§ 7 CHINA'S DATA STRATEGIES: INSTITUTIONALISATION, ACTIVATION, AND LAYERING

Content

A. Introduction: Data Strategies on Paper and in Practice

1 This chapter asks the question: what are China's data strategies in practice? On paper the Communist Party of China (CPC) and state actors (the party-state[1]) have stipulated many data policies and laws with strategic goals. Yet this chapter uses doctrinal and qualitative evidence to argue that in practice, the Chinese party-state adopt data strategies that can be conceptualised as institutionalisation, activation and layering, which help co-produce a knowledge-based regulatory state and a national digital economy. This conceptualisation draws from an institutionalist approach to law and economics, which emphasises law's role in co-producing the economy[2], coding/contesting property[3], and the law's co-evolution with technology in a path-dependent, non-ergodic and historically layered fashion[4].

I. China's Data Strategies expressed on Paper/in Policies

2 China's data strategies on paper officially appeared in 2015 under the rise of big data, when the CPC for the first time raised the concept of 'national big data strategy' in its top-level policy report.[5] Soon the State Council (SC) – China's top executive branch – stipulated *The Action Plan for Promoting Big data Development* (2015), aimed at competing with Obama's 2012 *Plan on Big data*.[6]

3 In March 2016, the National People's Congress (NPC) – China's highest legislator – passed *China's 13th Five-Year Plan (2016–2020)*, with Chapter 27 named as 'Implementing the National Big-data Strategy'. It specifically required the state to 'accelerate the opening and sharing of government data' (sec. 1), and 'promote healthy development of the big data industry' (sec. 2).[7]

---

[1] This chapter uses the phrase 'party-state' to simply mean both the CPC and state actors, their meshed relationship in the policy-making and strategy-implementation processes and as evidenced below. Party-state here is used as a more descriptive term, without addressing the 'party-state' question in Chinese studies, for example, on China's unique model of party-state capitalism or the cadre responsibility system. See e.g. Pearson/Rithmire/Tsai, *Current History* (2021) 120 (827): 207–213. Edin, in: Critical Readings on the Communist Party of China (4 Vols. Set), 2017.

[2] See, e.g., Deakin et al., *Journal of Comparative Economics* 45.1 (2017), 188–200. Ostrom, *American Economic Review* 100.3 (2010): 641–72. Deakin/Meng, *Journal of Institutional Economics* (2021): 1–15.

[3] Pistor, *The code of capital*, 2019. Ostrom, Beyond markets and states: polycentric governance of complex economic systems, *American Economic Review* 100.3 (2010): 641-72. Deakin/Meng, Resolving Douglass C. North's 'puzzle' concerning China's household responsibility system, *Journal of Institutional Economics* (2021): 1–15.

[4] Deakin, 7 *Review of Law and Economics* (2011). Deakin/Markou, Evolutionary Law and Economics: Theory and Method, *Northern Ireland Legal Quarterly* 72.4 (2021). Peters, The ergodicity problem in economics, *Nature Physics* 15.12 (2019): 1216–1221. Zuo, Governance by Algorithm: China's Social Credit System, 2020.

[5] 授权发布:中国共产党第十八届中央委员会第五次全体会议公报-新华网 (xinhuanet.com) [Report of the Fifth Plenary Session of the 18th Communist Party of China (CPC) Central Committee, 2015.] (last accessed 16 December 2022).

[6] 国务院关于印发促进大数据发展行动纲要的通知国发〔2015〕50号）[State Council's instructions on the action plans for promoting big data development, 2015. SC [2015] 50.]; Obama administration unveils "big data" initiative: announces $200 million in new r&d investments (Executive Office of the President, 2012).

[7] 中华人民共和国国民经济和社会发展第十三个五年规划纲要 [The 13th Five-Year Plan of the People's Republic of China on economic and social development, 2016].

The State Council followed up accordingly that year by issuing the *Provisional Measures on Government Information Resources Sharing* (2016) with the aim to regulate and facilitate the data flows between governmental agencies.[8] In December 2016, *The Big Data Industry Development Plan (2016–2020)* was promulgated as a leading industrial policy for big-data and the digital economy by the Ministry of Industry and Information Technology (MIIT). It opens with the claim that 'data is a national and foundational strategic resource; and it is the "diamonds mine" in the 21st century.'[9] 4

Moreover, China's data strategy can be seen as a foundation for and against the background of China's other national development strategies (at least on paper/in policies). In 2017, the Central Committee of the CPC emphasised in its top-level policy document (the *19th Report)* the need to 'integrate the Internet, *big data*, and artificial intelligence (AI) into the real economy (*shiti jingji*)' in order to 'build a Strong Manufacturing Nation'.[10] 5

The 'Strong Manufacturing Nation' goal is listed under Chapter Five of the *Report* –'Implementing New Development Visions', which also includes Sec. 2 'building an Innovative Nation'. The Innovation Nation project envisages an accelerated application of China's fundamental research and critical technologies in order to support projects like 'Strength in Cyberspace', 'Digital China', and 'Smart Society'.[11] It was around the same time (2015–2017) that national projects like 'Social Credit' (2014), 'Smart Cities' (2016), and 'Smart Courts' (2017) were promoted by high-level policy documents and action plans. These projects all require data-sharing, building data centres, and innovating data applications[12]. 6

In 2019, China's data strategies on paper expanded to agriculture and geographically to the rural regions with its 'Digital Villages'[13]. This project is supposed to cover more than 540 million people living in rural areas (2020), i.e. around 38.5 % of China's entire population (2020) and more than 1.5 times of the U.S. population (2020).[14] It started with the central Party-state's joint policy document *Strategic Plan for Digital Villages Development (2019)*[15]. This *Strategic Plan* was followed by the *2019–2025 Development Plan (2020)*[16], *Key Working Points (2020)*[17] and most recently the *Directives 1.0* (2021) 7

[8] 国务院关于印发政务信息资源共享管理暂行办法的通知国发〔2016〕51号〕 [State Council on the provisional measures to government information resources sharing and management. 2016, SC [2016] 51.] (last accessed 16 December 2022).

[9] 工业和信息化部关于印发大数据产业发展规划20162020年〕的通知 [MIIT on issuing the Big-data Industry Development Plan. MIIT [2016] 412.] available at http://www.cac.gov.cn/2017-01/17/c_1120330820.htm (last accessed 16 December 2022).

[10] 习近平决胜全面建成小康社会 夺取新时代中国特色社会主义伟大胜利——在中国共产党第十九次全国代表大会上的报告[Xi, Jinping, Report Delivered at the 19th National Congress of the Communist Party of China – Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era, 2017.10.18], available at http://www.gov.cn/zhuanti/2017-10/27/content_5234876.htm (last accessed 16 December 2022).

[11] *Ibid.*

[12] E.g. 国务院关于印发社会信用体系建设规划纲要2014—2020年〕的通知 ; 最高人民法院关于加快建设智慧法院的意见 ; 中共中央办公厅 国务院办公厅印发《国家信息化发展战略纲要》.

[13] 中共中央办公厅 国务院办公厅印发《数字乡村发展战略纲要》.

[14] Rural population – China | Data (worldbank.org); rural population (% of total population) – China | Data (worldbank.org); total Population – United States | Data (worldbank.org) 329,484,123 US population.

[15] 中共中央办公厅 国务院办公厅印发《数字乡村发展战略纲要》.

[16] 农业农村部　中央网络安全和信息化委员会办公室关于印发《数字农业农村发展规划2019–2025年〕》的通知〕》.

[17] 中央网信办等四部门联合印发《2020年数字乡村发展工作要点》.

for details of implementations[18]. These implementation policies and directives are all stipulated by the Cyberspace Administration of China (CAC) together with other top-level ministries, and they intend to shape China's rural data strategies and digital economy, for example by building public data platforms, big-data centres and introducing 'smart agriculture' applications, which are similar to their urban counterparts[19]. Some case studies were raised in the *Directives 1.0* (2021)[20], and practices like the *Blockchain Chicken Farm* also emerged[21].

8 While expanding agriculturally and geographically, China's data strategies also became more clearly market-oriented on paper. In 2020, the central Party-state for the first time jointly defined data as the fifth 'essential factor (of production)' following land, labour, capital, and technology in the top-level policy document *Instruction on Improving the Market Mechanism for Allocating Essential Factors (2020).* The document requires the state to 'foster a data factor market' by first, 'advancing open government data and sharing' (sec. 20), second, 'increasing the value of data resources' (sec. 21), and third, 'strengthening the integration and security protection of data resources' (sec. 22). Some emphases include to 'guide and cultivate the big-data trading market, and start data-trading according to laws and regulations' (sec. 26), and 'establish and improve mechanisms on data property transactions (*chanquan jiaoyi*) and self-governance by industrial associations' (sec. 27).[22]

II. Research Question and Gap of Understanding

9 While China's data strategies on paper have been laid out extensively, this chapter asks the question: what are China's data strategies in practice? Sub-questions include the following. Is data 'secured' and 'integrated' as the Party-state required in 2020? To whom and what extent do governments share data? Is data trading or 'property transaction' working well? Has the 'value of data' been realised?

10 For example, in contrast to the policy vision of data 'property transaction', as of January 2022, Chinese national laws in practice (deliberately) leave a grey zone for data property transactions and ownership, which encourages local and industrial experimentations (see below the Activation strategy)[23]. In fact, China's new Civil Code (2021) reaffirms that there is no clear data 'property' or 'ownership' at the national level (yet), which means doctrinally Chinese courts still cannot enforce traditional contractual clauses that cover data transactions[24]. Shenzhen also failed to write 'data property

[18] www.cac.gov.cn/rootimages/uploadimg/1632256402882582/1632256402882582.pdf (last accessed 16 December 2022).

[19] See, e.g. chapter 3 and 4 of the Directive 2021, available at www.cac.gov.cn/rootimages/uploadimg/1632256402882582/1632256402882582.pdf (last accessed 16 December 2022).

[20] *Ibid.*

[21] See Wang, Xiaowei. *Blockchain chicken farm: and other stories of tech in China's countryside*, 2020.

[22] 中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见 [CPC central committee and State Council: Instruction on Improving the Market Mechanism for Allocating Essential Factors, 2020.3.30.].

[23] See Part D.

