international digital footprint. China is home to a very large e-commerce market (Figure 2) – which is set to expand abroad.[13] While e-commerce remains chiefly a domestic business, cross-border e-commerce in China is increasing steadily (Figure 3). By the end of 2019, it accounted for around 1.6% of total e-commerce revenue in the country and is projected to expand by nearly 300% in 2024.[14] Notably, this trend is in line with China's main geopolitical competitors. In the EU, cross-border e-commerce sales to the rest of the world carried out by businesses undertakings accounted for 2.1%[15] while in the US for 3%.[16]

Moreover, over the last 20 years, China has emerged as the main exporter of Information and Telecommunication Technology (ICT) goods at the global stage (Figure 4). In reading this, it is important to keep in mind that communication technology, is not just trade in goods, but rather in access points to a bundle of data-enabled services. As such, ICT goods exports comprise both retail devices and telecommunication infrastructure. In this, the digital component of the Belt and Road Initiative (BRI), also known as Digital Silk Road (DSR), plays a crucial role.[17]

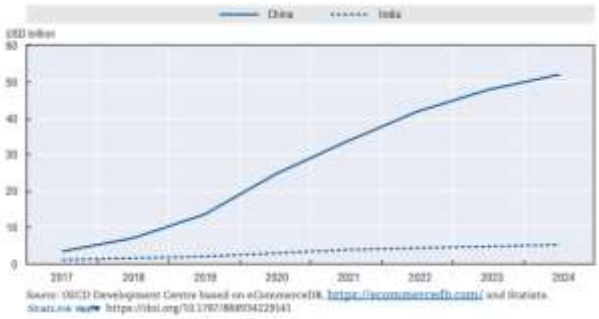
China, by contrast, is a relatively smaller player in services exports. A comparison with another large emerging economy, such as India is instructive. India is a net services exporter, with export services trade (exports plus imports) summing to approximately 12 percent of GDP in 2020. China is a net services importer, with services trade totaling a mere 4 percent of GDP (Figure 5).

Figure 2: Share of E-commerce in total retail sales, in percent



Source: IMF[18]

Figure 3: Cross-border e-commerce in China and India



Source: OECD

[13] Longmei Zhang and Sally Chen, "China's Digital Economy: Opportunities and Risks", IMF Working Papers n. 16, 2019.

[14] OECD, "Economic Outlook for Southeast Asia, China and India 2021", 98.

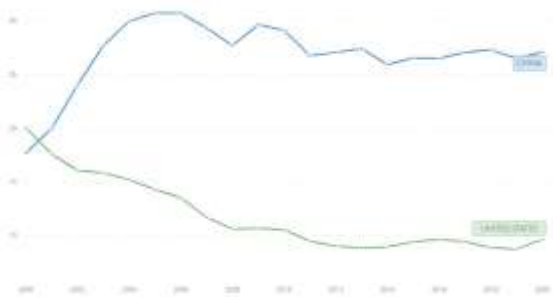
[15] OECD, "Going Digital Toolkit".

[16] Statista Research Department, "Revenue share of the cross-border e-commerce market in the U.S. 2017-2025".

[17] The BRI has emerged as a landmark development within Chinese international relationships. The BRI comes with a broad spectrum of infrastructure projects to foster the movement of capital, services, goods, energy, and labor between China and 146 countries across the globe, developing networks and economic environments which could reinforce China-dependent value chains. For an overview, see: Jonathan E. Hillman, "The Digital Silk Road: China's Quest to Wire the World and Win the Future" (Harper Collins, 2021); Alex He, "The Digital Silk Road and China's Influence on Standard Setting", CIGI Papers No. 264 — April 2022.

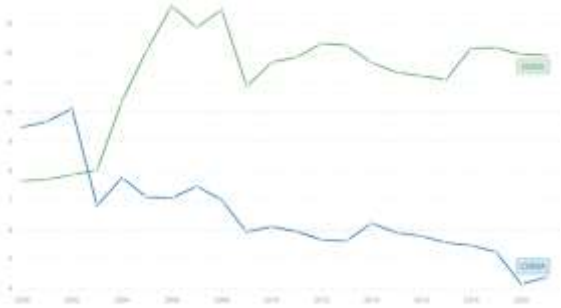
[18] Longmei Zhang and Sally Chen, "China's Digital Economy: Opportunities and Risks", IMF Working Papers n. 16, 2019.

Figure 4: ICT goods exports (% of total goods exports) - China, United States



Source: World Bank, 2022[19]

Figure 5: Trade in services (exports plus imports, % of GDP) - China, India



Source: World Bank

Understanding China's framework for data governance is particularly important. This is because China will have a major role in shaping (or undermining) the development of a global data governance framework. China's influence has taken shape by several statements and informal steps at WTO negotiating tables.

As transnational data governance goes beyond treaties and negotiations, it is also important to recognize the ability of China's DSR to create new technological dependencies with an impact on international relations. As digital environments are directly dependent upon the infrastructural level on which data are gathered, stored, and transferred (such as data centers, cables, satellites, etc.), the DSR should be considered an integral part of China's global data governance strategy.

The Chinese policy behavior in this field has been referred to as "Beijing Effect", namely a combination of push and pull factors that explains China's growing influence in transnational data governance.[20] Although the official narrative states that China does not seek to influence other states' data governance policies, this position appears to hide a fundamental contradiction. While it is true that China has consistently advocated for national autonomy over data governance issues, it is also trying to establish technological and infrastructural dependencies within the digital space of several countries. In particular, technological dependencies are established whenever the digital infrastructure relies on standards, software and hardware that cannot be autonomously maintained without active support from Chinese players. Such efforts hold the potential to frustrate hosting jurisdictions' ability to enjoy proper national self-determination when it comes to the digital economy.

Basically, China has enabled a quick digitalization process in DSR participating countries that takes place without paying attention to the existence of commensurate legal frameworks able to minimize the risks of market failures and the spread of in-country inequality (for instance, with regard to antitrust, platform regulation, and taxation). The fact that EU, Australia, UK, Canada, and US are still struggling to tackle these very problems in an effective way makes the problem even more pressing for developing countries targeted by China's digital investment projects. Digital integration can turn to be counter-productive in the absence of sound legal safeguards in place. Thus, the DSR stands in

[19] Based on United Nations Conference on Trade and Development's UNCTADstat database at unctadstat.unctad.org/ReportFolders/reportFolders.aspx.

[20] The Beijing Effect contrasts with the Brussels Effect "whereby companies' global operations gravitate towards the EU's regulations. It also deviates from US efforts to shape global data governance through instruments of international economic law". See Matthew S. Erie, Thomas Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance", 54 N.Y.U. J. Int'l L. & Pol. 1 (2021).

stark contrast with China's explicit intention to preserve each country national sovereignty over data governance issues.

Against this backdrop, the article provides a detailed analysis of the rationale and architecture underpinning the new bulk of legislation that shaped Chinese data governance over the last five years. This understanding is key to assess the approach adopted by China at the international level on data governance issues, such as the regulation of cross-border data flows. As such, we argue that Chinese domestic priorities over data content control are aligned with the extremely cautious attitude towards international initiatives pushing for global data governance harmonization and free flows of information across borders (such as the on-going WTO Initiative on E-commerce).[21] This explains why US-led initiatives aimed at facilitating cross-border data flows in the G20 context are unlikely to be supported by China (Annex 1).[22]

The article is structured as follows. Section 2 provides an up-to-date overview of the most relevant pieces of legislation which lay at the heart of domestic Chinese data governance. Section 3 delves into the Chinese approach to global trade negotiations involving data governance and its renewed sensitivity for the "trade-related aspects" of cross-border data flows. Section 4 illustrates how the DSR fits into the broader Chinese global strategy for data governance. Section 5 concludes by advancing some policy remarks.

Note that this paper does not dwell on how countries other than China are dealing with transnational data governance. Thus, the reader should be mindful that this analysis is not meant to provide a comprehensive comparative assessment of how all major jurisdictions are reciprocally influencing each other in the global race for digital hegemony.

2. Data governance in China: the primacy of state control

The so-called data regulation with "Chinese characteristics" has taken shape over a twenty-five-year period.[23] From a substantive perspective, the focus of regulation has shifted significantly during this time span. While in the '80s and '90s hardware control was at the core of policy makers' concerns, data content and localization have now been targeted as the most sensitive issues. As Internet-enabled communication and business are increasingly considered a key threat to the power consolidated by the ruling Party in China, data governance has emerged through several pieces of legislation as an unavoidable route to ensure national security and government control over the Chinese society.

From an institutional perspective, the Cyberspace Administration of China (CAC) has emerged as the leading supervisor on both data and Internet governance, with the Ministry of Industry and Information Technology and Ministry of Public Security playing ancillary roles. Despite its broad power, the CAC is granted a high level of administrative opacity and substantial jurisdictional immunity as opposed to other state agencies which are increasingly subject to legal requirements of due process, transparency, and accountability.[24] For instance, reviews conducted by the CAC in the

[21] Since 2017, the WTO has focused its attention on trade-related aspects of e-commerce, under the heading of "Joint Statement Initiative on E-Commerce". See WTO, "Joint Statement on Electronic Commerce", Ministerial Conference, World Trade Organization.

