One Data State, Two Data Logics: Unfolding China's Data Governance

Cancan Wang, Chunrong Liu

Abstract

China's data governance has recently caught international attention with its newly launched National Data Bureau. As China appears as a powerful data state on the global stage, its data governance presents a puzzling picture of interests between economic development, national security, and social justice, each demanding a different form of control, raising questions on the approach of Chinese state in the data domain. This chapter provides an account of China as a data state through its recent policies, regulations and their implementations. We argue that China's data state is not a monolithic top-down machine of control. Rather it is dynamic across contexts, with deliberate efforts to embrace different forms of data politics, that is contentious politics and institutional politics. This chapter serves as an exploratory effort of constructing a potential typology of data state by identifying two data logics (i.e., data as strategic assets and data as commons) that drive the building of China as a data state. We propose three future research directions to further this line of research by calling for a holistic perspective on China as a data state, comparison studies between China and other states' practices in the data domain, and more in-depth investigation into the relationship between state, public sector and tech giants.

Introduction

On March 7, 2023, during the annual National People's Congress session, China's State Council revealed its plan to establish a new government agency – a National Data Bureau (NDB), to centralize its management of the country's vast stores of data and deepen the reform of the Communist Party of China and the state institutions (The State Council of the People's Republic of China, 2023). The new bureau will be placed under China's main economic planning agency - the National Development and Reform Commission. According to the draft plan, the new bureau is set out to oversee "coordinating the integration, sharing, development, and utilization of data resources," and "pushing forward the planning and building of a Digital China, a digital economy, and a digital society." In this sense, NDB will split the data responsibility with the Cyberspace Administration of China (CAC), with NDB focusing primarily on data-related economic, social and technical development and CAC on data security.

On the one hand, the reorganization of the data management bureaus seems to confirm China's approach to data governance, which Cheung and Chen (2021, p. 2) referred to as the "data state", describing "a governance model enabling the state to comprehensively monitor, evaluate, and control its subjects through datafication". The reorganization also suggests that China's data state is specifically driven by two tropes of narratives, that is, development and security. However, looking closely at China's data governance practices, the state's relationships with citizens and businesses are not as stable, with priorities, such as, security, welfare and economic development often in-flux, painting a more complex picture about the role of the Chinese state in the data domain.

As different nation-states establish their own authority over the collection, processing, transfer, sale or use of data, China makes an interesting case from both an empirical and a theoretical point of view. Historically, China has long established the strategic importance of data in economic development and have sustained interests in utilizing data as an important instrument for social governance as exemplified in the social credit system initiative. Today, with Chinese tech giants' expansion domestically and across borders, China has become the center of politics around personal data, such as, data privacy and cross-border data transfer. Meanwhile, through movements such as open data, non-state actors such as citizens and civil organizations have also actively engaged in different forms of exploration that utilizes data to participate in various governance areas such public services and environmental issues.

Taking the point of departure that data is "a force generative of new forms of power relations" (Ruppert et al., 2017, p. 2), this chapter provides an account of China as a data state through its recent policies, regulations and their implementations. We argue that China's data state is not a monolithic top-down machine of control. Rather it is dynamic across contexts, with deliberate efforts to embrace different forms of data politics, that is *contentious politics* and *institutional politics.*

We start this chapter by contextualising the development of China's recent data policies, regulations, and initiatives. We argue such development heralds two forms of data politics institutional politics and contentious politics, and provides a typology that helps to explain these two concepts. We showcase how these two concepts can be used as heuristic devices for unpacking the relations between Chinese state, citizens, and businesses by analysing the narrative around the latest Data Security Law in China. We end the chapter with a suggestion for future research to investigate the state building practices around data in China.

Contextualising A Digital China

China's focus on data is a result of its sustained, long-term focus that dates back to the "reform and opening up" period in the 1980s, when the Chinese state has launched a series of parallel administrative reform and informatization policies that aimed to harness the potential of information technology to drive the transformation of economy and society (Qiang, 2007). In this section, we provide a historical overview of China's public administrative reform, contextualise how data and digital technologies took centre stage in China's policy focus, and highlight the changes and continuities across different periods.

Administrative Reform, Informatization, and E-government (1980s – 2000s)

Since the "reform and opening up" took place in 1978, China has undergone a series of market-oriented economic and political reforms, transitioning from planned economy to market economy. This also resulted in paralleled changes in public administration (Chen et al., 2017; Ma et al., 2005; Yu, 2018). After a decade of political uncertainty, the administrative reform was initially designed to support China's long-term economic development agenda. It started in the 1980s from an internal focus on clarifying functions between central and local government operations.

As the economic reform deepened with more state-owned enterprises becoming privatized in the 1990s, the focus of administrative reform has shifted to enhancing the transparency of internal processes, standardizing and strengthening coordination between market-facing government functions to better support the business activities that were on the rise. In parallel to the administrative form during this period, a lot of the emphasis began to be placed on harnessing the power of information technology to support the administrative reforms in relation to these aspects (Du & Wang, 2009; Holliday & Yep, 2005; Ma et al., 2005; Schlæger, 2013; Wu & Bauer, 2010).

In 1993, China initiated a series of "Informatization" plans, known as the three "Golden" projects (i.e., Golden-Bridge, Golden-Customs, and Golden-Card) to implement information technology management in the government (China Internet Network Information Center, 2016a). In 1999, three "Online" Projects (i.e., Government Online Projects, Enterprise Online Projects, and Family Online Projects) were announced, where all levels of government were required to build websites as windows to the public to deliver government information. At the same time, large-scale development of Internet infrastructure and personal computer facilities

took place to ensure country-wide Internet accessibility (Du & Wang, 2009; Holliday & Yep, 2005; Ma et al., 2005).