[24] For a literature review of Chinese legal debates on data property rights, see 孔祥俊商业数据权数字时代的新型工业产权，《比较法研究》，202201）pp 2–3; 彭辉数据权属的逻辑结构与赋权边界，《比较法研究》, 202201）. It is also worth noting that China's Civil Code Article 127 stated that 'abide by laws where data and internet virtual assets are protected'. This is understood more as a protection for virtual assets like coins in online game purchases rather than data sets.

rights' into its municipal data legislation (2021)[25]. Many Chinese scholars have in fact recently argued against a general data property rights.[26]

A potential alternative to 'property transaction' is to use licensing, sharing or 'contact' (*jiechu*) agreements under intellectual property (IP) laws to approximate data sets as IP objects. However, legal professionals have pointed out the risk is that current Chinese IP laws do not clarify data as IP objects[27]. Legal scholars recently raised possibilities for 'data compulsory licensing' (*qiangzhi xuke*) based on 'essential facilities' provisions in antitrust and IP laws[28]. However, the *2021 Antitrust Guideline on Platform Economy* in its final version scrapped the part on 'considering data as an essential facility' (*cf.* Draft 2020).[29] Kong (2022) recently argued that instead of a general data property, China should start by stipulating 'commercial data rights' under IP law which delineate industrial data from more sensitive data types like personal/public data. This is an attempt to specify data governance regimes and use trade/commercial secret law as an inspiration to create new 'industrial IP rights' categories[30]. **11**

Moreover, Feng argued for an unfair competition law approach to protect those data interests that do not qualify for IP protections.[31] For example, the Hangzhou Internet Court ruled (and Hangzhou Intermediary Court affirmed) in the 'Wechat/Tencent unfair competition case' (2019, 2020) that the two plaintiffs (corporations of Tencent) have 'competition interests (*jngzheng quanyi*)' with regards to their 'data resource totality (*shuju ziyuan zhengti*)'. It also explicitly ruled that these corporations are only limited to the right of use rights to their 'individual data units (*danyi shuju geti*)' rather than the whole bundle of property rights.[32] **12**

Besides property, IP, and compulsory licensing, and the unfair competition protection, legal professionals also discussed the potential of data service agreements (as a service, AAS) to help data transaction and flow, especially concerning increasing data localisation rules around the world[33]. There are also five local Data Exchanges as emerging data brokers who experiment new modes of data transactions as of January 2022 (Guizhou 2015, Shaanxi 2015, Beijing 2021, Shanghai 2021, Changsha 2022), where Beijing raised the idea of 'use without retaining' (similar to AAS)[34]. But, in short, China's data trading and 'property transaction' is still in a legal grey zone, and there is a gap of understanding on the rapidly evolving practices being experimented. **13**

Moreover, very few works in the existing literature have comprehensively examined China's data strategies in practice. Ding briefly discussed China's global data strategy based **14**

[25] See Part D. II. Also see legal scholar's discussions: 地方无权对"数据权"立法深圳数据条例意见稿引专家热议 available at https://www.xuehua.us/a/5f15cb4ce3809536eb952075?lang=zh-cn (last accessed 16 December 2022).

[26] See literature reviews in 彭辉数据权属的逻辑结构与赋权边界，《比较法研究》, 202201）. 孔祥俊商业数据权数字时代的新型工业产权，《比较法研究》，202201）.

[27] See e.g. . 数据交易合同的法律问题 | China Law Insight; 刘一民律师数据交易架构和数据许可.

[28] 曾彩霞，朱雪忠数字经济背景下构建数据强制许可制度的合理性，基本原则和监管思路. 《电子政务》2021. 陈永伟: 数据是否应适用必需设施原则——基于"两种错误"的分析，《竞争政策研究》2021:4. 李世佳: 论数据构成必需设施的标准——兼评《关于平台经济领域的反垄断指南》第十四条之修改, 河南财经政法大学学报. 2021, 36 (05).

[29] *Cf.* Antitrust Guideline 2021 and 2020 draft.

[30] 孔祥俊商业数据权数字时代的新型工业产权，《比较法研究》，202201）.

[31] 冯晓青数据财产化及其法律规制的理论阐释与构建 《政法论丛》202104）.

[32] ((2019) 浙8601民初1987号 [2019, Zhejiang, 8601 Civil first instance case no. 1987]; 2020）浙01民终5889号 [2020, Zhejiang, 01 Civil appeal case no. 5889].

[33] 数据交易合同的法律问题 | China Law Insight; 刘一民律师数据交易架构和数据许可.

[34] See 中部地区唯一新型数据交易所在长沙试运营|长沙市_新浪财经_新浪网 (sina.com.cn); also see D. II.

on existing legal and policy documents.[35] Dai used a law and economics approach to conceptualise the government's strategies to use reputation in a 2x2 matrix of 'regulation', 'searchlight', 'incorporation' and 'institutionalization' (figure 1). This conceptualisation touches on China's data strategies in the case of the Social Credit System (SCS), where for example public data is shared and used by public authorities in public administration. But Dai's paper does not intend to systematically examine the data practices or strategies involved. He also suggests a deficit of empirical evidence in his research.[36]

	Private sector information	**Public sector information**
Private actors' decision-making	regulation	searchlight
Public authorities' decision-making	incorporation	institutionalization

Figure 1. Dai's 2x2 martix for the theorisations of state strategies in the SCS, see n 36

15 This chapter fills a gap of understanding on China's data strategies in practice. It builds on doctrinal and empirical evidence and adopts an institutionalist approach in order to provide better conceptual models. The chapter argues that China's data strategies can be understood in practice as:

(1) Institutionalisation[37], or the co-production of formal institutions by public and private actors to address data harms/risks and stabilise the expectations of these actors;
(2) activation, or the party-state's adoptions of flexible policies and practices in order to mobilise data sharing and use, and
(3) layering, or the construction of long-term data habitat/ecosystems in order to achieve high-value data use and interpretation.

16 These practical strategies emerged to deal with three real predicaments in China's data governance:

(1) Security and privacy concerns under concentrated corporate (and state) power;
(2) fragmented data access and use by private and public actors; and
(3) the lack of valuable data use, interpretation, and long-term scaling.

III. Scope and Structure of the Chapter

17 The chapter limits the scope of discussion to China's data strategies practised within its borders. It is worth noting that China does not have explicit laws or policies on its

[35] 丁晓东构建全球数据竞争的中国战略，学习时报，2020 [Ding, Xiaodong, Qiushi.cn (last accessed 9 October 2020)].

[36] Dai, Xin. "Toward A Reputation State: A Comprehensive View of China's Social Credit System Project." *Social Credit Rating: Reputation und Vertrauen beurteilen* (2020): 139–163.

[37] This is broader than Dai's definition of the state's 'institutionalization strategy' in 2018, which means the government's use of its own public data for reputational regulations (G2G), such as the Shanghai public credit information system that provides public risk-scores for corporations. In this chapter however, institutionalision means setting up formal legal frameworks as focal points in order to allow organisations and individuals to compete and coordinate, mostly for private actors but not for governments. The government's data sharing would be more relevant in the second strategy of *activation*. Institutionalisation in this chapter nevertheless includes Dai's other three state data strategies in terms of reputational governance, i.e. regulation (of private reputation data market like Uber and Airbnb, B2B), searchlight (public information used by private individuals and corporations for decision-making, G2B), and incorporation (private data used for public decision-making, B2G).

extra-territorial data strategy, except for a 'Global Data Security Initiative' published by the Chinese Foreign Ministry (2020)[38]. However, recent Chinese laws and regulations have in practice formed a territorially defensive data strategy that prevents certain data from crossing China's geographical border. These practices include the stipulation of data localisation rules[39] and security reviews for cross-border data transfer, which culminated in the 2021 CAC review of DiDi's IPO in New York (C.).

18 In contrast to this formally instituted defensive strategy of retaining data within Chinese borders, it can be argued that China in practice has informally carried out an extra-territorial data strategy under the name of the 'digital silk road' (DSR). The DSR idea was first raised in a speech given by President Xi Jinping to corporate and to government partners around the world at the '2017 Belt-and-Road Initiative (BRI) Summit'[40]. Since then, many public and private practices were identified as the DSR, including the early 'China-Myanmar land cable networks' (2014) built by China Unicom[41], the 2017 DSR summits respectively held between China and the Czech Republic, Hungary and Serbia, the 'Digital Hub' jointly set up by China's Alibaba and a Malaysian company in Kuala Lumpur (2018), the 'China-Philippine Data Harbour' (2018) and so on[42]. These practices, together with the recent expansion of Chinese big-tech companies abroad, contributed to the apprehensions on whether China's DSR would in practice 'control the global internet' and shape the order of global digital governance. Even without explicit state policies, China's investments, businesses, and ICT infrastructure constructions are viewed as practices of China's expansive data strategy in African, Asian, European, and Latin American countries via the BRI[43]. Some argued that these expansive practices constitute a hard 'Beijing effect' compared to the soft 'Brussels effect'[44].

19 This chapter focuses on China's domestic data strategy in practice, and all qualitative evidence is collected in cities rather than villages, due to practical limits of the fieldwork and the scope of this chapter.

20 The chapter proceeds by first introducing its institutionalist framing and the conceptual models of institutionalisation, activation, and layering (B. Institutionalist Theory, Conceptual Model and Methodology). It then discusses these three data strategies respectively by analysing doctrinal and qualitative evidence (C. Institutionalisation: Data Security, Protection, and Antitrust, D. Activation: Data Property, Commons, or 'Party manages data'?, E. Layering: Data Cycles, Local Habitats, and Sustainable Design), and in the end concludes (F. Conclusion).

B. Institutionalist Theory, Conceptual Model and Methodology

21 The conceptual categories of institutionalisation, activation, and layering are inspired by institutionalist theories of law and economics. Institutionalisation draws from the state's

[38] 外交部全球数据安全倡议, Foreign Ministry, *Global Data Security Initiative*, 2020.

[39] See civil code 2021, and Personal Information Protection Law 2021, and Data Security Law 2021.

[40] 携手推进"一带一路"建设--时政--人民网 (people.com.cn) (2017).

[41] 大数据与"一带一路"--理论-人民网 (people.com.cn) (2016); 中国缅甸国际陆地光缆工程全线贯通_地方报道_新闻_中国政府网 (www.gov.cn) (2014).

[42] 中国大数据企业走上"一带一路" (xinhuanet.com) (2018).

[43] See e.g. https://leidenasiacentre.nl/wp-content/uploads/2021/01/LAC-IPCS-DSR-Report-Aug-2020.pdf; Will China Control the Global Internet Via its Digital Silk Road? – Carnegie Endowment for International Peace (2020); China's Digital Silk Road and the Global Digital Order – The Diplomat (2021).

[44] Erie/Streinz, *The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance*, 2021.

instituting capacity that co-produces the economy.[45] The activation strategy derives from law's capacity to code/contest property rights and facilitate access, transaction, and pooling practices[46]. The layering strategy is inspired by theories of long-term law-tech co-evolution, where law and technologies are institutionally 'layered' and imprinted through time.[47] These groups of theories together hold that institutions are path-dependent, non-ergodic (time irreversible)[48], and embedded in history.[49] In such evolutionary processes, institutions retain shared cognition and knowledge of governance practices as the 'sediments of time'.[50] This part explains the conceptual models of institutionalisation, activation, and layering, and their groundings in institutionalist theories.