[22] Indonesia's G20 presidency, "Minister of Communications and Informatics Emphasizes Digital Sovereignty in Cross-Border Data Flow", 20 July 2022. As argued in Oscar Borgogno, Michele Savini Zangrandi, "Data governance and the regulation of the platform economy", QEF Banca d'Italia n. 652 For an overview of the G7 and G20 deliberations in the areas of Data Free Flow with Trust and cross-border data flows, see Annex 1.

[23] Henry S. Gao, "Data Regulation with Chinese Characteristics" in Big Data and Global Trade Law (edited by Mira Burri), Cambridge University Press, 9 July 2021.

[24] Jamie P. Horsley, "Behind the Facade of China's Cyber Super-Regulator", DigiChina (Stanford University), 8 August 2022.

field of data security, are final and not subject to external appeal. Moreover, the agency does not publish its organizational structure, other than the names and brief biographies of its director and four deputy directors. This makes it extremely tricky for analysts and business players to reach an adequate level of legal predictability as to what is forbidden and what is allowed under the current Chinese data governance framework.

Against this background, the following sub-sections illustrate the legislative building blocks which laid the foundation of modern Chinese data governance.

2.1. Cyber security

The modern data governance framework in China has traditionally hinged on cybersecurity considerations. In 2013, the Third Plenum Conference of the Eighteenth Party Congress decided to establish a specific policy strategy aimed at ensuring "the security of national Internet and information". For the first time in Chinese history, Internet governance was considered a topic of public security by the ruling party. As President Xi put it, Internet and information security were "a matter of national security and social stability, and a new composite challenge facing China".[25] The lack of adequate pieces of legislation addressing the matter together with overlapping competencies of diverse agencies were targeted as the main weaknesses of the Chinese Internet governance. Accordingly, the Central Leading Group on Cyber Security and Informatization (the "Group") was set up in February 2014 with top-ranked officials under direct leadership of President Xi. They were officially entrusted with the task of overseeing internet and data governance. As the Group was based within the CAC, the agency got centre stage within the Chinese bureaucracy as the most powerful player in the Chinese data governance landscape.[26] Accordingly, the CAC was put in charge of carrying out cyberspace content regulation on behalf of the State Council.[27]

Further, in 2015, the new "**National Security Law**" made clear that cyber security was key to reach national security, defined in article 2 as "a situation in which the national regime, sovereignty, unity and territorial integrity, the welfare of the people, the sustained development of the economy and society and other major State interests are not in danger or under internal or external threat, as well as the capacity to ensure a sustained situation of security".[28] In particular, the new objective was to make "secure and controllable" all the "core technology of the Internet and information, key infrastructure and the information system".[29] Notably, Article 77 of the act compels all citizens and legal entities to report in a timely manner any activity that could endanger national security and provide all the support to government agencies. So far, this provision has not been enforced strictly, but allows the government to access any digital communication within the Chinese jurisdiction.

Further emphasis on the matter was finally added in 2016 with the "**Cyber Security Law**", which reiterated that national security and cyber-sovereignty were ranking high in the Chinese policy agenda. Article 8 of the law entrusted the CAC with the task of overseeing all the supervision work

[25] Xi Jinping, "Explanations of the Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Comprehensively Deepening Reform", 9 November 2013.

[26] "National Internet Information Office Restructured, State Council Delegated the Power on Internet Content Administration and Enforcement", guancha.cn, 28 August 2014. See also Jamie P. Horsley, "Behind the Facade of China's Cyber Super-Regulator", DigiChina (Stanford University), 8 August 2022.

[27] PRC State Council, "Notice on Delegation of Power on Administration of Internet Information Content to the National Internet Information Office", Guofa No 33 (2014), 26 August 2014.

[28] National Security Law of the People's Republic of China, article 2. Translation provided by Prof. Rogier Creemers of the University of Leiden.

[29] National Security Law of the People's Republic of China, Article 25. This piece of legislation was adopted at the Fifteenth Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on 1 July 2015, available at www.chinalawinfo.com.

on cybersecurity. Further, the law expanded the liability regime for transferring illegal online content between firms and individuals (Articles 12 and 48).[30] Since then, any internet information service provider in China has been under an obligation to file online complaints and reports to the CAC.[31]

The Cyber Security Law marked a shift from data content oversight to data localization requirements, under which several categories of data must be stored domestically. For instance, pursuant to Article 37, operators of "critical information infrastructure" shall store within Chinese borders all personal information and important data (a concept still lacking an official definition) collected and generated. While the former pertains to information that is related to an identified or identifiable natural person, the latter is loosely understood as data which involves economic security, social stability, and national security issues. In order to comply with the new data localization requirements, Apple entrusted Guizhou-Cloud Big Data, a Chinese state-owned company, with the task of acting as the service provider for Apple customers in China.[32]

Admittedly, it is not entirely clear what "critical information infrastructure" means as the wording of the legislative definition is broad and vague. The wording covers all "important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs" whose data transfer could result in "serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage". Since this definition is not useful to implement the law effectively, the State Council has been entrusted with the task of identifying critical infrastructure on a case-by-case basis. In order to bring more legal predictability, the CAC released the National Network Security Inspection Operation Manual and the Guide on the Determination of Critical Information Infrastructure based on both quantitative and qualitative criteria.[33]

However, it is worth noting that even infrastructure that do not fulfil such conditions may fall within the concept of "critical information infrastructure" whenever they could "lead to leakage of sensitive information about firms or enterprises, or leakage of fundamental national data on geology, population and resources, or seriously harming the image of the government or social order, or national security".[34]

For instance, in October 2018, BGI Group, the world's largest genome research organization, was fined by the Chinese Ministry of Science and Technology for exporting online certain human genome information abroad without authorization.[35] The company illegally carried out a "leakage of fundamental national data on population". Also, on 2 July 2021, CAC suddenly launched its first ever cybersecurity investigation, targeting ride-hailing DiDi Global due to unspecified potential data and

[30] Already under the 2000 Administrative Measures, the Internet information service providers are required, upon discovering prohibited information on their website, to stop the transmission, keep relevant records, and report to the relevant state authorities.

[31] In 2018 and 2019, around 25 million reports were filed every month, with the majority targeting the major social media websites, such as Weibo, Tencent and search engines, such as Baidu. See Cyberspace Administration of China (National Internet Information Office), the Centre for Reporting Illegal and Bad Information, Acceptance of National Network Reporting in June 2019, 3 July 2019.

[32] Jack Nicas, Raymond Zhong and Daisuke Wakabayashi, "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China" 17 June 2021, New York Times.

[33] Critical information infrastructure are grouped into three categories: (i) websites, which includes websites of government and party organizations, enterprises and public institutions, and newsmedia; (ii) platforms, which include Internet service platforms for instant messaging, online shopping, online payment, search engines, emails, online forum, maps, and audio video; and (iii) production operations, which include office and business systems, industrial control systems, big data centres, cloud computing and TV broadcasting systems.

[34] Henry S. Gao, "Data Regulation with Chinese Characteristics" in Big Data and Global Trade Law (edited by Mira Burri), Cambridge University Press, 9 July 2021.

[35] David Cyranoski, "China's crackdown on genetics breaches could deter data sharing", Nature, 13 November 2018.

national security risks. This happened just two days after the company raised US$4.4 billion in a New York initial public offering.[36] The CAC suspended new user registrations while the investigation was ongoing in order to prevent any exacerbation of risks. The CAC ordered the company to remove its own mobile application from Chinese digital stores. Finally, in order to address concerns of data accumulation that mobile app operators like DiDi are amassing, a government-backed app has been envisaged to integrate a variety of services including ride hailing.[37] By so doing, the party-state would maintain the exclusive ability to oversee online activity as well as the movements of individuals and government officials.

2.2. Personal data protection

On top of cyber security legislation, in recent years, China has shaped a comprehensive data protection framework building on two main legislative pillars, namely the "Data Security Law" (DSL) and the "Personal Information Protection Law" (PIPL), which are expected to be followed by a series of administrative rules and implementation regulations.

China's "**Data Security Law**" entered into force on 1 September 2021 and is primarily aimed at regulating data processing and handling activities that could influence national security.[38] The law applies to all companies, individuals, and public entities which carry out data collection activities within China by imposing on them a number of high-level data protection and security obligations.

One of the most remarkable elements of the Data Security Law is that it provides for a "hierarchical system for data protection". This means that all data would need to be categorised according to its importance in "economic and social development; and […] the impact on national security, the public interest, or the lawful rights and interests of citizens or organizations if it is falsified, destroyed, leaked or illegally acquired, or illegally used".[39] Accordingly, the DSL identifies the category of "important data", for which additional requirements apply, including obligations to:

1. submit a risk assessment report including details of the type of data being processed, and how security risks are being addressed;
2. designate a data security officer and set up a management office to fulfil data security protection responsibilities;
3. periodically conduct risk assessments on their data processing activities.