Marching into the early 2000s, the Chinese public administration underwent a transformation that largely resembled the new public management reform (Christensen & Fan, 2018). Central government started to push to reduce the cost of public transactions and improve the service quality to further support business development. This resulted in continued efforts in streamlining government by decentralizing government functions to local authorities, reducing redundant administrative examination and approval requirements, and eliminating overlapping functions within government agencies. These changes were accompanied by a new evaluation system of civil servants that is based on performance rather than adherence to formal processes.

In 2002, driven by the central government's push to reduce the cost of public transactions and improve the efficiency and quality of government decision-making processes and public services, the State Council announced its *No.17 Guidance on the Development of E-government* which aimed to converge three types of internal operations: government internal management and supervision; revenue and expenditure improvements; and social management and public services (Du & Wang, 2009). More specifically, the guidance reorganized the national plan for e-government development into four priorities: "Two Nets, One Website, Four Databases and Twelve Golden Systems". "Two Nets" referred to the building of government intranet and internet as the infrastructure for the Chinese e-government development. "One Website" was the national portal - www.gov.cn, which disseminates information from the State Council and the central government and functions as a catalog of government services and local government portals. "Four databases" covered database building for demographics, legal entities, natural resources and geographic information, and macroeconomic management. "Twelve Golden Systems" were aimed to accelerate the building of key information systems in twelve areas including fiscal government, agriculture, police, social security, tax, domestic and international trade, water governance, quality assurance, auditing, electronic currency and business. By 2010, these top-down e-government designs have largely been implemented (E-gov.org.cn, 2018).

Data and Digital China (2010s - present)

Entering into 2010s, social media based service apps such as WeChat, Taobao, Didi became central features in everyday social and economic life, and mobile payments replace cash for most daily economic transactions in China, producing unparalleled amount of data about

China's enterprises and citizens. This fast-paced digitization has spawned a series of tech firms and startups. By market capitalization, Alibaba and Tencent were ranked in the top 10 publicly traded corporations globally as of early 2020. In 2014, China elevated the status of big data to a national strategy (The State Council of the People's Republic of China, 2015a). As a follow up, in 2015, the Chinese Prime Minister Li Keqiang proposed an implementation plan for the big data strategy in the government work plan *the Internet Plus* (The State Council of the People's Republic of China, 2015b). In 2019, the central government has listed data as one of its five basic factors of production, alongside land, labor, capital and technology (National Development and Reform Commission, 2022).

Such rapid digitization also gave the Chinese government an opportunity to use data as a new bridge to foster collaborative governance with business and society and improve governance capability to promote law-based, people-centered, and scientific governance (People's Daily, 2018). One example is China's Social Credit Systems that has been under development since 2014. Much of the impetus derives from decades of unsustainable and corrupt business practices, a lack of trust towards economic actors in China (Dai, 2018), and failures in enforcing laws and regulations concerning economic activity across a range of industries (Zhang & Zhang, 2016). Thus, the core concept of Social Credit Systems is to impose "self-regulation of enterprise" in which businesses comply with laws and regulations of their own accord, thereby easing the burdens on existing enforcement and compliance structures (State Council, 2017).

In parallel to the top-down push for data utilization in governance, there was also a bottom-up open data movement from local governments, NGOs, research institutes and businesses that advocate for the use of government data to enhance transparency and improve the effectiveness and efficiency of public services. These local data movement resulted in local open data contests, data portals and data maps that are accessible for the citizens to monitor the quality of government services and jointly govern societal issues such as environmental issues (Gao 2018; Wang and Staykova 2019).

While data has provided ample opportunities for China's economic development and improving its governance capacity, it also has its own challenges. Domestically, data privacy has reportedly become a concern for citizens regarding ride-hailing, online shopping, social networks and other online services (Xinhua, 2018). Internationally, as the domestic success has driven China's digital sector to go global with Chinese tech companies such as Alibaba and

Didi becoming publicly listed in the US stock exchange, the trans-border data flow became a concern of national sovereignty (People.com.cn, 2022).

Since 2017, China has released three national-level laws, including the Personal Information Protection Law (PIPL), the Cyber Security Law (CSL), and the Data Security Law (DSL), making them three main pillars of data regulations in China. In February 2023, the Communist Party of China Central Committee and the State Council have rolled out a plan to build a digital China. The plan aims to ensure China becomes the global forefront of digital development by 2035 with three emphases: an effective interconnectivity in digital infrastructure, a significantly improved digital economy, and major breakthroughs achieved in digital technology innovation. The reorganization of data responsibilities between NDB and CAC is a first step into the further digitalisation of Chinese government, society and economy. While it has become obvious that the role of the Chinese state is growing in various data-related aspects in the country's social and economic life, how should we understand data governance in China, especially the role of the Chinese state in relation to citizens and businesses in the domain of data?

Datafication and the Return of State

China is hardly the only country that sees data as the lifeblood of its economy and society and has registered the proliferation of data or acts on the policy front. In general, the global society is undergoing a profound transformation of datafication, where "both system and life world are transmuted into data and/or mediated by data" (Beraldo & Milan, 2019, p. 1). As the mass collection, storage and analysis of data becomes possible, data has become a critical governing subject and an important source of new power dynamics (Ruppert et al., 2017), especially with regard to the role of the state and its sovereign power (Pohle & Thiel, 2021).

Starting in the 1990s when the early development of Internet flourished, Internet and computer-supported communication technologies were seen as the demise of state sovereignty in terms of national jurisdictions, legislative procedures, and the attribution of liability (Hassan, 1999). Scholars have predicted the decline in the importance of state, as democracy in the West were anticipated to be more closely associated with participation from the private sector and the civil society (e.g., Coleman & Blumler, 2009). Indeed, as the commercialisation of the Internet deepened, corporate actors such as Google and Facebook who own vital digital infrastructures and have access to a paramount amount of personal data started to emerge (Birch & Bronson, 2022). Through the enormous resources they command and the ways they exercise control,

the so-called tech giants have become one of the biggest challenges to democracy and the state's sovereign power (Pohle & Thiel, 2021; Zuboff, 2019).