I. Institutionalisation: State-market Co-Production

22 First, 'institutionalisation' is used to describe the state's use of formal institutions and practices to initiate knowledge exchange with private actors and co-produce the economy. This conceptual category is inspired by institutionalist theories of state-market co-production. In early literatures, Ostrom and co-authors used 'co-production' to explain public services being carried out by both paid (public) and unpaid (private) labours[51]. For example, 'safety' as a public good achieved by both the police walking on beat and the communities' anti-crime efforts. Her case study in Indianapolis[52] and neighbourhoods of African Americans[53] shows that instead of large-scale patrolling in their cars, the police walking on the streets (as formal institutions) exchange informal/tacit knowledge with people in the communities, who despite unpaid, voluntarily contribute to local crime prevention and reduction. Her later case studies shows similar synergetic mechanisms of co-production in U.S. education policy[54], urban infrastructure policy in Brazil, and education in Nigeria[55]. Her collaborative empirical studies on common-pool resources further demonstrated how the state and private communities need each other to co-produce both formal and informal institutions. Law in her framework is thus not merely about legal rules, but also the constitutive processes and practices that facilitate public-private knowledge exchange and collective actions.[56]

---

[45] *Supra* n 1.

[46] *Supra* n 2.

[47] *Supra* n 3.

[48] The non-ergodic concept is drawn from an emerging school of ergodicity economics. See Peters, *Quantitative Finance* 11.11 (2011), 1593–1602. Peters, *Nature Physics* 15.12 (2019), 1216–1221.

[49] See, Deakin/Markou, *Northern Ireland Legal Quarterly* 72.4 (2021). Deakin, 7 *Review of Law and Economics* (2011). Deakin, 55 *Current Legal Problems* (2002). Deakin/Wilkinson, *The Law of the Labour Market: Industrialisation, Employment, and Legal Evolution*, 2005.

[50] Aoki, *Corporations in evolving diversity: Cognition, governance, and institutions,* 2010; Koselleck, *Sediments of Time: on possible histories*, 2018; Deakin/Meng, The Governance of Covid-19: Anthropogenic Risk, Evolutionary Learning, and the Future of the Social State, *Industrial Law Journal* 49.4 (2020): 539–594; Zuo, *Governance by Algorithm: China's Social Credit System* (working paper), 2020, available at https://www.finance.group.cam.ac.uk/system/files/documents/GovernancebyAlgorithm_CERF_Zhenbin6.16.2020.pdf (last accessed 16 December 2022).

[51] Parks/Baker/Kiser/Oakerson/Ostrom/Ostrom/Percy/Vandivort/Whitaker/Wilson, *Policy studies journal*, *9*(7), (1981) 1001–1011.

[52] Ostrom/Whitaker, *American Journal of Political Science* (1973), 48–76.

[53] Ostrom/Whitaker, Community control and governmental responsiveness: The case of police in black neighborhoods, *Improving the quality of urban management* 10.4 (1974), 303-34.

[54] Davis/Ostrom, *International Political Science Review* 12.4 (1991), 313–335.

[55] Ostrom, *World development* 24.6 (1996): 1073–1087.

[56] Ostrom, *American Economic Review* 100.3 (2010): 641-72.

In more recent literatures, Aoki uses the concept of 'embedded cognition' to describe institutions' capacity to store and transmit knowledge through time. He argued that states and corporations are not 'bundles of contracts' but epistemic communities that maintain focal points and cognitive structures embedded in society.[57] Deakin et al. further raise 'legal institutionalism' as a law and economics paradigm to explain how the rule-of-law state co-produces the modern market economy at its current global scales.[58] They argue that industrialisation and modern economic development require a clear boundary between the state and market, where co-production of public service becomes possible between public and private actors working with complementarity.[59] 23

Deakin, Chen and collaborators further used qualitative evidence to show that China's large scale industrialisation have been accompanied with the emergence of a rule-of-law state, which enforces contracts, property rights, corporate governance structures and so on. They argue that this recent rising rule-of-law state complements and constitutes China's traditional *guanxi*-based economy. Such state-market complementarity helps the Chinese economy to break from its previous limits, which come from traditional modes of cooperation and enforcement that heavily rely on informal social norms within close-knit groups and geographical regions. A Chinese rule-of-law state, at least by enforcing private and commercial laws, thus co-produces the Chinese modern market economy.[60] Deakin and Meng also use the case of COVID-19 governance in Wuhan to further illustrate how legal institutions at national and international levels helped retain public health knowledge and coordinated large-scale collective actions[61]. 24

In the context of data strategy, evidence shows that in 2021 China has intensive legislation and enforcement practices on cyber/data security, data protection, and antitrust. They are examples where the state uses data institutionalisation to initiate state-market co-production of common knowledge to address data harms/risks, stabilise corporate expectations, and scale up the digital economy. 25

II. Activation: Coding Property or Pooling Commons

Second, the term 'activation' is used to describe the experimental processes of state-market co-production before new forms of practices and knowledge are stabilised and coded into laws. In this dynamic period, the state strategically encourages or acquiesces the flexible legal and policy spaces that allow for competing practices to emerge and 'activate' new forms of market transactions, pooling and/or use of undefined things or assets, including data. It can be viewed as a strategy that often chronologically precedes the institutionalisation strategy, or is adopted in-between stabilised periods of 'punctuated equilibrium' to trigger change in legal evolution.[62] 26

'Activation' is inspired by institutionalist theories that reveal the processes of legal 'coding' of things into property and capital, and the polycentric governance of common-pool resources (CPR) co-produced by the public and private actors. 27

[57] Aoki, *Corporations in evolving diversity: Cognition, governance, and institutions*, 2010.
[58] Deakin et al., *Journal of Comparative Economics* 45.1 (2017): 188–200.
[59] *Ibid.*
[60] Chen/Deakin, *Law and Development Review* 8.1 (2015), 123–145. Chen et al., *Journal of Corporate Law Studies* 17.2 (2017), 257–290.
[61] Deakin/Meng, *Industrial Law Journal* 49.4 (2020), 539–594.
[62] See Deakin, 7 *Review of Law and Economics* (2011). Deakin, 55 *Current Legal Problems* (2002). Deakin/Wilkinson, *The Law of the Labour Market: Industrialisation, Employment, and Legal Evolution*, 2005.

28 Pistor describes how the law has historically 'coded' (or categorised) land, technology, financial instruments, and other tangible/intangible things into property, patents and/or capital. She argues that legal institutions and lawyer's innovative practices are always in the process of creating or contesting property rights and new forms of transactions. The legal community in this sense helps the state authorities to code/decode shared understandings and practices on coercive measures and exchange informal knowledge that allows for large-scale market transactions, global cooperation, as well as wealth and inequality.[63] This aligns with Ostrom's description of the state-market co-production process in the case of CPR governance. Her cases studies show that forests, fisheries, and other 'things' that trigger collective action problems can hardly be governed by a dichotomy of state monopoly or private property rights. Thus, the formal legal coding and arrangements of CPR need more dynamic and diverse considerations of the natures of the CPR and their specific community contexts. These context-specific formal legal practices require, while co-producing, informal local knowledge in the communities.[64]

29 Deakin and Meng, moreover, recently used the case of 'household responsibility system' that governs China's rural lands to argue that ownership should move beyond the concept of 'legally enforced private property rights'. Instead it should be understood as an 'emergent, diverse and complex institution'. Deakin and Meng's arguments draw from and emphasise Ostrom's theories of CPR governance and legal institutions capacity to code/contest property.[65]

30 In the context of data, there has been no consensus on how law can code 'data',as a new 'thing', into an existing or novel legal category. This leaves an elastic legal and political space for major jurisdictions including the U.S., the EU, and China to compete in innovating data ownership and access practices.[66] Evidence will show that the Chinese state uses the activation strategy to allow for legal innovations on data trading, sharing, and use against data fragmentation. These legal ingenuities include the Central Bank's provisional license to Ant Group on handling personal credit information, techno-legal arrangements in Beijing International Data Exchange (BIDE) in contrast to Shenzhen's local legislative attempts on data property rights, and Tianjin's emerging practice of 'Party manages data'.

III. Layering: Law-Tech Co-Evolution

31 Third, 'layering' is categorised as a strategy that describes the state's efforts to construct sustainable ecosystems of institutions for long-term public governance in changing environments. It requires the state to make timely adjustments to the often fragile fits between formal institutions and their environments layered in history with path-dependency. In the data context, layering means the state builds useful data cycles and sustainable data habitats/ecosystems for valuable data applications. It is concerned with better designs of law and technologies in order to achieve valuable and long-term data use in public governance. It is a strategy of sustainability which could complement the stabilising strategy of institutionalisation, and the contestation strategy of activation. This layering strategy is inspired by institutionalist and design theories that understand law as

[63] Pistor, *The code of capital*, 2019.

[64] Ostrom, *American Economic Review* 100.3 (2010), 641-72.

[65] Deakin/Meng, *Journal of Institutional Economics* (2021), 1–15.

[66] See theoretical discussions on data property, transaction and practices, e.g. Litman, *Stanford Law Review* (2000), 1283–1313. Evans, *Harv. JL & Tech.* 25 (2011), 69. Victor, *Yale LJ* 123 (2013), 513. Wiebe, *Journal of Intellectual Property Law & Practice* 12.1 (2017), 62–71. China has tried to raise the data property concept in Shenzhen for example, but failed in the end (see discussed below).

co-evolved with technology through time. In early literature, Deakin argued that juridical categories like 'employment' evolved in history with path-dependency.[67] Similar to the evolution of technologies such as the computer keyboard arrangement (QWERTY), these juridical concepts can have 'frozen accidents' and exhibit 'punctuated equilibrium' through time.[68]

Applying design and affordance theories to law, Hildebrandt argues that modern positive law is made possible by printing technologies, and the emerging pervasive smart technologies are likely to afford the design of data-driven laws.[69] Deakin and Markou combine this observation with legal evolution theory. They use the case of recent machine-learning applications in law to reveal the co-evolution between law and technology as institutionally path-dependent and non-ergodic, i.e. embedded in irreversible time. They argue that machine-learning and other data-driven technologies can lock-in the past, just like law's path-dependency in evolution, but with even more closed ends. They present the risk that while law is afforded by natural language that allows for flexible interpretations and breaking from the past, the numbers and code presented in data can be more rigid and thus trap the society into its past once applied to law and governance.[70] Hildebrandt uses the term 'freezing' to describe shared apprehensions that pervasive data and code-driven technologies will exacerbate law's negative imprinting of the past.[71] **32**

Zuo builds on these literatures to elaborate the concept of 'layering' in law-tech co-evolution. He argues that data categories/abstractions, which are more formalised, are layered on less formalised legal and social categories in a path-dependent way. For example, the data-driven algorithms for employment status prediction (e.g. for tax returns purposes) must input data categories that are based on existing legal categories like 'employee', 'worker' or 'independent contractor'. When new forms of employment appear in society, the corresponding legal categories will change, which will require a change in the data categories in the predictive algorithms.[72] **33**

For example, when the UK court decided to define drivers working on ride-hailing platforms as 'workers' (like Uber drivers), new population will be added to existing data categories or require creating new data categories in the mathematical models. This requires timely updates of both data sets and the algorithms to prevent model decay caused by such 'concept drifts'. Otherwise as time passes by the shift in social reality will impede valuable long-term data interpretation and/or prediction, and the data use will not be sustainable or scalable.[73] **34**

'Layering' as drawn from the law-tech evolutionary literatures is useful to illustrate the need for long-term interpretation of data in a sustainable 'habitat/ecosystem'. Evidence in Shanghai and Qingdao is raised focusing on practices in Smart Court and social/financial credit systems, complemented by secondary sources from Huawei, Alibaba and research institutes. **35**

---

[67] Deakin/Wilkinson, *The Law of the Labour Market: Industrialisation, Employment, and Legal Evolution*, 2005.