Finally, under the umbrella of "core national data" the law encompasses all information referring to "national security, the lifelines of the national economy, important aspects of people's livelihoods, major public interests, etc".[40] Such data is subject to an even stricter management system. It is worth noting that this is distinct from "important data" under the Cyber Security Law (which has not been defined in detail so far). The definition of "core national data" is not centralized: local governments and regulators are charged with task of detailing important data catalogues for their own industry sectors and geographic areas.

At the moment, the process of categorisation has not been carried out in a comprehensive fashion. For instance, the CAC has already published guidelines relating to smart cities.[41] These guidelines

[36] See Ryan McMorrow, "Didi fined over $1bn by Beijing for 'vile' breaches of data laws", Financial Times, 21 July 2022.

[37] Bloomberg, "China Creates 'Strong Nation' App as Data Regime Tightens", 19 January 2023.

[38] "Data Security Law of the People's Republic of China", translation by DigiChina, 29 June 2021.

[39] DSL, art. 21.

[40] DSL, art. 21.

[41] Even though the term "Smart city" is a fuzzy and evades a unitary characterisation, we can define it as "a city in which information and communication technologies (ICT) are intertwined with the urban environment, enabling, coordinating

point out what is considered "important data" and "core national data" for this industrial sector, and what types of data transfers need to be approved before being carried out.

As this law is poorly defined in many aspects, it is likely that such new requirements will need to be narrowed down through forthcoming implementing regulations, and new official documentation. The law is generally regarded as a counter-move to the U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act) enacted in 2018, which facilitate US law enforcement authorities the power to compel companies under US jurisdiction to share requested data regardless of where the data is stored.

In brief, all companies handling personal data within Chinese borders are now under an obligation to:

1. set up data security management systems across their entire workflow, adopt technical measures to safeguard data security, and conduct data security training;
2. monitor potential risks, and in the event of data security incidents notify users and report incidents to the relevant regulatory authorities.

Finally, the DSL explicitly prevent any entity which must store data within the mainland territory of the PRC from sharing it with law enforcement foreign institutions without preliminary approval from competent authorities. The law provides for specific sanctions in case of non-compliance, particularly in term of cross-border transfers. For example, fines of up to two million RMB (€272,000 - exchange rate as of December 2022) could be levied in cases where "corrections are refused or a large data leak or other serious consequences are caused".[42]

The "**Personal Information Protection Law**" (PIPL) entered into force on 1 November 2021 and introduced a general legal framework for the treatment of personal data relating to individuals located in China.[43] Unlike the Data Security Law, this act focuses on privacy considerations and the right to confidentiality rather than on national security concerns.[44] For starters, the law clarifies that the concept of "personal information" covers "all kinds of information related to identifiable natural persons recorded by electronic or other means, excluding information processed anonymously". Similarly, entities that will be considered "personal information processors" are defined as "organisations or individuals that independently decide the purpose and method of processing of personal information". Importantly, foreign firms operating in China must appoint representatives or establish designated agencies to take responsibility for issues related to the handling and protection of personal information.

Still, the PIPL does not restrict domestic security and police services from gathering and processing data for their statutory purposes, as well as the use of personal information in other large-scale state-led projects, including the forthcoming Social Credit System.[45] This is a mechanism providing for a massive aggregation and exchange of data about "credit subjects" with the ultimate goal of applying such credit information in public and private decision-making processes involving citizens and corporations.[46]

---

or integrating the functioning of its infrastructures". See Lorenzo Dalla Corte, "Safeguarding data protection in an open data world", University of Tilburg, 2020.

[42] An interesting comparison could be made with reference to the long-lasting debate on auditing data in accounting. See YJ Fischer, "Resolving the Lack of Audit Transparency in China and Hong Kong" 2022.

[43] "Personal Information Protection Law of the People's Republic of China", translation by DigiChina, 10 August 2021.

[44] Rogier Creemers, "China's Emerging Data Protection Framework", Journal of Cybersecurity, Volume 8, Issue 1, 2022.

[45] Its legal framework was presented as a draft law on 14 November 2022, by the National Development and Reform Commission & People's Bank of China, "Law of the People's Republic of China on Developing the Social Credit System" 2022.

[46] Negatively impact social credit records can range from severe law breaking to more minor infractions like misconduct on the subway, and often include political behaviour like protesting or spreading unsanctioned information online. In some cities, poor social credit records can be the basis for punishments, such as travel and internet restrictions. Chuncheng

It is worth noting that the PIPL is the only piece of legislation within the Chinese data governance framework having an explicit extraterritorial effect echoing the EU GDPR (*General Data Protection Regulation*). Indeed, it applies also to organisations based out of China that process any personally identifiable information collected and produced in China. The implication of this extraterritorial application is that foreign entities in this position will have to establish designated agencies or appoint representatives based in China to take responsibility for issues related to the handling and protection of personal information. Admittedly, it is possible to find many correspondences between the PIPL and the GDPR.[47]

When it comes to cross-border data transfers, the PIPL requires companies to meet specific criteria before transferring personal information to foreign jurisdictions. One option is for an entity to pass an assessment or undergo certification as administered by the CAC. Another is for firms to sign a "standard contract" issued by the CAC agreeing the rights and responsibilities of both sides. In addition, entities would also need to obtain separate consent from individuals regarding transfer of their personal information. Admittedly, despite some technical differences, there are important similarities with the approach implemented by the GDPR in the EU for clearing data transfers outside the European Economic Area.[48]

Overall, the PIPL was designed having in mind the bargaining power of individuals within the digital economy. This is why the law introduced specific requirements for firms enjoying "massive number of users, who operate complex types of business activities". Such operators (commonly known as BigTech firms) are expected to appoint personal information protection officers, to be responsible for supervising personal information handling activities as well as for stopping to provide services to third-party operators on the platform who violate personal information laws and regulations, and regularly release Corporate Social Responsibility reports on personal information protection.[49] Such role is similar to the position of data protection officer (DPO) under the GDPR. Notably, this act fits within the broader regulatory crackdown which unfolded under Xi leadership over the last two years as it constraints internet platforms ability to disrupt existing institutional framework and challenge the Chinese party-state.[50]

In brief, the PIPL aims to find a balance between three different policy objectives: protecting individuals from malicious or improper data collection and use, ensuring trust and contestability within the digital economy, while prioritizing the public interest as the ruling party defines. Rather than creating fundamental rights or general legal principles, it does so by regulating different categories of actors and the relations between them in a highly detailed manner, depending on the potential perceived risks or harms that may arise. Finally, the PIPL is also clearly meant to build foreign recognition for Chinese personal data protection efforts, thereby facilitating international

---

Liu, "Who Supports Expanding Surveillance? Exploring Public Opinion of Chinese Social Credit Systems", International Sociological Association, 2022; Marianne Von Blomberg, "The Social Credit System And China's Rule Of Law", Mapping China Journal 2, 2022.

[47] Deng & Dai (2021) "A comparison between China's PIPL and EU's GDPR".

[48] Unlike the standard contractual clauses (SCC) for the cross-border transfer of personal information under the GDPR, which follow a modular approach and are designed to provide safeguards for transfers of PI to third countries (outside of the European Economic Area) in different transfer scenarios, the obligations set forth under the SCCs apply similarly to all forms of transfers between data handlers in China and the corresponding overseas recipients. There are, however, certain similarities between the SCCs and the GDPR Standard Contract Clauses, such as: (i) providing for third-party beneficiary rights of personal information subjects; (ii) foreseeing a warranty that the parties have conducted a transfer impact assessment; (iii) safeguarding the processing of personal data by taking effective technical and management measures to ensure the security of the information; (iv) allowing for audits by the data protection officer; and (v) accepting joint and several liability for claims brought by data subjects.

[49] PIPL, art. 52.

[50] Ernan Cui, "The Drivers Of The Regulatory Crackdown", Gavekal Dragonomics, 2021.

cooperation on cross-border data flows issues. As a matter of fact, the Chinese policy maker is striving to ensure personal data protection safeguards to build trust in its data governance framework.

3. The Chinese approach to international digital trade

By analyzing the evolution of data governance in China over the last 20 years, it is possible to identify two overall trends. First, regulation has increasingly expanded its scope in the digital domain until reaching a tipping point characterized by overlapping powers and poor legal certainty.[51] Second, the CAC has surfaced as the leading agency which is now entrusted not only with the task of enforcing data governance but also Internet surveillance within national borders.

It is worth noting that this institutional evolution fits into an overall shift in priorities for Chinese policy makers. While the focus was originally on software, and then to content, now it is on the interplay between data and national security. This explains why understanding data governance in China is crucial to correctly gauge the current approach of the country towards international initiatives shaping common rules for the digital economy. On a broader level, it must be noted that Chinese approach fits within a global trend towards data localization obligation in order to facilitate law enforcement and national security concerns.