Meanwhile, the Big Data technologies have also enabled states to conduct large-scale surveillance not only on its own citizens but also across national territories. In 2013, the computer security consultant Edward Snowden revealed the classified global surveillance programmes run by the US government in cooperation with the intelligence services of Australia, the UK and Canada, where government intelligence services and tech companies were acting like sovereign entities across territorial boundaries. After a short period of backlash, political actors managed to take advantage of the exposure, by highlighting the risks of foreign surveillance, manipulation and disinformation using data, triggering a demand for national sovereignty, thus "the return of state" in a digital domain (Pohle & Thiel, 2021).

The exposure of existing mass surveillance programme and tech giants' abuse of personal data also made citizens aware of the exploitative process inherent in datafication and the lack of involvement of citizens in generating and utilising knowledge about themselves. As a response, groups of citizens and civic organizations began to reconsider the agency of the publics and explore new forms of participation and political engagement, such as the open data movement, that utilise collaborative ways of organizing, evaluating and acting with data to instigate more inclusive and responsible data futures (Baack, 2015; Beraldo & Milan, 2019; Lehtiniemi & Ruckenstein, 2019).

Along this line, state and its sovereignty, defined as the state's authority over a specific domain, that are traditionally thought to be the bedrock of modern politics, have become a contested area in the advent of datafication, especially regarding its strategic interactions with sovereign states, or with non-state actors such as businesses and citizens (Liu, 2021). It also reveals different logics that drive the state's involvement in datafication, posing questions such as how can national security and privacy coexist in entrepreneurial innovation-based use of data? And to what extent can we imagine China as a data state within its socio-economic context?

One Data State, Two Data Politics

Against this background, there is emerging research regarding how data generates new political problems in China, and the role of state in data domains. Scholars are particularly interested in the role of the Chinese state, regarding its interactions with non-state actors (Aho & Duffield, 2020; Cheung & Chen, 2021) and other states (Liu, 2021). For instance, based on the study of Social Credit Systems, Cheung and Chen focus on the heightened social control by Chinese

state that is enabled by datafication. They coined the term "data state" to describe "a governance model enabling the state to comprehensively monitor, evaluate, and control its subjects through datafication"(Cheung & Chen, 2021, p. 2). Focusing on China's global engagement in the data domain, Liu investigated how China's Cybersecurity Law affected non-Chinese tech companies' activities in China, and the influence of the EU and the US' regulations and political initiatives on Chinese tech companies such as social media company TikTok and bike-riding startup Mobike. Liu argues that data has generated new political and economic problems that shapes the Chinese state's approach to sovereignty in the data domain.

These studies often emphasise the importance of top-down control from central government in China's data state. Drawing on existing studies and different empirical examples, we argue that China's state-led approach to economic development and the transition from a planned to a market economy has largely shaped its governance approach to data. Meanwhile, through policy experimentation and regulations, the Chinese state also tries to adapt to bottom-up data movement such as open data. China's data state is therefore multifaceted and dynamic depending on the governance areas.

We introduce two concepts - institutional and contentious politics, as heuristic devices to unpack how China's data state is driven by a duality of data logics. On the one hand, there is an institutional politics which highlights data as a strategic asset of the state, thus focusing primarily on market-driven efficiency and national security in the policy and legislative practice around the use, sale and transfer of data. On the other hand, the data state also addresses the contentious politics which foregrounds data as commons, thus pays attention to the interests of citizens and civil society actors, such as welfare, justice and privacy related issues in the collection, processing and use of data (see Table 1).

Table 1. Two Politics of China's Data State

Politics	**Driving data logics**	**Emphasis**	**Policy Narrative**	**Political Process**
Institutional Politics	Data as strategic assets	Market-driven efficiency National security Surveillance	Digital economy Data security Digital sovereignty	Top-down
Contentious Politics	Data as common goods	Welfare Justice	Open Data Data Rights	Bottom-up

		Privacy		

Institutional Politics on Economic Development and Administrative Reform

The emerging research on the data state suggests data is a new strategic asset for the state, thus affecting its engagement with other states and non-state actors, such as businesses and citizens (Jørgensen, 2021; Liu, 2021; Tupasela et al., 2020). These studies are built upon the assumption that data is a new type of economic good with two characteristics: nonrivalry and partial excludability, generating specific political and economic problems requiring state coordination. Nonrivalry means that data can be reused indefinitely and by many parties simultaneously, which has two economic implications: when widely shared across firms and countries, there may be substantial social gains; when concentrated in a few firms and countries, it can generate a competitive advantage against other actors in the market. Partial excludability means that it is not always possible to prevent nonpaying individuals from consuming data. This is because data is inexpensive to duplicate and transfer over a long distance, which generates a high risk for unauthorized sales, usage, or theft of data. Although data can be made excludable through encryption, anonymization or offline storage, these methods can be costly and makes the data less valuable. This line of research argues that data as an economic good can lead to both positive benefits for welfare and economic development, and negative consequences on privacy and surveillance. But politically unfettered market coordination and voluntary efforts are often limited for mitigating the negative consequences. Thus, the state has become central in establishing political orders around data.