[68] Deakin, 55 *Current Legal Problems* (2002). Deakin, 7 *Review of Law and Economics* (2011). Deakin, *Historical Social Research/Historische Sozialforschung* (2015), 170–184.

[69] Hildebrandt, *The Modern Law Review* 79.1 (2016): 1–30.

[70] Markou/Deakin, in: Markou/Deakin (eds.), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence,* 2020.

[71] See Hildebrandt, in: Markou/Deakin (eds.), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence,* 2020. Hildebrandt, *Journal of Cross-disciplinary Research in Computational Law* 1.1 (2021).

[72] Zuo, *Governance by Algorithm: China's Social Credit System* (working paper), 2020; also see Supiot, *Governance by numbers: The making of a legal model of allegiance,* 2017.

[73] *Ibid.*

36 'Qualitative Method': Based on these conceptual models and theoretical groundings, the research combines doctrinal and qualitative methods. The doctrinal data include legislations, regulations, their drafts and legislative notes, administrative and judicial decisions, and other publicly available legal documents. The empirical data include archival or internal documents, and semi-structured interviews conducted in China between 12/2020 and 4/2021. Grey secondary sources such as news and reports were also used as evidence to triangulate findings. Interview data and documents collected are limited by time and available social networks. However, they can cover a certain in-depth understanding of the cases involved.[74]

C. Institutionalisation: Data Security, Protection, and Antitrust

37 Heldt and Hennemann argued that the 'Roaring Twenties' of EU technology regulations are dawning. Drafts of the EU *Digital Services Act* (2020), *Digital Markets Act* (2020), *Data Governance Act* (2020), and the *AI Regulation* (2021) are at the forefronts, which they described as a strategy of 'upward convergence' in regulatory standards similar to the Brussels Effect[75]. This part evidences a similar legislative and regulatory trend in China that started with the 'Roaring Summer of 2021'. The Chinese strategy is however conceptualised as 'institutionalisation'. In the data context this means the state's initiation of a market-state co-production of public services and common knowledge within epistemic communities of data governance, in order to stabilise and scale up a national digital economy. Three major institutionalisation efforts respectively addressed emerging forms of harms/risks in data security, privacy, and competition: (1) Cybersecurity review of the Chinese ride-hailing giant DiDi Chuxing after its IPO at the New York Stock Exchange (NYSE: DiDi Global Inc); (2) the completion of China's data protection legal framework featuring 'gatekeeper' and managerial liabilities; (3) antitrust actions that restrain data power and facilitate interoperability.

I. DiDi's 2021 Cyber/Data Security Review

1. Security Concerns over DiDi *before* its IPO in New York

38 In 2016, China's *Cybersecurity Law*[76] was passed as the first high-level law that regulates data security.[77] It created a new legal category the 'critical information infrastructure (CII) Operators' with high-level obligations on cyber/data security (Article 31) and localisation requirements (Article 37). These high-level compliance requirements on CII Operators are stipulated because they are, by name, 'critical' in handling/managing data and its infrastructures. The Cyberspace Administration of China (CAC) is the top-level party-state organ that oversees such high-level security compliance.[78]

---

[74] See case study methodology. Poteete/Janssen/Ostrom, *Working together*, 2010. Buchanan/Chai/Deakin, *Hedge fund activism in Japan: The limits of shareholder primacy*, 2012. Chen et al., *Journal of Corporate Law Studies* 17.2 (2017), 257–290.

[75] Heldt/Hennemann *Tagesspiegel Background*, 15 July 2021.

[76] Effective since June 1st 2017.

[77] 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China 2017].

[78] Cybersecurity Law 2017. Chapter 3, section 2 on CII operators. Including article 37 on storing important data in China. 中华人民共和国网络安全法_中国人大网 (npc.gov.cn).

Soon after DiDi Chuxing got listed at the NYSE in the U.S. in June 2021, the CAC started a security review/investigation under the *Cybersecurity Law* (2017), which effectively deemed DiDi as a 'CII Operator'[79]. Such security review after an outbound IPO is arguably functionally similar (as it does not stop the IPO) to the U.S. national security review by The Committee on Foreign Investment in the United States (CFIUS) which can pause and stop cross-border mergers and acquisitions[80]. **39**

DiDi is a ride-hailing tech giant born in China, and a major competitor with Uber in the global ride-hailing market.[81] DiDi claims in its SEC filing that between March 2020 and March 2021 it had 377 million annual active users (which is larger than the U.S. population) and 156 million monthly active users (MAU) in China[82], compared to Uber's 93 million MAU in the world (last quarter of 2020)[83]. **40**

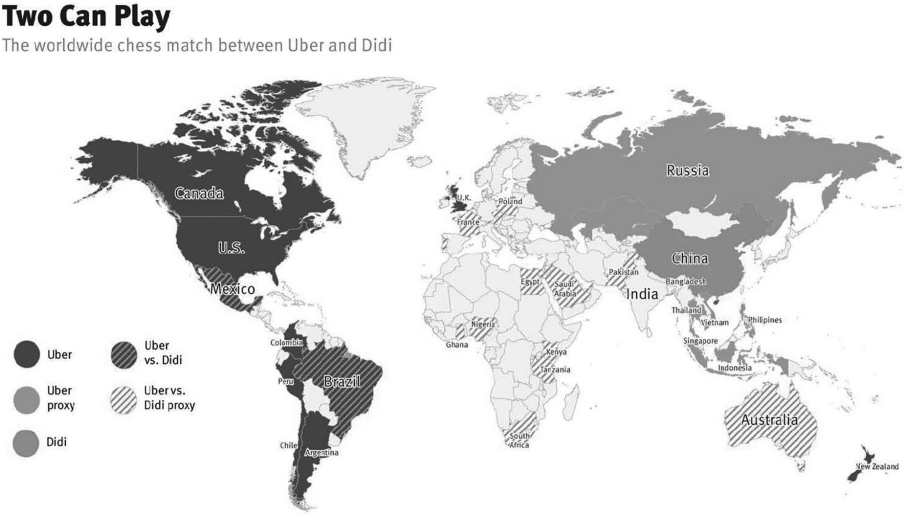

Figure 2. Uber and DiDi global market coverage (2018) supra n 81

Evidence shows that the regulatory agency had difficulty in addressing DiDi's cyber/data security issues long before DiDi's IPO in NYSE (June 2021). First, DiDi Shanghai was already investigated and raided by various Shanghai regulators based on security concerns in 2018. These include 'fake cars', illegal drivers and incomplete data filing to the ride-hailing regulatory agencies. But nothing was found when the enforcement team arrived. DiDi was reported to even have prepared several boxes of chaotic and useless files in advance for the enforcement team's third inspection.[84] Respondent X, a governmental official in Shanghai, complained in a closed group discussion that DiDi **41**

[79] 2021a CAC announcement on DiDi.

[80] See e.g. Griffin, *Fordham L. Rev.* 85 (2016), 1757. Also see a classic case of Shuanghui's acquisition of Smithfield. China Inc. and the CFIUS National Security Review – The Diplomat, available at https://thediplomat.com/2013/12/china-inc-and-the-cfius-national-security-review/ (last accessed 16 December 2022).

[81] The New Global Order in Ride Hailing: Didi vs. Uber – The Information, available at https://www.theinformation.com/articles/the-new-global-order-in-ride-hailing-didi-vs-uber (last accessed 16 December 2022); *cf* below.

[82] Didi Global Inc Prospectus 424B4 (sec.report) 2021.

[83] Uber's users of ride-sharing services worldwide 2017–2020 | Statista, available at https://www.statista.com/statistics/833743/us-users-ride-sharing-services/ (last accessed 16 December 2022) *supra* n 81.

[84] 上海检查组第四次上门检查滴滴　　数据已接入将复查|滴滴|检查组|上海_新浪科技_新浪网 (sina.com.cn).

is not concerned with their everyday fines from violations of regulations: 'they see such administrative fines as the cost in their financial reports'[85].

42 Second, Respondent Y raised in the same closed group discussion that

> *'the CAC is afraid of reviewing data security in cross-border transfers because they don't have the technical expertise yet.'*

43 This was especially acute with regards to the massive amount of geographical data generated each day on ride-hailing platforms like DiDi. Respondent Y claimed that one concern of the CAC was that such geographical big-data can be used to infer and reveal the locations of military bases or other sensitive places. However, the CAC did not have the technical team to understand how to evaluate such risks (Legal scholar Y, Shanghai, 2021).

44 Third, the sensory and audio-visual big-data collected by the cameras on self-driving cars were of particular concern with the rapid roll-out of autonomous vehicles like Tesla, and DiDi's robo-taxi in cities like Shanghai.[86] Respondent X and Y, for example, discussed the data risks of Tesla's self-driving cars in Shanghai. They claimed that Tesla's cameras and sensors collect an extensive amount of real-time visual data of its surroundings including people's faces, buildings, other vehicles and so on, and can transfer them abroad. Sensitive information can be inferred from such big-data where data security and privacy stakes are high (March 2021, Shanghai).

45 These security concerns over sensitive geographic data was later confirmed in May 2021 with the CAC's stipulation of *Several Provisions on the Management of Automobile Data Security (Draft for Comment)*.[87] Article 3 listed six types of 'important data' which include for example,

- A3 (1) 'Data on the flow of people and traffic in military administrative areas, national defence science and industrial units or other units that involve state secrets, or sensitive, important areas of Party and government administrative units above the county level, etc.';
- A3 (3) 'Data on the operation of automobile charging networks'; and
- A3 (5) 'Audio-visual data of individuals' faces, voices, and license plates, etc., outside the vehicle'[88].