3.1. Chinese data governance in the face of international trade policy

As digital trade is inherently meant to overcome borders and geographic obstacles, it makes good sense to target the matter by means of international law tools and multilateral cooperation. Over the last 20 years, the World Trade Organization (WTO) framework has constantly witnessed attempts to incorporate data regulation and Internet-enabled business.[52] However, the WTO multilateral architecture has proved to be too onerous to reach workable compromise on the many issues which underpin transnational data governance. In fact, each state's approach to data regulation and Internet is directly shaped by domestic policies involving national security, fundamental rights, and competition policy.[53] China is no exception to this phenomenon. This explains why most of the countries willing to build consensus on common data governance frameworks resorted to free trade agreements (FTAs) and plurilateral Trade in Services Agreement (TiSA) initiatives.[54]

When it comes to international trade law and control over digital contents, China experienced setbacks which contributed to the current cautious approach towards new multilateral initiatives in the field. For instance, the first China's data governance international litigation involving WTO rules

[51] As to the negative effects on legal certainty and overall administrative coherence of Chinese bureaucracy arising from the regulatory crackdown in data governance and competition law, see: Angela Huyue Zhang, "Chinese Antitrust Exceptionalism", 2021, Oxford University Press.

[52] For an overview of the issues, see Henry Gao, 'Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation', Legal Issues of Economic Integration 45, 2018, 47–70.

[53] Oscar Borgogno, Michele Savini Zangrandi, "Data governance and the regulation of the platform economy", QEF Occasional Papers, n. 652.

[54] As to the US, this new model of data governance obligations started out in the 2004 FTAs the US signed with Chile, Singapore, and Australia. It finally culminated in the Trans-Pacific Partnership (TPP) that was finalized in 2016. While the Trump Administration withdrew from the TPP, the e-commerce chapter maintained the shape that was originally envisaged by the US and was finally incorporated into the new Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) that the remaining 11 TPP-members signed in March 2018. As to the EU, on 7 October 2022, while negotiating the Economic Partnership Agreement (EPA) with Japan, the EU managed to include rules on cross-border data flows and to prohibit unjustified data localization requirements.

was about the publication of audio-visual content.[55] Notably, this was the first WTO case concerning China's digital censorship policy. The United States alleged that China infringed its commitments on "sound recording distribution services" by not allowing foreign companies to electronically import and distribute audiovisual products.[56] China lost the case and was eventually forced to change its domestic approach.

After such a troublesome experience, China's approach to data governance and internet regulation in international trade bodies became much more prudent, if not hostile. This stands in stark contrast to the United States and, to a lesser extent, the European Union which have embraced discussions on data governance frameworks transnationally in international fora.[57] For instance, the vast majority of the FTAs signed so far by China do not provide for regulation in this area. The most notable exceptions are the amendment of the FTA signed with Chile in 2018, and the two FTAs China signed with South Korea and Australia in 2015.[58] Such documents are not very ambitious as they address e-commerce-related issues, namely the moratorium on customs duties on electronic transmissions, electronic authentication as well as electronic signatures, paperless trading, and the protection of personal information in e-commerce. Contrary to the FTAs adopted by the US, such agreements do not include provisions on free flow of data and ban on data localization requirements. As such, they only partially interact with proper data governance issues.

The same approach has been replicated in the context of WTO negotiations. While the US has pushed for common rules enabling so-called free cross-border data flows and banning data localization requirements, China opposed this agenda. For instance, the WTO Eleventh Ministerial Conference, held in 2017, was followed by a joint Pakistan and China communication on e-commerce focusing solely on "cross-border trade in goods enabled by Internet, together with services directly supporting such trade in goods, such as payment and logistics services".[59] This view should not come as a surprise as it reflects the business nature of several Chinese platform-based firms, which center on trade in physical goods enabled by the Internet, rather than the provision of digital services (e.g. Google and Netflix). Admittedly, this approach does not facilitate the international activity and expansion of other Chinese players which focus on digital services, such as social networks and cloud (TikTok, SenseTime, Alibaba Cloud, Tencent Cloud, etc.).

Most importantly, China did not join the statement issued in December 2017 about the launch of the negotiations on e-commerce within the WTO Eleventh Ministerial Conference. However, once the e-

[55] From its part, China argued that the provision was meant to cover only "traditional" recordings in physical form (such as audio tapes) and not "network music services" which merely supply consumers with the right to use a musical content.[55] The reasoning of the United States built on the *US-Gambling* case under which "the GATS does not limit the various technologically possible means of delivery under mode 1". Finally, the principle of "technological neutrality" enshrined in the "Work Programme on Electronic Commerce" convinced the WTO panel and the Appellate Body that the term "distribution" covers the provision of sound recording through electronic means. See WTO Panel Report, China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products (China – Publications and Audiovisual Products), WT/DS363/R and Corr.1, adopted 19 January 2010, as modified by Appellate Body Report WT/DS363/AB/R.

[56] Ibid., paras. 7.1168–7.1265.

[57] See note 6.

[58] See also Henry S. Gao, "E-Commerce in ChAFTA: New Wine in Old Wineskins?", in Colin B Picker, Heng Wang and Weihuan Zhou (eds), The China Australia Free Trade Agreement: A Twenty-first-Century Model, (Oxford: Hart Publishing, 2018), 283–303.

[59] WTO General Council, Council for Trade in Goods, Council for Trade in Services, Committee on Trade and Development, Work Programme on Electronic Commerce: Aiming at the Eleventh Ministerial Conference, Communication from the People's Republic of China and Pakistan, Revision, JOB/GC/110/Rev.1, JOB/CTG/2/Rev.1, JOB/ SERV/243/Rev.1, JOB/DEV/39/Rev.1 (2016).

commerce initiative was officially established, China decided to get onboard.[60] Its official position issued in April 2019 stressed the importance of respecting each country's "design of the electronic commerce development paths, and the legitimate right to adopt regulatory measures in order to achieve reasonable public policy objectives".[61]

China acknowledged the US arguments to facilitate data flows and minimize data localization requirements. However, by referring to the "complexity and sensitivity" of these issues as well as to "the vastly divergent views among the Members", China concluded that the time was not ripe to discuss these issues in the early stages of the negotiation. Rather, the Chinese statement called for more exploratory discussions aimed at allowing Members "to fully understand their implications and impacts, as well as related challenges and opportunities".[62] Admittedly, this sounded as a diplomatic way to rule out any serious discussion of the matter. As of May 2022, 86 WTO members (China included) representing over 90% of global trade, have been taking part in the negotiations, which are still on-going under the lead of Australia, Japan and Singapore.[63] On 20 June 2022, the WTO Committee on Trade and Development welcomed the decision taken by the 12th Ministerial Conference (MC12) to reinvigorate activities under the Work Programme on E-Commerce.[64]

It is worth noting that China implicitly put forward an alternative proposal, albeit more modest, focused on trade-related aspects of data flows, which "are of great importance to trade development". Interestingly, the statement avoided to mention the concept of "free flow of data", which is how the US has always described the topic in its submissions. Conversely, data flows are considered by China worthy of free movement across borders only as long as they relate to trade in goods bought via online platforms yet delivered in physical forms offline.[65] This means that when it comes to other non-trade related circumstances, data could be legitimately locked in within each jurisdiction.

Last but not least, the wording at stake shows a clear reliance on the "policy space" exception, a concept developed in trade negotiations in order to justify differential treatments from agreed standards. This means that the national security concerns which represent the main pillar of domestic Chinese data governance are set to trigger general exception clauses under the traditional framework of the General Agreement on Tariffs and Trade (GATT) and General Agreement on Trade in Services (GATS) in order to shield the data content supervision on data entering and exiting the Chinese borders.

Accordingly, China pointed out that data flows "should be subject to the precondition of security" and should "flow orderly in compliance with Members' respective laws and regulations". By explicitly referring to the need of ensuring each WTO member full "internet sovereignty", China made clear the importance it attaches to shielding its data governance framework as well as the willingness to rule out that the cyber sphere could escape from national jurisdictions.

In line with this new approach, in November 2020 China signed the Regional and Comprehensive Economic Partnership (RCEP) Agreement.[66] Notably, the e-commerce chapter provides for

[60] Leika Kihara, "DAVOS – Nearly Half WTO Members Agree to Talks on New E-Commerce Rules", Reuters, 25 January 2019.

[61] WTO, Joint Statement on Electronic Commerce, Communication from China, INF/ECOM/ 19, 24 April 2019.

[62] WTO, Communication from China, par. 4.2.

[63] Ministers of Australia, Japan and Singapore, "WTO Joint Statement Initiative on E-commerce Statement", December 2021.

[64] WTO, "Ministerial Conference Decision - Work Programme on Electronic Commerce", 17 June 2022.

[65] Henry S. Gao, "Digital or Trade? The Contrasting Approaches of China and US to Digital Trade", Journal of International Economic Law, 2018, 21, 297-321.