Similarly, the Chinese state frames data as a functional need for the efficiency and productivity of Chinese economy and encourages corporate actors to utilize data in economic activities. For instance, in the Chinese government work plan Internet Plus (2015 - 2020), advanced data-driven technologies are viewed as key in transforming conventional industries including manufacturing, finance, medical systems, and agriculture (The State Council of the People's Republic of China, 2015b). In 2020, the state council formally designated data as factor of production for generating economic value. Since then, China has embarked on a process of carefully defining property rights for data, including the type of stakeholders and their rights, the purpose and process of usage, and a granular categorization of data types (Boullenois, 2021). In a series of government workplans and announcements issued by the Chinese central government, specific measures were outlined to strengthen its data economy, including

developing data infrastructures, with the aim of "activating the value of data as a production factor" to "create a strong domestic market that is innovation-driven and high-quality" (The Central Commission for Cybersecurity and Informatization, 2021).

The logic of data as a strategic asset has also found its way through policy initiatives on welfare and administrative reform. In 2015, through the Internet Plus government work plan, the Chinese central government put emphasis on integrating data technologies into the government design and operations. As we have illustrated, the strategic importance of data was the result of the Chinese government's long-term focus on harnessing the power of information technologies in administrative reform. Nonetheless, the Chinese tech giants including Alibaba and Tencent, and domestic telecommunication companies such as China Mobile, China Telecom and Huawei have actively pushed for public-private partnerships in providing digital public infrastructures and services. Since 2014, Alibaba and Tencent have been competing against each other to jointly develop public services with provincial governments on platforms such as WeChat and Alipay. In 2017, the competition intensified to the extent that Tencent and the state-owned telecom giant China Telecom have won tenders on cloud computing platforms with a price tag of "Zero Yuan". According to China Economic Weekly – a branch of the Chinese Communist Party's mouthpiece People's Daily, the "Zero Yuan" tender is a result of turf battle to gain access on government data between the private and state-owned Chinese tech giants (Sina Finance, 2018).

Institutional Politics on Data Security

While the domestic collection and sharing of personal data promises positive welfare and economic gains, the possibility of trans-border data exchange can also expose citizens to foreign surveillance, hacking, and data breaches. There are two uncertainties regarding the reuse of data that generates concerns about foreign government surveillance: 1) multi-national firms may share personal data with their home government; 2) the home government may abuse personal data for surveillance or other political purposes that encroach on individual liberty. The logic of data as a strategic asset, in this sense, also drives the Chinese state to emphasise data security and sovereignty in their data governance practices (Liu, 2021).

In 2014, the same year as the Big Data national strategy announcement, the concept of "comprehensive national security" that emphasises safeguarding state sovereignty and territorial integrity also started to arise. At the first meeting of the Central National Security Commission, President Xi remarked that comprehensive national security should "take

people's security as the purpose, political security as the base, economic security as the foundation, military, cultural and social security as the guarantee, and promotion of international security as the backbone, thus embarking on a national security path with Chinese characteristics"(China.com.cn, 2014). While the statement demonstrates the importance of security as a national concern, it also shows the different meanings security can take on in different contexts, ranging from military defense to economic stability that point more towards stable income to sustain the population's needs of living.

In 2021, the Data Security Law (DSL) was issued as a legal mechanism to calibrate state control over data security, which refers to "ensuring that data is effectively protected and lawfully used through adopting necessary measures, and to processing the capacity to guarantee the continuous security of data" (The National People's Congress of the People's Republic China, 2021).The DSL suggests that the approach to data security should be congruent with the overall approach to national security, and focus on establishing sound data security governance system, as well as improving data security and data protection capabilities. The DSL (i.e., chapter 3 Data Security Systems) asserted that the state is responsible for the decision-making, deliberation, and coordination of the national security work, including researching, formulating, and guiding the implementation of the national security strategy and related major guidelines and policies. The state is also in charge of establishing a coordination mechanism as well as coordinating major work that is related to national data security. Meanwhile, the DSL encourages the participation of societal actors including relevant government departments, industry organizations, research institutions, enterprises, and individuals in data security protection.

The voluntary participation of market is critical for the implementation of security consideration in practice, as they are often quite generic and loose at a policy level. For this reason, the Chinese state used the DSL to advocate for the development of data security as an industry and views the law as an institutional push for such development. In return, these initiatives that aimed to drive the development of data security as an industry are also supposed to drive the development of the *data industry in general*. These initiatives include 1) implementing the big data strategy, advancing the construction of data *infrastructure*, and encouraging and supporting the application of data across industries and fields; 2) advancing the *standardization* of data utilization and security; 3) encouraging the development of *data security services* including data security testing, evaluation and accreditation, especially based on the service required by the law; 4) establishing a *data trading market* that supports the flow

of data in the development of digital economy; and 5) developing *national capabilities* in data securities by supporting education and research institutions, enterprises, and other entities in carrying out education and training (The National People's Congress of the People's Republic China, 2021).

Domestically, the Chinese state especially emphasizes the relation of data security to the development of public services. Even though there is no specification in terms of which public services that data security would help to improve, the Chinese state asserts their support in data development and utilization to render public services smarter (The National People's Congress of the People's Republic China, 2021). Big vendors such as Tencent responded to the state's security concerns with detailed blueprints on how they would implement them in the services they provide to the public sector. For instance, in 2020, Tencent has issued a white paper on the security of government collaboration platform, detailing on their plans and experiences working with data security in the public sector (China Daily, 2020).

Internationally, on the one hand, the Chinese state portrays itself as an active participant in the international exchange and collaboration, especially in the making of international rules and standards for data security, in order to promote "safe and free flow of data across borders" (The National People's Congress of the People's Republic China, 2021). On the other hand, the DSL also emphasizes that the Chinese state applies export control on data related to controlled items and concerns national security and interests and the performance of international obligations. It also warns that the Chinese state may take countermeasures against the country or the region if any country or region adopts discriminatory prohibitions, restrictions, or other similar measures against the People's Republic of China in respect of investment, trade or any other field related to data and data development and utilization technologies. In 2020, days after China's ride-hailing giant Didi announced the company's IPO on the New York Stock Exchange, China's national data security agency CAC started a year-long investigation into Didi's data collection and processing methods. In 2021, the CAC fined Didi 8.026 billion yuan ($1.19 billion) for violating China's network security law, data security law and personal information protection law. According to a released statement by the CAC, Didi had illegally processed 64.7 billion pieces of personal information since 2015, including users' age group information, home addresses, locations, driver education and other data. Two months before the verdict, Didi's investors voted to delist from the New York Stock Exchange, putting a stop to the uncertainties posed by potential transborder exchange of personal data (People.com.cn, 2022).