2. Institutionalisation in the DiDi Security Review 2021

46 DiDi's 2021 security review is not that surprising against the background of CAC and local regulators' security concerns. On July 2nd 2021, two days after DiDi's IPO at NYSE, the CAC announced its review of DiDi's cybersecurity compliance, and required that no new users be registered on DiDi's ride-hailing platform immediately. The announcement cited the *Cybersecurity Review Measure (2020)* as the applicable law, and used

[85] Government official X, Shanghai, 2021.3.

[86] AutoX launches its RoboTaxi service in Shanghai, competing with Didi's pilot program | TechCrunch 2020.

[87] Translation: Several Provisions on the Management of Automobile Data Security (Draft for Comment) | DigiChina (stanford.edu), available at https://digichina.stanford.edu/work/translation-several-provisions-on-the-management-of-automobile-data-security-draft-for-comment/ (last accessed 16 December 2022).

[88] (2) Survey and map data that is more precise than maps publicly issued by the state (4) Data on types and traffic volume, etc., of vehicles on the road (…); (6) Other data that might affect national security and the public interest, as specified by the state cybersecurity and informatization department and relevant departments of the State Council.

National Security Law (2015) and the *Cybersecurity Law (2017)* as the higher-level legal sources.[89] In this way CAC effectively deemed DiDi as a 'CII Operator' which is the only subject regulated under the scope of Article 1 and 2 of the current *Measure (2020)* ('national security risks were brought about by the CII Operators' procurement of network products and services'). Data security is listed in Art. 9 (1) as one of the risk factors for review ('theft, leak or damage of important data').[90]

47 On July 4th, CAC confirmed DiDi's 'severe violation of data regulations' and required all App Stores in China to delist DiDi's online ride-hailing app, despite allowing existing riders and drivers to keep using the app. It demanded DiDi to make changes to comply with the *Measure (2020)* and other security standards.[91] Two months after this sanction it was reported that DiDi's daily active users dropped by 30 % (comparing August to June).[92]

48 Besides DiDi, on July 5th 2021 CAC initiated similar investigations and disciplines on three more Chinese tech giants that recently got listed in the U.S. These big-techs are all deemed as CII operators, which have cyber and data security concerns in their public listing abroad. Two other Chinese tech giants later cancelled their listing plans after the CAC's four reviews[93].

49 Within a week's time, on July 10th the CAC also released a new *Cybersecurity Review Measures (2021, Draft for Public Comments)* that has provisions targeting big-tech outbound IPOs. It requires any 'CII Operator with more than 1 million user information that wish to be publicly listed abroad, must file a cybersecurity review to the Cybersecurity Review Office' (Art. 6).

50 Seven 'major factors' were listed concerning risks to national security (Art. 10), including the risk that 'after an IPO abroad is completed, the CII, core data, important data or massive amounts of personal information are influenced, controlled or maliciously used by foreign governments'. It also expanded the CAC's general review mandate to all 'data handlers' instead of just the 'CII Operators' (Art. 2).[94] More clarity would be provided regarding security concerns for both data handlers and CII operators when the revised *Measure 2021* is finalised and taken into effect.

51 A more detailed *CII Security Protection Regulation (2021)* was also later passed in August 2021. This new *CII Regulation* (2021) adds granularity to the existing *Cybersecurity Law (2017)* and *Review Measure (2020*), and clarifies important obligations for CII Operators to, first perform data security accountability and establish protection institutions (Art. 15); second, to prevent data leakage (Art. 2, 9, 18), and third, to maintain data completeness, confidentiality and usability (Art. 6).

52 In addition, it is worth noting that China passed its long-due *Data Security Law (2021)* in June 2021, about three weeks before DiDi's IPO. It is a high-level legislation as important as the *Cybersecurity Law (2017)*, and came into effect on the same date with

[89] 2021a CAC announcement on DiDi.

[90] See 2020 Review Measure.

[91] 2021a CAC announcement on DiDi.

[92] Didi loses 30 % of daily users after Beijing crackdown following IPO | Financial Times 2021 Sep, available at https://www.ft.com/content/13a768b0-1000-4cad-8a03-36a1e66f460b (last accessed 16 December 2022).

[93] See various analysis articles written by lawyers in China 从实施网络安全审查到APP下架，数据安全律师对滴滴事件梳理了八个核心问题-移动支付网 (mpaypass.com.cn) and in the U.S., After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come Into Focus | DigiChina (stanford.edu) 深度"滴滴"网络安全审查事件的全景分析与合规指引_腾讯新闻 (qq.com), available at https://new.qq.com/omn/20210710/20210710A087S900.html (last accessed 16 December 2022).

[94] 国家互联网信息办公室关于《网络安全审查办法修订草案征求意见稿）》公开征求意见的通知-中共中央网络安全和信息化委员会办公室 (cac.gov.cn).

the *CII Security Protection Regulation (2021)* on September 1st 2021[95]. Its Chapter IV detailed the 'Data Security Protection Obligations' for all 'handlers of important data' (a broader concept than CII Providers), where two articles are crucial:

53 (1) Article 27 requires 'The conduct of data handling activities using the Internet or other such information networks shall perform the data security protection obligations described above on the basis of the cybersecurity Multi-Level Protection System (MLPS)'.[96] The MLPS 1.0 was a ministerial standard for cybersecurity that functioned as early as 2007 before the big-data and algorithmic technologies took off in China[97]. Since 2019, the MLPS 2.0 is the revised standard in effect, which was updated by legal and technical communities entering the big-data era, and shall be used for more granular reviews on DiDi's data security issues[98].

54 (2) Article 31 stipulates the data security checks for 'outbound security management' for CII Operators and other data handlers working in China pursuant to the *Cybersecurity Law (2017)*.[99] This article raises data security concerns when data handlers change their corporate governance structures, e.g. by listing outside of China.

55 In DiDi's case the CAC cybersecurity review might be complicated if the U.S. regulatory authority Security Exchange Commission (SEC) requires data disclosure or access to third-party auditing due to DiDi's IPO at NYSE. For example, under the U.S. *Holding Foreign Companies Accountable Act 2020 (HFCAA),* the SEC and the Public Company Accounting Oversight Board (PCAOB) can access third-party audit papers of non-US firms listed in the U.S. required by the Sarbanes-Oxley Act 2002.[100] Besides, outbound data transfer concerns can also be triggered when the voting structure within the board changes and new decisions can be made on data transfer. Article 31 aligns with the latest proposed rules on security reviews of public listing abroad under the new *Cybersecurity Review Measures (2021, Draft for Public Comments).*

56 There are also rapid legislative moves on the security of cross-border data transfer. Most recently on October 29th 2021, the CAC also issued a new *Security Assessment Measures on the Cross-border Data Transfer (Draft for comments)*. It specified the conditions, procedures, materials necessary for filing, and redress.[101] Shanghai's local legislature also passed a *Shanghai Data Regulation (Draft for comments 2021)* which requires the making of a 'low-risk catalogue' for certain types of cross-border data transfers in order to facilitate data flow in its *Lin Gang* free trade zone pilot (A66, 67).[102]

---

[95] 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China 2021], available at http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml (last accessed 16 December 2022).

[96] Translation: Data Security Law of the People's Republic of China | DigiChina (stanford.edu).

[97] MLPS 2007.

[98] MLPS 2.0, 2019.

[99] 'The provisions of the Cybersecurity Law of the PRC apply to the outbound security management of important data collected or produced by critical information infrastructure operators operating within the mainland territory of the PRC; outbound security management measures for other data handlers collecting or producing important data within the mainland territory of the PRC are to be jointly formulated by the national cybersecurity and informatization department and relevant departments of the State Council.' 中华人民共和国数据安全法.

[100] 15 U.S.C. § 7211, Holding Foreign Companies Accountable Act 2020 (HFCAA); Congress Passes the "Holding Foreign Companies Accountable Act" (harvard.edu) 2021, available at https://corpgov.law.harvard.edu/2021/01/10/congress-passes-the-holding-foreign-companies-accountable-act/#1b (last accessed 16 December 2022); Senators call on US securities regulator to investigate Didi IPO | Financial Times (ft.com) 2021, available at https://www.ft.com/content/40c179f1-6450-43fd-9baf-f42425712016 (last accessed 16 December 2022).

[101] 国家互联网信息办公室关于《数据出境安全评估办法征求意见稿）》公开征求意见的通知.

[102] 上海人大 (spcsc.sh.cn); 《上海市数据条例草案）》解读一丨全国首提制定低风险跨境流动数据目录.

3. Co-Production of Knowledge in Cyber/Data Security

The above legislative and regulatory practices do not only establish rules, but more importantly shape new common knowledge within emerging cyber and data securities communities. As the evidence shows, the Shanghai local regulators had problems enforcing regulations against DiDi's massive real-time operations, and CAC started with little expertise facing new data security risks on such large-scale ride-hailing platforms and the roll-out of autonomous vehicles. **57**

DiDi's security review thus became a point of institutionalisation where existing concerns are addressed by the state's legislative and enforcement practices. These CAC practices also initiate informal knowledge exchange with private actors to make more detailed regulations. DiDi's case sets an example for future security compliances by other private actors such as Tesla, whose autonomous vehicles collect massive amounts of data in China. **58**

It is debatable whether DiDi's ongoing review is political in nature, but the process at least would help stabilise market expectations on**:** **59**

(1) what is a 'CII operator' that should be reviewed,
(2) what are the review procedures and requirements;
(3) what knowledge and expertise the CAC needs and retains to review automobile data (including self-driving cars), foreign listing and cross-border data transfer.