[66] RCEP was signed between the ten ASEAN members and their major trading partners China, Japan, South Korea, Australia, and New Zealand, after India had departed the negotiations. It entered into force on 1 January 2022. As to the legal text of the RCEP Agreement, see here.

exceptions to the general cross-border data transfers and data localization rules based on countries' unconstrained self-assessment.[67] Indeed, provisions allowing data free flow as well as the prohibition for data localization and for requirements on source codes are not enforceable.[68]

3.2. Chinese approach to international technical standardization

In addition to adopting a cautious stance towards cross-border legislative harmonization, China has increasingly worked to build consensus around its data governance model in several Information and Communication Technology (ICT) governance institutions.[69] In particular, China voiced its position also within the UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security.[70] In all such fora, China emphasized the importance of preserving cyber sovereignty and ultimately country's domestic data governance policies.

Standards refers to defining and establishing uniform specifications and characteristics for products and services. Standards can facilitate the creation and integration of markets, foster positive feedback loops, reduce uncertainty in the marketplace, and lower costs and prices for downstream products.[71] By ensuring interoperability, they make networks more valuable.

China's first national plan for building a standardization system was introduced in 2015, when the BRI began to operate in full swing and the digital economy began to surge in China. Accordingly, standards connectivity between China and BRI countries and the promotion of China's standards along the BRI became one of the national plan's priorities. China's influence on the digital economy and related standard setting increasingly relies on Huawei and other private big tech firms and start-ups. In sum, the growing Chinese footprint in international technical standardization is not just a source of influence for Chinese companies but empowers the party-state. By exerting an influence over ICT technical standardization, China aims to control access to the technological enabler of data governance.

Given the importance of standards for the digital economy, China has prioritized its participation in standard development organizations (SDOs).[72] In particular, SDOs perform three main functions. They identify and unlock the value of various combinations of functionalities (discovery function); they select specific technological options and steer market players towards the systematic adoption of a particular technology (standardization function); and they require the owners of patents covered

---

[67] RCEP, arts. 12.14, 12.15. See also Thomas Streinz, "RCEP's Contribution to Global Data Governance", AfronomicsLaw, 19 February 2021.

[68] So Umezaki, "E-Commerce Provisions in the Regional Comprehensive Economic Partnership: A Milestone for a Global Rule?" (2022) IDE Research Columns; Patrick Leblond, "Digital Trade: Is RCEP the WTO's Future?" (2020) CIGI, stating that "the RCEP's chapter 12 is much weaker than the Comprehensive and Progressive Agreement for Trans-Pacific Partnership's chapter 14, to the point of rendering the provisions meaningless in terms of liberalizing cross-border digital trade and data flows".

[69] Among these, we find the International Telecommunication Union (ITU) as well as the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN).

[70] The group held its first meeting in 2019 and submitted its final report to the General Assembly in 2021. See here for more details. In order to escape US resistance, China set up in 2018 the Open Ended Working Group, which is an alternative group to the current one.

[71] OECD, 'Licensing of IP Rights and Competition Law' (2019) <http://www.oecd.org/daf/competition/licensing-of-ip-rights-and-competition-law.htm> accessed 5 December 2020.

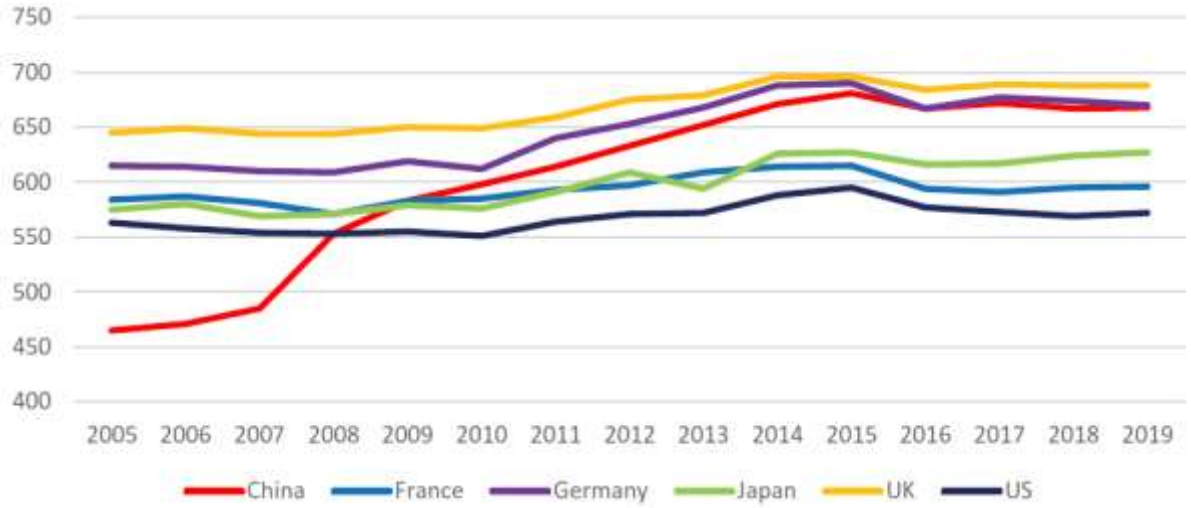
[72] Standards are often referred to as the building blocks of the modern global economy. They play a key role in ensuring interoperability and technical compatibility across a broad range of industries. Standards can facilitate the creation and integration of markets, foster positive feedback loops, reduce uncertainty in the marketplace and lower costs and prices for downstream products.

by the standard to grant licenses on fair, reasonable, and non-discriminatory (FRAND) terms (regulation function).

Strikingly, technical standardization is a crucial field of world-wide data governance. A country's ability to influence technical standardization carries influence in terms of national security, economic development, and international relation. Arguably, China's influence on international standardization does not only empower private actors but the Chinese party-state.[73] The issue got center stage in international relations as we are witnessing for the first time Chinese commercial and technological leadership in cellular networks, namely the fifth generation (5G) standard for transmission of mobile data.

Since 2008, China has significantly increased its engagement with the International Organization for Standardization (ISO), which is a world-wide leading SDOs also in the digital domain, and is now one of its most active participant (see Figure 6). More generally, these new technological capabilities allow Chinese players to exercise significant and growing influence in international technical standard-setting bodies.

Figure 6: Active membership in ISO - Technical Committees and Sub-committees[74]



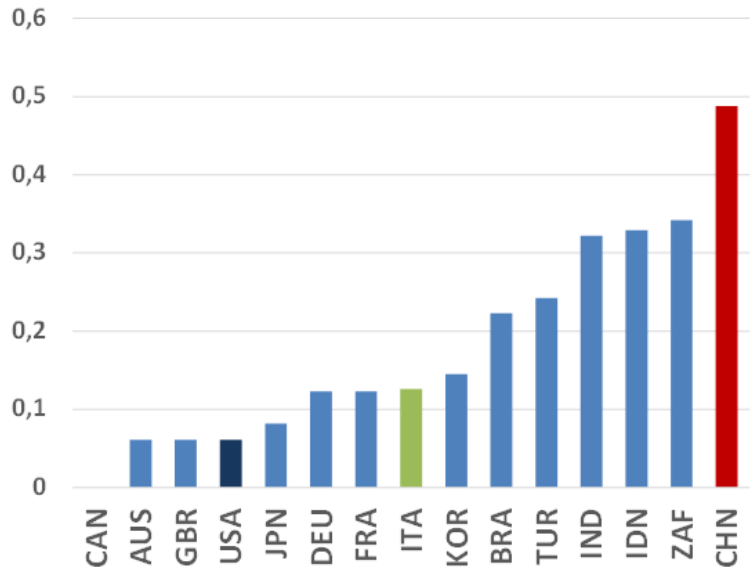
The Chinese strategy to popularize its vision for data governance as well as Internet control, including cyber sovereignty, relies on soft power initiatives as well. For instance, since 2014, the CAC and the People's Government of Zhejiang Province have been co-hosting the "World Internet Conference", also known as the "Wuzhen Summit" in Wuzhen, Zhejiang, the province that is the birthplace of Alibaba.[75] Further, there are a number of other initiative which contribute to emphasize Chinese data governance, such as the China-ASEAN Information Port Forum, the China-U.S. Internet Forum, the China-U.K. Internet Roundtable, the China-Singapore Internet Forum, and the China-Arab Countries Online Silk Road Forum. Finally, in September 2020, China advanced a Global Data Security

[73] Tim Rühlig, "Chinese Influence through Technical Standardization Power", Journal of Contemporary China, 2022.
[74] AFNOR.
[75] Matthew S. Erie, Thomas Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance", 54 N.Y.U. J. Int'l L. & Pol. 1 (2021), noting that "The Wuzhen Summit has been a vehicle for China to popularize its vision for the Internet, including cyber sovereignty".

Initiative, which stresses the importance to ensure countries' sovereignty, data management rights, and jurisdiction in cyberspaces.[76]

In summary, the Chinese approach to transnational data governance is fairly averse to the adoption of common rules. However, there can be exceptions as long as legal harmonization relates to trade and does not jeopardise national security concerns. While China avoided to engage extensively in international law negotiations involving data governance, it must be considered that it acted to gain more influence in global organizations and regulatory networks impacting data regulation.[77] This approach signals the willingness to leverage international diplomacy to maintain full control over domestic data governance as opposed to the "free data flow" narrative consistently voiced by the US. It is clear that, at the moment, Chinese policy makers have decided to prioritize domestic data control over the goal of facilitating digital economy expansion and the growth of its own digital champions by means of free data flows.[78] As shown in Figure 7, this is in line with the evidence gathered in the OECD Digital Services Trade Restrictiveness Index (DSTRI), which measures cross-cutting barriers that inhibit or completely prohibit firms' ability to supply services using electronic networks, regardless of the sector in which they operate.