Overall, from the standpoint of "comprehensive national security" one can argue, the Chinese state is incentivized to regulate data security for at least two reasons: first, safeguarding the development of a digital economy with data as a key factor of production; and second, protecting the data-related rights and interests of individuals and businesses. While the Chinese state asserts its control on data security matters, it however requires market participation to develop detailed implementation plan in different areas such as public services, and has diverse approaches to data security.

Contentious Politics

Another view of data that drives the Chinese state's approach to data governance is the idea of data as commons. Civic data that is shared to the public is often considered as a 'data commons'. In this case, data is not viewed as a private asset owned by a company or a strategic asset of the state, but a common resource shared by members of a community. A key concern here is how non-market mechanisms are used by communities to enact data stewardship and to ensure sustainability of such resources (Beckwith et al., 2019, pp. 208–209). We argue that the logic of data as commons has found its way through a bottom-up political process that we refer to as contentious politics. In general, contentious politics occurs when ordinary people - often in alliance with more influential citizens and with changes in public mood - join forces in confrontation with elites, authorities, and opponents. When backed by well-structured social networks and galvanized by culturally resonant, action-oriented symbols, contentious politics take the form of social movements (Tarrow, 2011, p. 6).

The logic of data as commons puts forward concerns about the value, ownership, accessibility, and collection of data that often needs negotiation and arbitration among the community. For example, the value of a database can be difficult to discern in the abstract without proper analysis. This uncertain value makes it difficult to know when the privacy interest ought to succumb to the public interest in data sharing, as well as to what extent data collection is sufficient in the public interest and when it is not (Yakowitz, 2011, p. 10). Given data is often created through the interaction of multiple parties, each stakeholder may feel entitled to claim ownership of created data, generating questions about who in a community can or cannot have access to certain data, what is the appropriate form of data stewardship, and what is the role of state. The role of state is particularly interesting in terms of its relationship with local community and the non-market mechanisms used by communities to govern data commons.

In the past decade, China has seen exponential growth in the availability of public data. Since 2012, there has been a push to make civic data available through open public data movements. Open public data is defined as "non-privacy-restricted and non-confidential data which is produced with public money and is made available without any restrictions on its usage or distribution" (Janssen et al., 2012, p. 258), which draws parallel to the state-coordinated development of big data. While open public data is gradually being institutionalised across more than half of the provinces in China today through local regulations, it was initially driven by global movement on open knowledge and open data (Wang & Perriam, 2022). Domestically, it involves journalists and NGOs that are active in specific domains such as environmental protection and is often driven by interests that represent the citizens' welfare and lawful rights. As the movement developed, these drives are translated into local initiatives and data platforms that satisfy the need of data disclosure and encourage citizens' use of data in a way that makes sense to the market as well (Gao, 2018).

These local experiments and initiatives in the opening and utilization of public data have paved the way for a national push around open public data. In January 2018, Shanghai Beijing, Zhejiang, Fujian, and Guizhou were appointed as pilot municipalities and provinces to open their local public data (Xinhua Daily Telegraph, 2018). Interestingly, in the DSL, there is a full chapter (Chapter 5 Security and Openness of Government Data) that deliberates the relationships between the security and openness of government data. Focusing on the government database, the DSL promotes the use of government data for economic and social development. In doing so, the state organs, including both central and local governments, are required to disclose government data in a timely and accurate manner, under "the principles of fairness, equality and convenience for the people" (The National People's Congress of the People's Republic China, 2021). The state seems to have signed up for three roles in opening government data, including 1) formulating the catalog of open government data, 2) building an open, standardized, interconnected, safe and controllable government data platform, and 3) promoting the release and utilization of government data.

Meanwhile, the Chinese state also emphasizes the security of government data by inserting itself at the center of building data security management systems and setting the parameters for the appropriate use of government data. For instance, when Chinese governments collect or use data to perform their statutory duties, they are only allowed to do so within the scope as needed for performance of their statutory duties and under the legal and regulatory conditions and procedures provided. Matters such as personal privacy, personal information, trade secrets,

and confidential business information are particularly mentioned to be protected (Article 38). Indirectly, this also means that when Chinese governments entrust a private actor to develop or maintain digial public services, they are also supposed to exert control of private actors through "strict approval procedures" and supervision of the private actors' performance of data security protection obligations (Article 40).

On the one hand, one can interpret the emphasis on data related rights as an indicator of Chinese policymakers' sensitivity to the tendency of monopolistic and unfair competition by tech giants. Recent data regulations thus strive to protect consumers from collective harms arising from data technologies. On the other hand, through the DSL, the Chinese state is also securing individual rights in order to pave way for the development of a lawful digital economy. The DSL, along with the *Personal Information protection Law* which went into effect on November 1 2021, shows some elements reminiscent of the EU's GDPR in processing personal information (Aho & Duffield, 2020). In this sense, individual and organization's rights around data are viewed as the foundation to ensure the free flow and the effective use of data.