This also enables the wider legal and technical community of cyber/data security to update common knowledge, for example, by revising the MLPS 1.0 (2007) standards to MLPS 2.0 in 2019 which aligns with high-level legislations and emerging technologies. The informal knowledge exchange within these epistemic communities engenders self-governance of data risks. Such private efforts evolve around but also shape the state's centralised instituting efforts to keep updating common knowledge and practices. In this sense, the CAC and regulators used the institutionalisation strategy to initiate the market-state co-production of knowledge on data security governance that stabilises corporate expectations and scales the digital economy. **60**

II. Data Protection, Gatekeeper, and Managerial Liabilities

Besides security, data protection is the second area that shows extensive evidence of China's institutionalisation strategy. China's Personal Information Protection Law (PIPL) was recently passed in August 2021 and came into effect on 1st November.[103] It is considered as China's equivalent of the EU's General Data Protection Regulation (GDPR, 2018), but also features rather unique provisions such as gatekeeper and managerial liabilities inspired by/in competition with both the U.S. FTC decision on Facebook re third-party data violations (2020) and the EU's recent legislative proposals on digital markets and services (2020). **61**

1. 'China's GDPR': Personal Information Protection Law (PIPL) 2021

To emphasise the importance of this legislation, the *National People's Congress (NPC) Legislative Note on PIPL (2020)* claims at the beginning that 'by March 2020 China's **62**

[103] 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China, 2021], available at http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80-b53a172bb753fe.shtml (last accessed 16 December 2022).

internet users reached 900 million.'[104] The *Note* followed, however, that data violations and harms on people's daily life are rampant and require change: 'an objective demand to enhance PI protection' and 'a real demand for maintaining a healthy ecosystem of the cyberspace'. To show this real predicament the *Note* cited reports and initiatives from the NPC with strong societal demands as well as the central Party's concerns over societal complaints.[105]

63 In addition to addressing the data privacy concerns, the PIPL is also considered as an 'important measure to promote healthy development of the digital economy'. The *Note (2021)* adopted the SC's understanding of 'data as an essential factor (of production)' and claimed that 'data competition becomes important in global competition, and PI is the core and foundation of big-data.'[106] It further raised that 'in coping with COVID-19', many big-data applications are useful and become more pervasive, but a comprehensive data protection framework needs to be built and applied.[107]

64 Doctrinally, the PIPL 2021 completes China's data protection framework. Its ultimate legal authority of data protection laws comes from the Chinese Constitution: Art. 33 on human rights, Art. 38 on human dignity, and Art. 40 on freedom and privacy in communication. In 2021, the *State Council's Human Rights Action Plan (2021–2025)* also highlighted in the protection of 'privacy rights' and 'personal information interests (PII , *geren xinxi quanyi*)'[108].

65 However, the earliest high-level data protection law in effect is the *Ninth Amendment of the Criminal Code (2015)*. It stipulates a maximum of seven years of prison for severe offences of stealing, selling or abusing people's personal information. This was targeted at the privacy concerns at that time with the rise of big-data technology. The *Ninth Amendment (2015)* was later followed by the *Judicial Interpretations on Personal Information Crime (2017)* issued by China's Supreme People's Court (SPC) and the Supreme People's Procuratorate (SPP). Some high-profile criminal cases have been reported for example, in Shanghai and Hangzhou where big-data companies illegally collect and store personal information. They were heavily fined and their legal representative and CTO were sentenced to three years of prison (but with reprieve periods).[109]

66 Besides the criminal code, China's new *Civil Code 2021* sets two layers of protection for personal information. First, Art. 1032 stipulates the 'privacy right' that is similar to the Art. 8 'right to private life' in the European Convention of Human Rights (ECHR). The Art. 1032 right protects private spaces, activities and communication at the right-level with human dignity as the foundation. Although privacy is afforded with higher-level protection, the scope of privacy is narrower compared to 'personal information interests' (PII).

67 Art. 1034 *Civil Code 2021* stipulates the protection of PII, which is not protected at the level of 'rights', but includes a larger scope of interests related to both private and non-private personal information. After the *PIPL 2021* came into effect, PII is protected in

---

[104] This is more than the total population of the EU, U.K. and U.S. combined, but only about 65 % of the Chinese population.

[105] 关于《中华人民共和国个人信息保护法草案）》的说明_中国人大网 (npc.gov.cn), 2020.

[106] *Ibid.*

[107] *Ibid.*

[108] 2021.9. Human Rights Plan Section chapter 2, section 3. 国家人权行动计划20212025年） (scio.gov.cn).

[109] See, e.g. (2020) 浙0106刑初437号 [2020, Zhejiang, 0106, Criminal Court, first instance case no. 437]. Also see 淘宝11.8亿条用户隐私被泄露 两男子被判刑 available at https://www.sohu.com/na/472780318_120957976 (last accessed 8 February 2023) [Taobao 1.18 billion pieces of user information leaked, two men sentenced. Sina news, 2021.6.17].

detail by this field-specific legislation. This completes the two-layer civil protection of personal information, and it is worth noting that as private information is part of personal information, it is doctrinally also protected under specific rules of the PIPL 2021[110].

Other important legislations on China's data protection include the *Cybersecurity Law* 2017 and the *Data Security Law 2021,* together with other specific regulations concerning security issues. These security laws are excluded from and in parallel with the PIPL, and together cyber/data security and data protection form the two arms of China's data governance regime.[111] **68**

The *Consumer Protection Law 2014* and *E-Commerce Law 2019* broadly touched upon personal information with articles that link the jurisdictions to PIPL 2021.[112] There are also many low-level personal information protections standards (e.g. *Guidance for personal information security impact assessment 2020*)[113] and local legislations (e.g. *Shenzhen Data Regulation 2021*, *Shanghai Data Regulation 2021*).[114] **69**

The Chinese courts are also active in the data protection regime where various courts have made high-profile decisions. Even before the new Civil Code 2021, the Beijing Internet Court for example in 2020 had already made two decisions that WeRead (of Tencent, linked to Wechat) and TikTok (of Bytedance) respectively violated personal information protections laws. The court found WeRead had misled users to consent on displaying their favourite/liked books to Wechat friends and contacts, and required WeRead to stop accessing users' Wechat friendship list and delete all relevant information. It also required WeRead to stop showing users' data to the user's friends, such as favourite books, what is being read and so on. The Court also found violations of 'personal information interests' where TikTok's Beijing operator accessed the name and phone number of the plaintiff Ling via Ling's friend's contact book, but without consent from either Ling or Ling's contact. It ruled the deletion of related data including the name, phone number and the geographical data of Ling, and an apology with compensation of 1,000 RMB to Ling.[115]After the new Civil Code 2021, the first civil collective action case appeared where the Hangzhou Internet Court ruled both criminal punishment and civil liabilities to Sun who bought and then publicly sold more than 45,000 pieces of personal information online for profit.[116] **70**

Recently, the Supreme People's Court also issued the *Judicial Interpretations on Facial Recognitions (2021)*.[117] The latest facial recognition related case also was accepted in Changsha on data protection basis, where a legal intern sued the building **71**

[110] 中华人民共和国民法典 [Civil Code of the People's Republic of China 2021.] Art 1032, 1034, available at http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml (last accessed 16 December 2022).

[111] 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China 2017], available athttp://www.npc.gov.cn/ (last accessed 16 December 2022);. 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China 2021], available at http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml (last accessed 16 December 2022).

[112] *Consumer Protection Law 2014*; *E-Commerce Law 2019*.

[113] 信息安全技术—个人信息安全影响评估指南(GB/T 39335-2020) [Information security technology – Guidance for personal information security impact assessment (GB/T 39335-2020)].

[114] 《上海市数据条例》; 深圳市第七届人民代表大会常务委员会公告第十号）(2021), available at http://www.sz.gov.cn/zfgb/2021/gb1218/content/post_9307139.html (last accessed 8 February 2023) [Shenzhen 7th People's Congress Plenary Committee Report No. 10. On passing the Shenzhen Economic Special Zone's Data Regulation, 2021. Effective 1st December 2022].

[115] 北京互联网法院微信读书、抖音侵犯个人信息权--法治--人民网 (people.com.cn).

[116] 民法典实施后全国首例个人信息保护民事公益诉讼案当庭宣判--法治--人民网 (people.com.cn).

[117] SPC 2021 on facial recognition.

management company of his law firm for imposing compulsory facial recognition entrance registrations (pending after the PIPL).[118]

72 The PIPL 2021 builds on these previous laws and practices, and completes China's data protection framework. Detailed practices and the empirical effects of PIPL await to be observed after it came into effect on 1st November 2021. Nevertheless, the following PIPL legislative process featuring gatekeepers and managerial liabilities to a certain degree manifests the institutionalisation strategy that deliberately clarifies the state and market divide in order to co-produce common knowledge in China's data protection practices.

2. Gatekeeper and Managerial Liabilities in the PIPL 2021

73 PIPL 2021 features 'gatekeeper' and managerial liabilities that require big-techs in China to take up more public enforcement obligations with regards to their third-party suppliers. The legislative process followed an international trend in regulatory practices of mandating big-techs to self-regulate their third-party suppliers or App developers.

74 First, after the Cambridge Analytica incident, the U.S. Federal Trade Commission (FTC) in 2020 required Facebook (U.S. v Facebook 2020) to take more public obligations of regulating its third-party developers/suppliers in terms of data protection. It not only deemed Facebook liable for third-party's breach of consumer data protection, but also stipulated managerial liability, so that Mark Zuckerberg can be held personally liable in the future with potential civil, regulatory, and even criminal punishment.[119]

75 Van Loo theorised this practice by the FTC as a move towards 'gatekeeper liability', where regulators like the FTC can require big-tech platforms to be law-enforcers that supervise and regulate their third-party suppliers. He argued that this liability originates from the vicarious/third-party liability in torts that can penetrate corporate protection of individual officers or the board of directors. The Facebook case manifests what he calls the 'revival or the *respondeat superior*': where gatekeeper liability re-emerged alongside the big-tech's rising power. Big-tech's control over third-party suppliers' data access means vicarious liability.[120]

76 The FTC's gatekeeper and managerial liabilities imposed on Facebook is a sanction-backed legal arrangement to clarify big-tech's obligations to self-govern and prevent systematic harms/risks. This approach aligns with Shanghai's 'cooperation and deterrence' attitude towards big-tech companies, as expressed by Respondent Z:

77 *'The Chinese state has historically adopted this cooperation and deterrence attitude towards large businesses … Render unto market what is the market's, and unto state what is the state's. Then we won't disturb the foundational ecosystems of the citizens.' (Government official Z, March 2021).*

78 However, gatekeeper liability was not in the first draft of China's PIPL (October 2020). Only personal liability for executives of data-handlers was stipulated in this draft with moderate fines and various years of bans from the profession. These managerial liabilities do not require the data-handlers to be large platforms or 'gatekeepers'[121].

[118] (2021) 湖南人脸识别第一案大楼强制"刷脸"，原告望促个保法落地_, available at https://www.163.com/dy/article/GJES9OT205129QAF.html (last accessed 16 December 2022), (2021) Shanghai Data Regulation 2021, effective 1st January 2022 (available at https://www.shanghai.gov.cn/nw12344/20211129a1a38c3dfe8b4f8f8fcba5e79fbe9251.html, last accessed 8 February 2023).

[119] United States v. Facebook, Inc., No. 19-2184 (TJK), 2020 WL 1975785 at *5 (D.D.C. 23 April 2020)

[120] Van Loo, *Geo. LJ* 109 (2020): 141. Van Loo, *Va. L. Rev.* 106 (2020), 467.

[121] See PIPL first legislative draft for comments.