Figure 7: OECD Digital Services Trade Restrictiveness Index[79]



[76] Wang Yi (China State Councilor and Minister of Foreign Affairs), "Acting on the Global Security Initiative to Safeguard World Peace and Tranquility", 24 April 2022.

[77] Zha Daojiong & Ting Dong, "China in international digital economy governance", China Economic Journal, 2022; Lizhi Liu, "The Rise of Data Politics: Digital China and the World", Studies in Comparative International Development, 2021.

[78] Angela Huyue Zhang, "Agility Over Stability: China's Great Reversal in Regulating the Platform Economy" Harvard International Law Journal, Vol. 63, No. 2, 2022.

[79] The OECD Going Digital Toolkit, based on the OECD Digital Services Trade Restrictiveness Index, https://oe.cd/stri-db.

4. The Digital Silk Road: data governance through infrastructural control

When dealing with data governance is important to acknowledge that data streams are a function of the underlying physical infrastructure.[80] As such, each country data governance hinges on a net of material components and related infrastructure, in the absence of which data cannot be transferred, stored, or processed. For instance, what is commonly known as the "Great Firewall" of China (GFW) is in reality a complex data control infrastructure that harness technical tools to exercise an intrusive (albeit far from absolute) level of control over internet communications. Thus, China's increasing influence in the global debate over data governance also relies on the ability of Chinese operators to develop, supply, and maintain the infrastructural pillars of the digital economy.

As a result, by manufacturing and providing physical components of modern digital networks on a global scale, China is able to influence transnational data governance also at the infrastructural level. Arguably, the infrastructural lever is playing a key role in complementing the trade diplomacy initiatives that China is carrying out to establish digital hegemony. This means that China is consistently acting to become an essential supplier of key infrastructure for sustaining the current digital economy in several countries. Since we are dealing with complex tools that often build on top of standardized solutions and require continued assistance and servicing from the provider, China is trying to become the orchestrator of a digital environment where hosting countries would be locked in from a technical perspective. The Digital Silk Road (DSR) appears as the perfect tool to implement this strategy.

Launched in 2017 within the framework of the Belt and Road Initiative (BRI), the DSR is China's global investment plan to build a complex digital infrastructure network connecting the world.[81] Over the last five years, this project has covered the most innovative areas of information and communication technology, such as the Internet of Things (IoT), fifth-generation (5G) mobile networks, artificial intelligence (AI), data centres, smart cities, cloud computing, and big data. While introducing the DSR at the first BRI Forum, Xi Jinping repeatedly mentioned the importance to deliver "cyberspace interoperability" in addition to connectivity as the main goal of this initiative.[82] By putting Xi's words into context, we can argue that China intends to lay the ground for data-driven trade between BRI countries through interoperable digital infrastructure built around common standards.

From an operational perspective, the DSR builds on two pillars. First, the focus of the DSR investments is on digital infrastructure such as data centers, smart city surveillance systems, terrestrial and submarine cables. Second, Chinese technology companies are systematically identified as the suppliers of such digital infrastructural projects. It is clear from this that China considers of the utmost importance to advance digital connectivity across beneficiary countries by fostering the influence of its own technological champions. Accordingly, this strategy is backed by new financial institutions focussed on non-Western countries, such as the Shanghai Cooperation Organization, the Asian

[80] Data and electronic communication flow on non-digital channels, such as copper and fiber-optic cables or through electromagnet radiation via antennas that build cell phone networks or via routers which underpin local-area networks (i.e., 5G, WiFi). Similarly, digital data are stored in thousands of massive data centers, which deploy as much energy power as a midsized city. Michele Savini Zangrandi, "Il ruolo geostrategico dei cavi sottomarini: le interconnessioni digitali come possibile ambito sanzionatorio", GeoTrade n. 2, 2021.

[81] As pointed out in Matthew S. Erie, Thomas Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance", 54 N.Y.U. J. Int'l L. & Pol. 1 (2021): "Policy documents over the years have interchangeably used "information silk road" (xinxi sichouzhilu), "silk road online" (wangshang sichouzhilu or hulian hutong zhi sichou zhilou), and "digital silk road," with a consensus usage preferring the latter as of roughly 2017, the year of the first BRI Forum in Beijing.".

[82] Xi Jinping, "Work Together to Build the Silk Road Economic Belt and the 21st Century Maritime Silk Road", Keynote Speech at the Opening Ceremony of the Belt and Road Forum for International Cooperation (14 May 2017).

Infrastructure Investment Bank, and the Silk Road Fund.[83] Notably, this strategy is enacted through private contracts, policy documents and memoranda of understandings (MOUs), rather than proper treaties under international law. This signals a marked difference with the approaches enacted by the EU and the US, which rely more on traditional international agreements (as pointed out in Section 1).

It is easy to grasp the importance of the DSR for transnational data flows (i.e. a key component of transnational data governance) by looking at the case of fiberoptic cables. They remain the world's most important physical infrastructure for channeling transnational data flows, that are a key enabler of cross-border trade in digital services.[84] For instance, China Mobile is involved in the "2Africa" project, which is about implanting one of the world's largest undersea cables (37000 kilometer) linking Africa, Middle East, and Europe.[85] Further, the Arctic Connect, a Finnish project in which Huawei took part, is seeking to link Asia to European countries by means of new submarine communication cable along the Northern Sea Route.[86]

Further, under the DSR several Chinese firms are setting up data centers in host countries. In 2017, Alibaba Cloud built cloud computing big data hubs called "Flying Apsaras Data Centers" (*feitian shuju zhongxin*) in seventeen regions of the world, including Malaysia, Indonesia, and Singapore, creating Asia's largest platform for cloud-based computing.[87] In August 2016, Alibaba launched the electronic world trade platform (eWTP), which is a private sector-led, multi-stakeholder initiative to promote public-private collaboration and dialogue in support of inclusive global trade (a sort of parallel World Trade Organisation for SMEs).[88] In November 2020, Huawei announced plans to build its third data centre in Thailand to turn the country into the digital hub of ASEAN China Telecom Global is building data centers in BRI countries to house large-capacity servers and data storage systems to host cloud computing services.[89] It remains to be seen if and how projects like these would take shape in the aftermath of the new set of export controls introduced by the US Commerce

[83] David Suter, "The Shanghai Cooperation Organisation a Chinese Practice of International Law", Zürcher Studien zum öffentlichen Recht N° 232 (Schulthess Publishers), 2015, ("There is even compelling reason
to believe that the agency of China was a conditio sine qua non to the path leading to, and ultimate founding of, this organisation. It is fair to say that China can make or break the SCO.").

[84] In the same vein, many other projects are taking shape: the submarine Bay of Bengal Gateway (BBG) and the Southeast Asia-Middle East-Western Europe submarine cable (SEA-ME-WE 5) across the Bay of Bengal, both with involvement of China Mobile; the Africa Europe-1 (AAE-1) submarine cable with participation by China Unicom; and the submarine Pakistan East Africa Cable Express that Huawei Marine is pursuing and for which the Chinese Hengtong group is supplying the fiber optic cable and two terrestrial cables, both with involvement of China Telecom: one between China (Kashgar) and Afghanistan (Faizabad) through the Wakhan region, the other between China (Jilongzhen) and Nepal (Rasuwagadi) outside Kathmandu. On this issue, see Michele Savini Zangrandi, "Il ruolo geostrategico dei cavi sottomarini: le interconnessioni digitali come possibile ambito sanzionatorio", GeoTrade n. 2, 2021.

[85] Reuters, "Facebook, telcos plan subsea cable to connect Africa, Middle East and Europe", 14 May 2020.

[86] The Arctic Connect subsea cable is a Finnish plan to link Europe and Asia through a submarine communication cable on the seabed along the Northern Sea Route (NSR). The total length of the Arctic Connect subsea cable will be 13,800 km. The Arctic Connect subsea cable project is expected to be finished between 2022-2023 with an estimated cost of 0.8 to 1.2 billion USD. See here for more details.

[87] Alibaba, "Alibaba Cloud to Launch New Data Centers and Innovate Products for a Hybrid Future", 21 October 2021. See also https://www.ewtp.org/.

[88] Financial Times, "Alibaba kicks off ambitious plan for frontier-free global trade", 22 March 2017.

[89] Huawei, "Huawei joins hands with PlanetComm to elevate competition in Thailand's Data Center Market", 3 October 2022; Komsan Tortermvasana, "Huawei investing B700m in new data centre in Thailand", Bangkok Post, 11 November 2020.