Concluding Remarks and Future Research

In this chapter, we have explored China's data state as a collective of emerging institutions and norms that arbitrate the usage, collection, and protection of data. Through the illustration of a series of data polities, regulations, and their implementation in China, we have demonstrated two different data logics that are driving the Chinese state's approach to data governance, namely data as strategic asset, and data as commons. These examples do not always seem to create a coherent and consistent imaginary of China as a data state that is organized entirely top-down (Cheung & Chen, 2021; Liu, 2021). Rather, they portrayed an image of the Chinese data state as "fragmented authoritarianism" in which state power is segmented due to bureaucratic ranking system and marketisation, entailing constant resource mobilization and consensus building in both vertical and horizontal dimensions (Mertha, 2009). It is in this institutional makeup that we can observe the multiple faces of Chinese state as "developmental state", "regulatory state" and "security state", which have been rigorously developed and tested in practice (e.g., Knight, 2014; Wang & Minzner, 2015; Yang, 2017).

Our analysis suggests an alternative account of data governance dynamics that entails sustained developments of existing state practices while adapting to emerging norms. The Chinese data state embodies the characteristics of managing the contradictions of pursuing economic development and innovation, preserving national security, as well as accommodating the needs

of welfare and social justice. Overall, this paper serves as an exploratory effort of constructing a potential typology of the data state by identifying relevant data logics that drive the building of China as a data state. Future research can take the theoretical proposal of a data state into at least three directions:

Calling for a holistic perspective on understanding China as a data state

We argue that China's data governance is multifaceted and not locked into one logic that is driven by either the social control of its citizens (Cheung & Chen, 2021) or guarding data as a strategic asset against other states (Liu, 2021). Instead, it is a highly dynamic action field with local experiments and central coordination, which has been evolving over time. As data is presented across China's social and economic fabrics, a holistic perspective is needed in considering the emerging role of the Chinese state in the data domain.

In the studies we drew our conceptual inspiration from the popular assumption that state is autonomous from society has been challenged (Wang, 2016). A diverse set of literatures has emerged to scrutinize the role of strategic interactions from non-state actors in shaping economic and social governance across the sectoral and territorial configurations. Researchers have pointed out that for the state to be effective, it largely relies on society providing elements of support. As society steps into new spheres such as the digital domain, the state also retains its governability by mapping its terrain, demarcating its people and developing new governance capacities (Scott, 2020). In turn, the state is also critical for collective action in society (Kohli, 2002; Migdal, 2001).

In our study, we have shown that datafication has rendered the boundaries of state-society and state-market blurrier in governance areas where the Chinese state traditionally takes the coordinating role, inviting the imaginaries of data state as an action field with competing narratives and multiple alternatives. We advocate for the concept of institutional politics and contentious politics as heuristic devices to unpack the nature and dynamics of China as a data state in practice, by identifying different driving data logics and their manifestations.

For instance, the DSL can be seen as the Chinese state's attempts to carefully embrace both data logics as strategic assets and commons, but questions if it is possible in practice. How could the development of a data security industry support smart public services? Can such developments place the needs and interests of "the elderly and the disabled" at the center? Domestically, would data security measures introduce new bureaucratic processes around security reviews? How would such centralized processes shape open public data, especially

considering the participation of citizens and civil society organizations in the access, processing, and application of such data?

Future research could also investigate the policy-making processes behind data regulations to understand how different data logics are enacted. For instance, researchers can investigate the hearing process of a regulation by looking at who the participants are, what their inputs are, and how inputs are addressed in different iterations of the drafts. From a structural-strategic perspective, data governance can be viewed as a complex process of cross-sectoral negotiation, strategic coordination, and institutional balancing (Jessop, 1990). It is through these socialization processes that a wide range of social conditions for data regulations are produced and multiple alternatives are manifested. This line of thinking offers a potentially promising perspective that shed new light on the institutional mechanism that shape the form and strength of the data state in comparative perspective.

Internationally, following the advent of DSL, how would the Chinese state act towards the emerging Chinese tech giants, such as TikTok, Tencent and Alibaba, as they seek capital internationally? Understanding such cases would help to reveal the boundary conditions under which different data logics take place.

Comparison studies on data state

Researchers could also engage in international comparison, such as between China and the EU, on the different governance models and driving logics of data state. For instance, following Zuboff (2015)'s notion of surveillance capitalism, there is an emerging strand of research investigating the driving data logics for the Nordic states (Tupasela et al., 2020). For example, Tupasela, Snell, and Tarkkala argue that the states of Finland and Denmark are driven by a logic of data accumulation where data is seen as a strategic asset of a nation and a new source of wealth. Similarly, previous research based on Nordic countries has established how digital transformation is discursively constructed in a way whereby neoliberal ideas of development that is closely related to businesses, framed as functional need for efficiency and productivity (Henriksson et al., 2019; Schou & Hjelholt, 2018, 2019). As such, datafication is built into the idea of marketization and a new regime of practices of institutionalized surveillance (Zuboff, 2015).

In the EU context, the term 'digital sovereignty' is invoked as a basis of safeguarding European values in the digital age. The EU's digital governance, especially in the practices of data protection, data processing and utilization, and cross-border data transfer, has been

characterized with a comprehensive regulator system which internally focuses on the protection of individual data rights and externally sets high standards on the cross-border transfer of data (i.e., through GDPR). However, analysis of the existing EU policies on digital sovereignty has demonstrated that although the policies pertaining to data governance may help to achieve some of the EU's claims regarding data rights, they are also listed with an aim to advance the EU's competitiveness and regulate the private sector (Aho & Duffield, 2020; Roberts et al., 2021). While such different aims may, in fact, be contradictory in safeguarding European values, they also showcase the divergence in the data logics that drive the formation of a data state, and the need to unpack the boundary conditions for these data logics to manifest. Existing studies on digital sovereignty are largely built upon analysis of EU policies. A comparison across nation-states would be thus beneficial for the theorising of data state as a concept across political and institutional regimes.