Comparatively, while the GDPR does not stipulate personal/managerial liabilities, the UK Data Protection Act (2018) has 'Liability of directors etc.' that penetrate the corporate protection.[122] Many other Chinese laws that focus on risk-related security compliance also have managerial liabilities, including the *Food Safety Law 2019, Cybersecurity Law 2017,* and *Data Security Law 2021.*[123]

79 Nevertheless, Art. 58 featuring gatekeeper liabilities appeared in the second draft of China's PIPL (April 2021). It stipulated a group of obligations onto big-techs which are similar to those in EU's *Digital Services Act (DSA, Draft 2020)* on 'very large online platforms' (VLOPs).[124] Art. 58 and the DSA share similar requirements on transparency, compliance structures and audits for big-tech companies in order to prevent systemic risks and to better regulate third-party suppliers or App developers[125]. Besides, The MIIT also accompanied the PIPL second draft with an *APP Personal Information Protection Regulations (Draft for comments)* in April 2021, which proposed more details on how to regulate third-party APPs on gatekeepers.[126]

80 It is worth noting that the Chinese legal academia and legislators became more aware of the term 'gatekeeper' after the EU's *Digital Markets Act (DMA, Draft 2020)* explicitly proposed 'gatekeeper obligations' for big-tech platforms in December 2020.[127] The focus of the *DMA (Draft 2020)* however is on fair competition for third-party developers/suppliers and interoperability, which is different from the obligations on VLOPs stipulated by the EU's *DSA (Draft 2020)* and the FTC's mandated gatekeeper's liabilities concerning data protection.[128]

81 The third and final version of the PIPL (August 2021) solidified Art. 58 as obligations for 'personal information handlers that provide important internet services, with very large amounts of users and complex business categories'. It added two more sections which further specified gatekeeper liabilities:

(i) 'platforms should set internal compliance institutions', and
(ii) 'platforms should obey transparent, just and fair principles, and should set platform rules that specify third-party's obligations on handling data.'[129]

These provisions to some extent established the state-market boundary and the division of labours and in regulating third-party providers.

82 Legal scholars' efforts are also considerable in the PIPL's drafting gatekeepers liabilities. For example, a comparative law article by Professor Zhang Xinbao at Renmin Law School introduced the concept of gatekeeper obligations in 2021 after the second draft of PIPL and the EU 2020 DMA and DSA proposals.[130] Professor Wang Xixin at Peking Law School advocated for a 'state protection obligation' from public law

[122] Data Protection Act 2018 c.12. Section 198.

[123] See China's *Food Safety Law 2019, Cybersecurity Law 2017,* and *Data Security Law 2021.*

[124] 《个人信息保护法草案二次审议稿）》[Second draft PIPL 2021.].

[125] COM (2020) 825: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Procedure 2020/0361/COD.

[126] 公开征求对《移动互联网应用程序个人信息保护管理暂行规定征求意见稿）》的意见 [MIIT Mobile Internet Application Personal Information Protection Provisional Regulations (Draft for Comments), 2021.4.26], available at http://www.gov.cn/hudong/2021-04/26/content_5602780.htm (last accessed 16 December 2022).

[127] See Zhang Xinbao. 2021.

[128] COM (2020) 842: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act) Procedure 2020/0374/COD.

[129] See PIPL.

[130] 张新宝互联网生态"守门人"个人信息保护特别义务设置研究，《比较法研究》，2021年第3期。[Zhang Xinbao, *Comparative Law Journal*, 2021 (3)].

perspective which requires the state to take up its protection role on personal information and coordinate both public and private efforts in data protection.[131] Professor Zhou Hanhua at the Chinese Academy of Social Science has also been deeply involved in the 15 year-long legislative process and the three versions of PIPL since 2020.[132]

3. State-market Co-Production of Data Protection and a soft 'Beijing Effect'

83 The above evidence describes China's legislative and regulatory processes on data protection, in particular featuring gatekeeper and managerial liabilities. Together they show the state's institutionalisation strategy that deliberately provides a division of labour between the state and market actors, which clarifies separate spaces for the co-production of common knowledge in data governance communities.

84 Data protection practices before the PIPL 2021 already started addressing data violations using criminal punishments which established redlines for data-handling activities. They did not however provide stable private expectations on what constitutes compliant data handling practices in daily operations. PIPL 2021 is the institutionalisation effort that tries to stabilise these accumulated practices and knowledge. The PIPL's gatekeeper provisions in particular provided the state with new tools to enforce data protection through big-techs like Alibaba and DiDi. This aligns with the state's 'cooperation and deterrence' attitude that involves big-techs in the daily data governance of their third-party supplies and users.

85 PIPL also competes with the EU's digital governance framework – GDPR (2018), DMA and DSA (drafts 2020) – for high standards of privacy and data protection. Respondent Z in Shanghai claimed that 'by implementing the law well at home, we can set good examples and reach our laws beyond China as best practices (Government official X, Shanghai, 2021.3). This raises the potential of a 'Beijing Effect' in data protection practices in competition with the 'Brussels Effect'.[133] More accurately, this can be a soft 'Beijing Effect' (which is more similar to the 'Brussels Effect') that does not necessarily require expansive foreign investments or infrastructure constructions, as compared to the 'hard' Beijing Effect as recently argued through the case of the Digital Silk Road.[134]

III. Antitrust: Data Power and Interoperability

86 The Chinese state also started an antitrust movement against big-tech companies during 2020–2021 alongside its institutionalisation on security and data protection. Major cases include first, the Central Bank's 2020 investigation of Ant Group (affiliate of Alibaba Group). Ant is China's Fintech giant for e-payment and consumer loans, and claims to have more than 1 billion annual active users within China. Second, the $2.75

[131] 王锡锌个人信息国家保护义务及展开，《中国法学》，2021年第1期。[Wang Xixin, *China Legal Science*, 2021 (1)].

[132] See e.g. Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law | DigiChina (stanford.edu).

[133] See Bradford, *The Brussels effect: How the European Union rules the world,* 2020.

[134] *Cf* Erie/Streinz, The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810256 (last accessed 16 December 2022).

billion fine (comparable to $2.8 billion EU antitrust fine on Google[135]) issued by China's antitrust agency State Administration for Market Regulation (SAMR) on Alibaba Group in April 2021. Alibaba is China's e-commerce tech-giant and equivalent of Amazon.[136] Third, the SAMR $530 million fine of Meituan, which is China's food delivery tech-giant and a rough equivalent of Deliveroo/Uber Eats (food delivery) plus Yelp (consumer rating and booking). It serves 340 million annual transacting users by 2018 as claimed in its 2018 IPO at the Hong Kong Stock Exchange (HKEX).[137]

First, on November 3rd 2020 the Shanghai Stock Exchange paused the public listing plan of Ant Group after China's Central Bank and other financial regulators launched a joint investigation[138]. The Central Bank later in its press conference listed 'using market advantage status to exclude competitors' as one of the problems of Ant Group. It also raised 'breaking monopolies … and maintaining a fair and competitive market order' as the first principle of the future regulations of big-tech platforms.[139] **87**

Soon, in November 2020, data became an important factor in the *Antitrust Guideline on Platform Economy (Draft for comments, 2020)* issued by the State Council Antitrust Committee at the SAMR. This top-level *Antitrust Guideline (2021)* was passed in February 2021, which listed 'the capacity to hold and process relevant data' as a determining factor in the evaluation of a platform's market dominance under the category of the platform's 'financial and technical conditions' (Art. 11 sec. 3).[140] **88**

'Platform's data occupation situation (平台占有数据情况)' also became a 'considering factor' in defining whether a platforms can be deemed as an 'essential facility' (*bixu sheshi*) (Art. 14). Whether data itself can be deemed as an 'essential facility', however, is not clear under the *Antitrust Guideline 2021*. In fact, the 2021 Guideline explicitly deleted the part on 'deeming data as essential facility' in Art. 14 of the 2020 draft. Data was instead added as a new factor for deeming whether platforms are essential facilities (*cf* 2020 draft).[141] **89**

Nevertheless, data is listed as one of the 'essential resources and facilities' (必要资源和必需设施) among 'technology, IP', 'channel (*qu dao*), and user' in the consideration of platform-related merger controls (Art. 20). These mixed signals imply the regulator's **90**

---

[135] Google loses challenge against EU antitrust ruling, $2.8-bln fine | Reuters 2021.11.10, available at https://www.reuters.com/technology/eu-court-upholds-eu-antitrust-ruling-against-google-2021-11-10/ (last accessed 16 December 2022).

[136] China fines Alibaba record $2.75 bln for anti-monopoly violations | Reuters, available at https://www.reuters.com/business/retail-consumer/china-regulators-fine-alibaba-275-bln-anti-monopoly-violations-2021-04-10/ (last accessed 16 December 2022); 市场监管总局依法对阿里巴巴集团控股有限公司在中国境内网络零售平台服务市场实施"二选一"垄断行为作出行政处罚 (samr.gov.cn) 2021 April 10th.

[137] China Fines Meituan $530 Million in Second Tech Antitrust Case – The New York Times (nytimes.com); 市场监管总局依法对美团在中国境内网络餐饮外卖平台服务市场实施"二选一"垄断行为作出行政处罚 (samr.gov.cn) 2021; 3802297-t01hkpo (todayir.com).

[138] 关于暂缓蚂蚁科技集团股份有限公司科创板上市的决定 | 上海证券交易所 (sse.com.cn).

[139] 央行联合约谈蚂蚁集团情况公布指出存在问题与5大整改要求_监管 (sohu.com).

[140] 国务院反垄断委员会关于平台经济领域的反垄断指南 [State Council Antitrust Committee [2021] 1, Antitrust Guideline on Platform Economy (2021)], available at http://www.gov.cn/xinwen/2021-02/07/content_5585758.htm (last accessed 16 December 2022).

[141] 《关于平台经济领域的反垄断指南征求意见稿）》 (china-cer.com.cn) 2020. '认定相关数据是否构成必需设施，一般需要综合考虑数据对于参与市场竞争是否不可或缺，数据是否存在其他获取渠道，数据开放的技术可行性，以及开放数据对占有数据的经营者可能造成的影响等因素。' 认定相关平台是否构成必需设施，一般需要综合考虑其他平台的可替代性、是否存在潜在可用平台、发展竞争性平台的可行性、交易相对人对该平台的依赖程度、开放平台对该平台经营者可能造成的影响等因素。国务院反垄断委员会关于平台经济领域的反垄断指南_部门政务_中国政府网 (www.gov.cn).

ambiguous attitudes towards considering data as an essential facility, and have triggered debates among Chinese antitrust scholars.[142]

91 'Data and algorithms' were also listed as technical tools to 'restrict transactions' (Art. 15), and added as ways to form horizontal (Art. 6), vertical (Art. 7) or 'Hub-and-spoke' agreements that are monopolistic (Art. 8). 'Depriving of data' (Art. 21 sec. 1) and 'opening data infrastructure' (Art. 21 sec. 2) were added as antitrust enforcement tools.[143]

92 After the passing of this *Guideline (2021),* two massive antitrust fines were respectively issued to Alibaba and Meituan. Among others, the use of 'technical tools of data and algorithms' was deemed by SAMR as conducive to Alibaba and Meituan's abuses of market dominance that excluded competitors by forcing suppliers to 'choose only one (platform) between two (options) (*er xuan yi*)'. Besides these two fines, SAMR also issued two similarly drafted 'administrative guidance' that respectively prohibits Alibaba and Meituan's future anticompetitive behaviours including those that involve 'the use of data and algorithms'[144].