Departments' Bureau of Industry and Security on 7 October 2022 to restrict China's ability to both purchase and manufacture certain high-end chips.[90]

4.1. The role of Chinese hybrid firms

In order to appreciate the influence over data governance of the DSR, it is key to understand that both state-owned enterprises (SOEs) and large private firms take part in the DSR. However, regardless from their property structure, they generally operate in an agent-principal relationship with the party-state.[91] Contrary to SOEs operating in physical infrastructure, most of firms involved in the DSR are not formally state-owned as they emerged from private entrepreneurs, such as Alibaba Group Holding Limited ("Alibaba"), Tencent Holding Limited ("Tencent"), J.D.com Incorporated ("Jingdong"), Huawei Technologies Company Limited ("Huawei"), and ZTE Corporation ("ZTE").

While China's state-owned enterprises are unanimously considered as party-state actors, in the case of private technology firms an intense debate about the party's influence over their conduct has been going on over the last decade.[92] Indeed, many of these firms' ownership structure is opaque thereby leading to the suspicion of hidden state control. Unsurprisingly, US concerns with Chinese-based companies operating globally ranged from leakages of sensitive information to outright espionage. The relationship between the party-state and Chinese firms, especially when effectively state-owned, has been one of the most contentious issue in the US-China trade relationship.[93] Moreover, the recent regulatory crackdown on large technology firms has showed that the party-state is now actively trying to regain control over those few large technology firms that were perceived to be as more independent and free.[94]

Admittedly, large Chinese private companies are already under an implicit but significant party-state influence. On top of that, national security concerns justify a significant level of state-intrusion in Chinese companies' activities. For instance, the "National Intelligence Law" of 2018 and the "Counter-Espionage Law" of 2014 require private firms to submit data to the government upon request.[95] Moreover, state capture is set to take place also beyond traditional business-to-government data access tools. The "PRC Law", for instance, requires all private operators and in particular technology companies to host a party cell within their organization.[96] For example, Alibaba has 200

---

[90] US Department of Commerce's Bureau of Industry and Security (BIS), "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)", 7 October 2022.

[91] Margaret Pearson, Meg Rithmire and Kellee Tsai, "Party-State Capitalism in China" (2020) HBS Working Paper Series No. 21-065.

[92] Thomas Gatley, "Rise Of The Hybrid Firm", GavekalDragonomics, InDepth Report, 9/07/2022.

[93] US Department of Justice, Press Release, "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets", 13 February 2020, detailing how a superseding indictment was handed down in federal court in Brooklyn, New York, charging Huawei with violating the Racketeer Influenced and Corrupt Organizations Act; U.S. Dep't of Commerce, Press Release, "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies", 15 May 2020, restricting Huawei's ability to use U.S. technology and software to design and manufacture its semiconductors abroad because "Huawei is engaged in activities that are contrary to U.S. national security or foreign policy interests.

[94] See Edward White, "China's chaotic regulatory crackdown reflects splits among policymakers", Financial Times, 19 May 2022.

[95] National Intelligence Law of the PRC, as amended in 2018, art. 7 (requiring that any organization or citizen shall support national intelligence work); Counterespionage Law of the PRC (promulgated by the National People's Congress, effective since 1 November 2014), art. 22 (mandating that organizations shall provide information or evidence to a national security authority when requested to do so).

[96] Companies Law of the PRC (revised on 26 October 2018), art. 19, requiring companies to provide the "necessary conditions" to facilitate the activities of party organizations: "The Chinese Communist Party may, according to the

party representatives, Huawei has 300, and Tencent has 89. As such, in particular after the regulatory crackdown, it has become extremely difficult to disentangle Chinese largest technology platforms behaviour from the interests of the party-state.

Hence, it should not come as a surprise that the dominant Chinese telecommunication firms fostered their global penetration thanks to the DSR. The three major Chinese telecom companies (China Mobile, China Unicom, and China Telecom), for instance, increased their market share in several developing countries through M&A activities and partnership agreements.[97] Thus, China Unicom International Ethernet Private Line is now operating in fifty major regions and countries.[98] China Unicom has established a global cloud platform that enable users to access any cloud node from all over the world.[99] China Unicom, in the same vein, developed ten overseas subsidiaries and 21 offices which coordinate 4G services in 112 countries (including Russia, India, Indonesia, Myanmar, United Arab Emirates, Malaysia, Vietnam, Thailand, Kazakhstan, South Africa, and Philippines).

Similarly, ZTE and Huawei are heavily involved in DSR projects, especially with reference to surveillance technology.[100] Since 2019, China has supplied security technology devices to 63 countries, 36 of which are BRI beneficiaries. Huawei plays a prominent role in the supply of this technological equipment as it operates in over 50 countries. For its part, ZTE is actively present in 53 BRI countries by providing wired and wireless networks. This state-owned enterprise contributed to the establishment of data centres which serve as the enabling tool for the services offered by the Chinese private firms. For instance, ZTE committed $100 million in the Bangladesh National Data Center. This example shows how state-owned and private technology firms are acting in a complementary fashion within the DSR initiative in order to establish regional digital hegemony in favour of China.

Lastly, Chinese technology firms are not confined to the mere provision of telecommunication infrastructure. An increasing number of companies are now offering social media platform services.[101] While Tencent's Weixin has emerged as the leading platform in domestic China with almost one billion daily users, its version for outside China (WeChat) gathers about 100-200 million active users each month, mainly concentrated in Southeast Asia (such as Malaysia and Thailand where the app is used by 17% of mobile users).

Further, TikTok has taken centre stage in the global market for social networks. After merging with the US-based app Musical.ly in August 2018, it was fined by the US Federal Trade Commission for illegally collecting information about individuals under thirteen. Like its western most successful competitors, this platform is facing an increasing level of regulatory scrutiny all over the world both in terms of competition policy and personal data protection. As TikTok is the most successful case of

---

Constitution of the Chinese Communist Party, establish its branches in companies to carry out activities of the Chinese Communist Party. The company shall provide necessary conditions to facilitate the activities of the Party.".

[97] Mure Cickie, "China Mobile expands with Paktel deal", Financial Tiems, 21 January 2007, stating that China Mobile acquired 88.86 percent interest in Paktel Ltd., the first cellular operator in Pakistan, for $460 million); June Yoon, "China's 'homecomers' herald flow of deals", Financial Times, 12 May 2022.

[98] Interestingly, the U.S. Federal Communications Commission (FCC) on 27 January 2022 voted to revoke the authorization for China Unicom to operate in the United States, citing national security concerns. See here for more details.

[99] Matthew S. Erie, Thomas Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance", 54 N.Y.U. J. Int'l L. & Pol. 1 (2021)

[100] Steven Feldstein, "The Global Expansion of AI Surveillance", Carnegie Endowment For International Peace 16, September 2019, clarifying that the export of "AI surveillance" technology is common across liberal and authoritarian countries.

[101] Danielle Cave, Dr Samantha Hoffman, Alex Joske, Fergus Ryan, Elise Thomas, "Mapping China's Tech Giants", Australian Strategic Policy Institute, 18 April 2019.

a Chinese social network widely adopted across western countries, it is interesting to note which data governance issues it raised for foreign authorities.

In particular, US lawmakers and regulators have long feared that Chinese party-state officials could access US users' data gathered by TikTok. National security and foreign policy concerns were so serious that, on 6 August 2020, the US President Trump signed an executive order directing the app's Chinese owner, ByteDance, to either sell TikTok to an American business within 45 days or see it forcibly removed from app stores and blocked.[102] The deadline was extended several times, and Oracle emerged as potential partner for TikTok to store the US users' data in its own cloud servers. At the moment, the Chinese firms is reorganising its US operations in order to finalize a deal with the Biden administration that would let the video-sharing site keep operating in the US.[103]

In summary, it is now clear that the DSR coupled with the strong influence exercised by the Chinese state-party over large technology firms could allow China to play an essential role in the functioning of global data governance.

4.2. Building core data infrastructure dependencies

Overall, the DSR is contributing to a general development under which Chinese firms, are taking part in the control over the core data infrastructure. It is worth noting that several BRI deals, financed by Chinese development banks, require Chinese contractors to be involved not only in the building, but also in the maintenance of the relevant infrastructure. As a result, Chinese technology companies increase their role as essential technology providers in the realm of the digital economy.

The official data governance approach underpinning the DSR was clearly illustrated in the December 2017 launch of the "Belt and Road Digital Economy International Cooperation Initiative" by China and six other BRI beneficiary states (Laos, Saudi Arabia, Serbia, Thailand, Turkey, and the United Arab Emirates).[104] While many principles are vague recommendations on strengthening connectivity and improve broadband quality, there is a clear stance on fully respecting cyber sovereignty of each country. At the same time, the declaration aims at fostering the establishment of a "peaceful, safe, open, cooperative, and orderly cyberspace". Hence, a difficult balance should be found between the goals of facilitating open connectivity, on the one the one hand, and ensuring full governmental scrutiny over digital data on the other. Additionally, it signals the Chinese formal intention of not influencing at the official level domestic data governance of host countries. Further, the principles go beyond data governance by involving global internet governance, which, according to these countries, should be more "multilateral, democratic, and transparent".[105]

Arguably, the "Belt and Road Digital Economy International Cooperation Initiative" laid the ground for continued and sustained dialogue between China and hosting countries government, industry players, scientific and academic bodies. This cooperation is explicitly aimed at sharing "best practices" as wells as "policy formulation and legislative experience".