Understanding the relationship between state, public sector and tech giants

In our study, the Chinese state largely encourages the Chinese tech giants to innovate with data to drive economic development and administrative reform. Although the Chinese state seems to have a tight control over the transborder data exchange, it also largely relies on the companies, such as Tencent, Alibaba and China Telecom, to provide more concrete security implementation security measures. This speaks to some of the existing studies on how tech giants have managed to find ways of accumulating data through public-private collaboration around 'smart governance'. Jørgensen (2021) criticises the current approach to 'smart governance', which on the surface seems like a happy marriage between tech giants and the digital welfare state. She argues such approach is built upon the narratives of data maximisation and techno optimism, which doesn't always place people and communities, especially minorities and the disadvantaged at the centre. She suggests that an uncriticised development of the digital welfare state may "disempower citizens and advance a digital technocracy that treats its citizens as data points suited for calculation and prediction"(Jørgensen, 2021, p. 2). It may also act against government's declared imaginaries of digital future that is constituted by human agency, individual control over data and fundamental rights.

Along this line of research, tech giants also interfere with the state at highly sensitive points, making them one of the biggest challenges to the idea of democratic sovereignty. Future studies could investigate how corporate actors that own vital digital platforms making up the infrastructure of our society, thrive in the commercialised internet environment, command

enormous resources, and exercise control on consumers in ways that near or go beyond the capabilities of nation-state.

References

Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, *49*(2), 187–212.

Baack, S. (2015). Datafication and empowerment: How the open data movement re-articulates notions of democracy, participation, and journalism. *Big Data & Society*, *2*(2), 2053951715594634. https://doi.org/10.1177/2053951715594634

Beckwith, R., Sherry, J., & Prendergast, D. (2019). Data Flow in the Smart City: Open Data Versus the Commons. In *The Hackable City* (pp. 205–221). Springer, Singapore.

Beraldo, D., & Milan, S. (2019). From data politics to the contentious politics of data. *Big Data & Society*, *6*(2), 2053951719885967.

Birch, K., & Bronson, K. (2022). Big tech. In *Science as Culture* (Vol. 31, Issue 1, pp. 1–14). Taylor & Francis.

Boullenois, C. (2021). China's Data Strategy: Creating a state-led market. *European Union Institute for Security Studies*.

Chen, Y., Dawes, S. S., & Chen, S. (2017). E-government Support for Administrative Reform in China. *Proceedings of the 18th Annual International Conference on Digital Government Research - Dg.o '17*, 329–335. https://doi.org/10.1145/3085228.3085269

Cheung, A. S., & Chen, Y. (2021). From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications. *Law & Social Inquiry*, 1–35.

China Daily. (2020). *Tencent has released <White Paper on the Security of Government Collaboration Platform>, facilitating the upgrade and iteration of digital government initiatives (腾讯云发布《政务协同平台安全白皮书》，助力数字政务升级迭代)*. https://caijing.chinadaily.com.cn/a/202009/04/WS5f51f207a310084978423538.html

China.com.cn. (2014). *Interpret China: Comprehensive National Security（解读中国：总体国家安全观）*. http://guoqing.china.com.cn/node_7204306.htm

Christensen, T., & Fan, Y. (2018). Post-New Public Management: A new administrative paradigm for China? *International Review of Administrative Sciences*, *84*(2), 389–404. https://doi.org/10.1177/0020852316633513

Coleman, S., & Blumler, J. G. (2009). *The Internet and Democratic Citizenship: Theory, Practice and Policy*. Cambridge University Press.

Du, L., & Wang, J. (2009). 我国电子政务发展回顾 (A Review of E-government Development in China). *E-Government*, *10*, 19–25.

E-gov.org.cn. (2018). *Twelve Golden Initiatives: One National Website, Four Databases, and Twelve Golden Initaitives*. http://www.e-gov.org.cn/article-166340.html

Gao, F. (2018, May 7). Driving urban innovation with open data: The birth of the Shanghai model. *Paris Innovation Review*. http://parisinnovationreview.com/articles-en/driving-urban-innovation-with-open-data-the-birth-of-the-shanghai-model

Hassan, R. (1999). GLOBALIZATION: INFORMATION TECHNOLOGY AND CULTURE WITHIN THE SPACE ECONOMY OF LATE CAPITALISM. *Information, Communication & Society*, *2*(3), 300–317. https://doi.org/10.1080/136911899359600

Henriksson, M., Witzell, J., & Isaksson, K. (2019). All change or business as usual? The discursive framing of digitalized smart accessibility in Sweden. *Transportation Research Procedia*, *41*, 625–636.

Holliday, I., & Yep, R. (2005). E-government in China. *Public Administration and Development*, *25*(3), 239–249. https://doi.org/10.1002/pad.361

Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management*, *29*(4), 258–268.

Jessop, B. (1990). Regulation theories in retrospect and prospect. *Economy and Society*, *19*(2), 153–216.

Jørgensen, R. F. (2021). Data and rights in the digital welfare state: The case of Denmark. *Information, Communication & Society*, *0*(0), 1–16. https://doi.org/10.1080/1369118X.2021.1934069

Knight, J. B. (2014). China as a developmental state. *The World Economy*, *37*(10), 1335–1347.

Kohli, A. (2002). *State, Society and Development. In Katznelson, Ira and Helen Milner (eds.), Political Science: The State of the Discipline (pp. 84-117). New York: Norton.* (Katznelson, Ira, & H. Milner, Eds.). Norton.

Lehtiniemi, T., & Ruckenstein, M. (2019). The social imaginaries of data activism. *Big Data & Society*, *6*(1), 2053951718821146. https://doi.org/10.1177/2053951718821146

Liu, L. (2021). The rise of data politics: Digital China and the world. *Studies in Comparative International Development*, *56*(1), 45–67.

Ma, L., Chung, J., & Thorson, S. (2005). E-government in China: Bringing economic development through administrative reform. *Government Information Quarterly*, *22*(1), 20–37. https://doi.org/10.1016/j.giq.2004.10.001

Mertha, A. (2009). "Fragmented authoritarianism 2.0": Political pluralization in the Chinese policy process. *The China Quarterly*, *200*, 995–1012.

Migdal, J. S. (2001). *State in society: Studying how states and societies transform and constitute one another*. Cambridge University Press.

National Development and Reform Commission. (2022). *Promoting the efficient circulation of data and accelerating the high-quality market development of data as a production factor*. https://www.ndrc.gov.cn/xxgk/jd/jd/202212/t20221219_1343662.html

People.com.cn. (2022). *Cyberspace Administration of China: Didi's data activities severely affects national security（国家网信办：滴滴存在严重影响国家安全的数据处理活动）*. http://finance.people.com.cn/n1/2022/0721/c1004-32482059.html

People's Daily. (2018). *用新思想指导新时代的社会治理创新 (New ideas for guiding social innovation in public governance in the new era)*. http://opinion.people.com.cn/n1/2018/0206/c1003-29807206.html

Pohle, J., & Thiel, T. (2021). Digital sovereignty. *Practicing Sovereignty: Digital Involvement in Times of Crises*, 47–67.

Qiang, C. Z.-W. (2007). *China's information revolution: Managing the economic and social transformation*. World Bank.

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*.

Ruppert, E., Isin, E., & Bigo, D. (2017). Data politics. *Big Data & Society*, *4*(2), 2053951717717749. https://doi.org/10.1177/2053951717717749

Schlæger, J. (2013). *E-Government in China: Technology, Power and Local Government Reform*. Routledge.

Schou, J., & Hjelholt, M. (2018). Digital citizenship and neoliberalization: Governing digital citizens in Denmark. *Citizenship Studies*, *22*(5), 507–522.

Schou, J., & Hjelholt, M. (2019). Digitalizing the welfare state: Citizenship discourses in Danish digitalization strategies from 2002 to 2015. *Critical Policy Studies*, *13*(1), 3–22.

Scott, J. C. (2020). *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Yale University Press.

Sina Finance. (2018). *Behind Tencent and China Telecom's Zero Yuan Tender: The cost of government cloud services is low, and the services are highly homogenous.（腾讯中国电信零元中标背后：政务云成本不高同质化严重）*. http://finance.sina.com.cn/roll/2017-07-24/doc-ifyihrit1334810.shtml

Tarrow, S. (2011). Global, conventional and warring movements and the suppression of contention. Themes in contentious politics research. *Política & Sociedade*, *10*(18), 25.

The Central Commission for Cybersecurity and Informatization. (2021). *The Central Commission for Cybersecurity and Informatization issued 14th Five-Year Plan for National Informatization (中央网络安全和信息化委员会印发《"十四五"国家信息化规划》)*. http://www.gov.cn/xinwen/2021-12/28/content_5664872.htm

The National People's Congress of the People's Republic China. (2021). *Data Security Law of the People's Republic of China*. http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml

The State Council of the People's Republic of China. (2015a). *Notice of the State Council on Issuing the Action Outline for Promoting the Development of Big Data*. http://en.pkulaw.cn/Display.aspx?lib=law&Cgid=256434

The State Council of the People's Republic of China. (2015b, December 31). *Premier Li Keqiang and Internet Plus*. http://english.gov.cn/policies/infographics/2015/12/31/content_281475263938767.htm

The State Council of the People's Republic of China. (2023). *The State Council of the People's Republic of China announced <Reform Plan of Party and State Institutions>*

（中共中央 国务院印发《党和国家机构改革方案》）.
http://www.gov.cn/zhengce/2023-03/16/content_5747072.htm

Tupasela, A., Snell, K., & Tarkkala, H. (2020). The Nordic data imaginary. *Big Data & Society*, *7*(1), 2053951720907107. https://doi.org/10.1177/2053951720907107

Wang, C., & Perriam, J. (2022). Murder Maps, Transport Apps, and Soup. *Historical Social Research/Historische Sozialforschung*, *47*(3 (181), 111–141.

Wang, Y. (2016). Beyond local protectionism: China's state–business relations in the last two decades. *The China Quarterly*, *226*, 319–341.

Wang, Y., & Minzner, C. (2015). The rise of the Chinese security state. *The China Quarterly*, *222*, 339–359.

Wu, Y. H., & Bauer, J. M. (2010). E-government in China: Deployment and driving forces of provincial government portals. *Chinese Journal of Communication*, *3*(3), 290–310. https://doi.org/Doi 10.1080/17544750.2010.499633

Xinhua. (2018). *Compliance supervision is becoming stricter, but there are still many safety hazards—Investigation of safety issues in the ride-hailing market（合规监管趋严，安全隐患仍不少——网约车市场安全调查）*.
http://www.xinhuanet.com/politics/2018-09/17/c_1123442268.htm

Xinhua Daily Telegraph. (2018). *Beijing, Shanghai, Zhejiang, Fujian, and Guizhou appointed as pilot areas to open local public information resources ("京沪浙闽黔将试点公共信息资源开放")*. http://www.xinhuanet.com/mrdx/2018-01/06/c_136875526.htm

Yakowitz, J. (2011). *TRAGEDY OF THE DATA COMMONS*. *25*(1), 67.

Yang, D. L. (2017). China's Illiberal Regulatory State in Comparative Perspective. *Chinese Political Science Review*, *2*(1), 114–133. https://doi.org/10.1007/s41111-017-0059-x

Yu, K. (2018). 中国的治理改革（1978-2018）(Aministrative Reform in China (1978-2018)). *武汉大学学报（哲学社会科学版）(Wuhan University Journal (Philosphy & Social Science))*, *71*(3), 48–59. https://doi.org/10.14086/j.cnki.wujss.2018.03.004

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019*. Profile Books.