---

[102] Hannah Murphy, "TikTok says it is working to 'safeguard' US data and national security", Financial Times, 1 July 2022.

[103] Patrick McGee and Cristina Criddle, "TikTok overhauls US business following advertising slump" Financial Times, 8 November 2022; Daniel Flatley, Brody Ford, and Emily Birnbaum, "TikTok Deal Remains Elusive as Biden Administration Works to Solve Data Concerns", Bloomberg, 26 September 2022.

[104] "Launch of the "Belt and Road" Digital Economy International Cooperation Initiative, Cyberspace Administration of China, 11 May 2018. More details here.

[105] China has traditionally argued for "more governmental control over the Internet within, rather than outside, the U.N. framework". Matthew S. Erie, Thomas Streinz, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance", 54 N.Y.U. J. Int'l L. & Pol. 1 (2021)

As to global institutional cooperation, it is interesting to note that China is not intentionally trying to displace existing international organizations. Where feasible, the DSR has launched projects within established platforms for international coordination, such as the International Telecommunication Union (ITU) and WTO.[106] For instance, the Export-Import Bank of China in 2019 signed a memorandum of understanding with ITU for leveraging BRI within the context of the 2030 Agenda for Sustainable Development.[107] Similarly, China entered into several agreements with the ITU and countries of the East African Community and Ethiopia to build "information highways" (digital infrastructure) in East Africa. Also, it has been stated that the struggle towards better connectivity and broadband networks shall be "consistent with international rules, including WTO rules and principles".[108]

In brief, the DSR is a remarkable step in the global data governance strategy of China. Rather than focussing on international law tools such as treaties and legal harmonization, China is looking to develop the digital infrastructure of several countries around the world. At the same time, there is no apparent willingness to influence domestic data governance policies in terms of personal data protection or cross-border information flows, thereby reinforcing its diplomatic stance on the importance to ensure complete cyber sovereignty. This marks a difference with G7 infrastructure development assistance programs which are usually conditional upon economic and social reforms.[109]

Having said that, the Chinese strategy comes with several risks in terms of new potential dependencies that could influence host countries' policymaking and data governance. In particular, while China has consistently advocated for national sovereignty over data governance issues in international fora, it is actively trying to establish technological and infrastructural dependencies within the digital space of several countries, which could frustrate their ability to enjoy proper digital sovereignty.[110]

On a related note, it must be acknowledged that the rapid transition of developing countries towards digital integration could expose them to an additional risk. If digital transformation does not come with the development of proper legal safeguards (for instance, with regard to antitrust, platform regulation, and taxation), market failures and in-country inequality could be exacerbated rather than alleviated, not to mention the protection of freedom of expression and information. Indeed, there is nothing to stop digital market dynamics from generating in developing countries the same economic problems, which are already affecting Western countries (market monopolization, personal data abuses, consumer and business discrimination, self-preferencing, etc.). The lack of adequate rule-of-law frameworks is likely to exacerbate those problems even further. This is a risk that should be seriously considered when gauging the impact of accelerated digital transitions in developing countries as the ones triggered by the DSR.

---

[106] For an in-depth analysis of China's increasing influence over global standardization initiatives, see: Tim Rühlig, "Chinese Influence through Technical Standardization Power", Journal of Contemporary China, 2022; Alex He, "The Digital Silk Road and China's Influence on Standard Setting", CIGI Papers No. 264 — April 2022.

[107] Ministry of Foreign Affairs of China, "List of Deliverables of the Second Belt and Road Forum for International Cooperation, Global Times", 27 April 2019.

[108] The other countries are Laos, Saudi Arabia, Serbia, Thailand, Turkey, and the UAE.

[109] Gisela Grieger, "Towards a joint Western alternative to the Belt and Road Initiative?", European Parliamentary Research Service, 2021.

[110] More specifically, by developing the digital infrastructure, China surreptitiously aspires to implicitly intrude in their data governance architecture. Ultimately, host countries' digital economies would depend upon the services provided by Chinese technology firms and domestic authorities would be far away from enjoying full digital sovereignty.

5. Concluding remarks

Over the past five years, China has built a complex legal framework which forms now the country's domestic data governance system. This article illustrated the major pillars of such legislative body, highlighting how the Chinese policy maker tried to pursue its overarching policy goal, i.e. preserving party-state domestic control across the digital economy.[111]

In particular, Chinese data governance features a two-pronged legal architecture in which the Cyberspace Administration of China plays a prominent role. The first bulk of legislative measures hinges on cyber security considerations. Even though they provide the state-party with broad powers to access any kind of data within the Chinese jurisdiction as well as the data localization requirements, there are still uncertainties as to their ultimate scope. The second bulk of data governance legislation is more recent and focuses on personal data protection. While the "Data Security Law" set up a hierarchical system for data protection as well as new data localization requirements with the goal of ensuring national security, the "Personal Information Protection Law" aims to safeguard individuals' privacy and bargaining power vis-à-vis large technology firms.

In light of this understanding, the article assessed the impact of domestic data governance over Chinese trade policy in international fora. Overall, China has proved to be extremely averse to any international legal agreement which could undermine its domestic data governance framework. This means that any proposal aiming at facilitating cross-border flows of data is set to encounter a strong skepticism from Chinese delegations, as already happened in 2019 with reference to new WTO negotiation on electronic commerce. Having said that, the article pointed out that China is not completely unsympathetic to the pro-competitive impact of harmonized data frameworks facilitating digital trade as long as they do not adversely affect national security. In fact, the Joint Statement on Electronic Commerce issued by China on 23 April 2019 made clear that the country was open to negotiate new rules on trade-related aspects of data flows.

Arguably, this signal is going to be regarded as a useful starting point to build consensus among G20 countries with reference to the Data Free Flow with Trust and Cross-Border Data Flow initiatives within the Digital Economy Working Group. Notably, on 15-16 November 2022, the Leaders of G20 who gathered for the final 2022 meeting in Bali explicitly "committed to further enable data free flow with trust and promote cross-border data flows".[112] It will be interesting to follow how China will approach transnational data governance issues under the 2023 Indian G20 presidency.

On a more pragmatic note, new attempts to build international consensus on transnational data governance are likely to focus exclusively on the trade-related aspects of data governance in order to reach middle-ground solutions. This would mean finding common rules to enable public-private standardization initiatives within multilateral organisations (e.g. ITU) fostering interoperability and common data standards as well as harmonized API between manufacturers of smart devices at the global stage. While this approach would not cover the whole spectrum of issues involving data governance (such as the flows of sensitive personal data or government access to privately stored data), it could allow to build consensus around a first bulk of international rules facilitating cross-

[111] K. Buysse and D. Essers, "Should we fear China's brave new digital world?" 2022 NBB Economic Review 5.

[112] G20 Leaders, "Bali Declaration", 15-16 November 2022: "We remain committed to further enable data free flow with trust and promote cross-border data flows. We will advance a more inclusive, human-centric, empowering, and sustainable digital transformation. We also reaffirm the role of data for development, economic growth and social well-being"

border digital trade. As such, the work which the OECD is carrying out with reference to data governance and cross-border data flows is extremely useful to keep track of new developments.[113]

Last but not least, the article delved into the infrastructural lever of data governance. With the Digital Silk Road initiative, China has showed a clear commitment to penetrate the digital infrastructure of host countries by means of large investments favouring national ICT champions. Further, Chinese large technology firms are expected to complement the Chinese government's goal to have more influence on international technological standard-setting organizations thanks to the funding flowing from the Belt and Road Initiative. Thus, the DSR stands in stark contrast with China's explicit intention to preserve each country national sovereignty over data governance issues.

We highlighted that the Chinese attempts to enter developing countries digital infrastructure might undermine their own ability to exercise national self-determination in the realm of data governance. This is even truer if we consider that the rapid digital transformation brought by the DSR could backlash against hosting countries. In fact, such a quick development is taking place without participating countries paying attention to the existence of commensurate legal frameworks able to minimize the risks of market failures and the spread of in-country inequality (for instance, with regard to antitrust, platform regulation, and taxation). The fact that EU, Australia, UK, Canada, and US are still grappling with these issues makes the problem more urgent for developing countries targeted by China's digital investment projects. The digital integration can hardly deliver on its welfare-enhancing promises without adequate legal safeguards in place.

Overall, this analysis shows that Chinese transnational data governance goes well beyond formal legal frameworks as it deeply interacts with international trade policy and investment strategies involving digital infrastructure in foreign countries. At the same time, since the BRI and the DSR are still on-going, there is a need to carefully assess how they are unfolding on a case-by-case basis while being aware of the geo-strategic rationale underpinning such initiatives.

[113] OECD, "Cross-border data flows taking stock of key policies and initiatives", 2022.