93 It is worth noting that SAMR, the antitrust agency, did *not* claim that data or algorithmic power were considered as defining factors for Alibaba or Meituan's market dominance. Therefore, no antitrust measures on firm structures were taken.[145]

94 Another high-profile antitrust practice focused on data and platform interoperability. In September 2021, the MIIT (the industrial regulator but not the antitrust agency) held an administrative guidance joint-meeting with big-tech companies including Douyin (the Chinese TikTok), Taobao (Alibaba), Wechat (Tencent) and others. The MIIT required these tech-giants to stop blocking each other's links and data flow on their platforms or affiliated companies within a week in order to improve interoperability.[146] This is similar to the EU's *DMA (2020 Draft)* which requires gatekeepers to ensure fair competition for their third-party suppliers.[147] While Wechat is still reported to be partly resisting Taobao (Alibaba) links[148], major platforms including Wechat, Alibaba and Douyin changed their technical architectures to comply with this administrative guidance.[149]

95 These antitrust practices combine new legislative efforts with state enforcement and administrative guidance, which together require big-techs to develop self-governance rules and help maintain a competitive digital market order. These practices institute a new antitrust regime in the digital economy and co-produce common knowledge in the new epistemic communities of antitrust agencies and private actors.

---

[142] 王健 吴宗泽论数据作为反垄断法中的必要设施 (shupl.edu.cn) 2021；陈永伟: 数据是否应适用必需设施原则——基于"两种错误"的分析，《竞争政策研究》2021:4. 李世佳: 论数据构成必需设施的标准——兼评《关于平台经济领域的反垄断指南》第十四条之修改， 河南财经政法大学学报. 2021,36(05).

[143] 国务院反垄断委员会关于平台经济领域的反垄断指南_部门政务_中国政府网 (www.gov.cn).

[144] 市场监管总局依法对阿里巴巴集团控股有限公司在中国境内网络零售平台服务市场实施"二选一"垄断行为作出行政处罚，available at https://www.samr.gov.cn/xw/zj/202104/t20210410_327702.html (last accessed 16 December 2022); 市场监管总局依法对美团在中国境内网络餐饮外卖平台服务市场实施"二选一"垄断行为作出行政处罚， available at https://www.samr.gov.cn/xw/zj/202110/t20211008_335364.html (last accessed 16 December 2022).

[145] Id.

[146] 工信部召开"屏蔽网址链接问题行政指导会"， available at http://tech.china.com.cn/internet/20210911/380718.shtml (last accessed 16 December 2022).

[147] COM (2020) 842: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act) 2020/0374/COD.

[148] 互联网行业如何"拆墙""安全"成焦点 乱码现象仍存在，available at http://news.hsw.cn/system/2021/1001/1377522.shtml (last accessed 16 December 2022).

[149] 微信能跳转淘宝了，互联网围墙"潜规则"将成往事，available at http://www.eeo.com.cn/2021/0917/504983.shtml (last accessed 16 December 2022).

Summary – State-Market Co-Production via Institutionalisation: The above evi- **96**
dence shows that the Chinese state has in recent years intensively adopted formal institutions in the fields of data security, data protection and antitrust to deal with data harms/risks in the rising digital 'economy'. This institutionalisation strategy co-produces and stabilises common knowledge in the epistemic communities of data governance in order to scale a national digital economy. Co-production means the efforts from both the state's formal practices and the private actors' informal knowledge exchange and self-governance at scales. The data security, privacy, and competitive market order in China's digital economy are provided by both formal and informal labour from public and private actors.

D. Activation: Data Property, Commons, or 'Party manages data'?

Evidence in China manifests data fragmentation at all levels. Public and private data **97**
handlers keep data to themselves and lack the incentives to share data as an 'essential factor' in the market. To deal with data fragmentation, the Chinese state adopted what this chapter calls the 'activation' strategy since 2015.

In the context of China's data governance, activation is used to contest data access **98**
and ownership, where the state innovates ways to 'activate' data flow and use by experimenting data licensing, ownership, 'use without retaining', and Party management. These different legal, technical or political arrangements 'code' or contest the socio-legal nature of data, before stabilised institutions and common knowledge can be co-produced.

Evidence of 'activation' is drawn from three cases. First, the push and pull between **99**
Ant Group and Central Bank over personal credit information, second, the contrasting approaches to data property between Shenzhen and Beijing, and third, Tianjin's case of 'Party manages data'.

I. Ant Group v the Central Bank–Licensing or Commons?

1. Central Bank's license to Ant Financial (2015–2018)

Between 2015–2018 the Chinese Central Bank used private licensing to activate the **100**
market use of personal financial credit information (which are different from personal public credit information or 'social credit'). Before 2015, the consumer credit-reporting (*geren zheng xin*) business was monopolised by the Central Bank, which meant that only public reporting of personal credit information was legal. This meant first, only the Central Bank's database can be analysed to provide risk-assessment services for commercial banks loan decisions (though commercial banks can always build their own risk models based on internal data for internal use). Second, the data types are also strictly limited, for example including, personal credit cards payment, mortgages payment, and other financial information.

However, in 2015 the Central Bank for the first time granted eight provisional **101**
licenses of consumer credit-reporting to Big-Techs including Ant Financial (before changing its name to Ant Group in 2020) and Tencent (whose consumer credit product

was never effectively online)[150]. This gave birth to Sesame Credit (of Ant Financial), which uses people's behavioural data to produce financial/social risk-scores.[151]

102 Central Bank's licenses in 2015 brought two main changes in terms of the use of personal information. First, it allowed private actors to handle personal credit information that they privately collected or acquired, giving up the Central Bank's monopoly on consumer credit-reporting. Second, the types of data being handled expanded from the narrow consumer credit data to the use of 'alternative data' including social networks, consumer habits, and other information collected by the FinTech giants.[152]

103 It is worth noting that in 2015 there were very few data protection laws in China except for the *Ninth Amendment of the Criminal Code* which served as a redline of deterrence towards novel data practices.[153] Meanwhile the 2013 *Regulation on Credit-reporting Industry* (similar to the U.S. *Fair Credit Reporting Act 1970*) only provides the legal framework for handling traditional consumer credit data in the credit-reporting industry.[154] The big-techs' handling of 'alternative data' for multiple analytical purposes was thus left in a legal grey zone, before the Central Bank's 2015 licenses granted them with more degrees of regulatory certainty and protections.

104 Respondent A, a law firm partner in Beijing, argued that these provisional licenses were taken not so much as an opening of the private consumer credit-reporting market, but as a regulatory haven for big-techs to collect data and innovate new technologies.

> *'The tech giants were desperate to get the Central Bank's provisional licenses not because of the consumer credit-reporting business itself. They wanted to have regulatory protections in collecting and analysing new data. That was a regulatory haven.'*[155]

105 In practice, Central Bank's 2015 provisional licenses provided a window period for data-driven and AI technological innovation. Sesame Credit (of Ant Financial) for example was able to experiment 'smart' projects on Alibaba's massive e-commerce ecosystem as well as collaborating with local governments in early social credit and smart city projects, though the real effects and normative aspects of these projects are debatable.[156]

2. Central Bank's Data Pooling Attempts after 2018

106 In 2018 however, the Central Bank did not renew the eight consumer credit-reporting licenses after realising the problem of data fragmentation and data silos created by these companies. It criticised the tech-giants like Ant and Tencent who kept their data strictly to themselves as 'data islands'.[157]

---

[150] 人民银行印发《关于做好个人征信业务准备工作的通知》, available at http://www.gov.cn/xinwen/2015-01/05/content_2800381.htm (last accessed 16 December 2022).

[151] See, explanation by sesame credit's former ITO 人民银行印发《关于做好个人征信业务准备工作的通知》 (antfin.com). Also see Dai, Xin, in: Everling (ed.), *Social Credit Rating: Reputation und Vertrauen beurteilen* (2020), 139–163.

[152] *Ibid.* See Sesame Credit's ITO explains how different types of data are used besides traditional financial credit-reporting data.

[153] *Ibid.*

[154] State Council's Regulation on Credit-reporting Industry 2013. No.631. 征信业管理条例 (www.gov.cn).

[155] Law firm partner A. Beijing, 2021.4

[156] See, e.g. Dai, Xin, in: Everling (ed.), *Social Credit Rating: Reputation und Vertrauen beurteilen*, 2020, 139–163. 刷芝麻信用"进"杭图借还图书 2017, available at https://zj.zjol.com.cn/news/621587.html (last accessed 16 December 2022).

[157] 万存知演讲全文八家个人征信试点机构无一合格，合格机构应该是这样, available at https://www.leiphone.com/category/fintech/9OZUYsGKPrV6I4fm.html (last accessed 16 December 2022).

The Central Bank instead established a fully licensed joint-venture, Baihang Credit in Shenzhen, with a shareholding structure that gave Ant Financial, Wechat (Tencent) and other seven companies each 8 % shareholdings. The goal was to incentivise these private tech giants to pool their personal credit data into this joint venture. However, such pooling effort is reported to have stagnated as of 2019.[158] This may have contributed to the motivation of the state to use antitrust measures against Ant Group as discussed above. **107**

In December 2020, the Central Bank fully licensed another consumer credit-reporting company, Pudao Credit, which situates in Beijing and is also a joint venture between state and corporate holders, including big-techs in China like JD.com (25 %), Xiaomi (17.5 %), and Kuangshi Technology (17.5 %)[159]. It is reported to be trialling new ways of big-data innovation for micro-finance, but it is unclear if data pooling is arranged between these shareholders as of 2021.[160] **108**

This history of the central bank v Ant Group since 2015 shows the push and pull between the state and corporations trying to deal with data fragmentation by activation. Moreover, the following section presents a local competition between Beijing's 'data pooling' approach, and Shenzhen's attempted data property right approach. **109**

II. Beijing v Shenzhen: 'Use without Retaining' or Property Right?

1. Data Fragmentation due to Ownership and Compliance Uncertainties

Respondent X, a Shanghai official, claimed that it is very difficult for local governmental agencies with share data with each other because there are risks that internal mistakes would be made known to another public department. There are not many incentives to share data, while sharing means potential exposure of one's weaknesses.[161] **110**

Respondent C complained about lack of data access as a data scientist and product manager in a state-affiliated credit-reporting company in Qingdao. The Central Bank's credit payment data is the most important data type to train and test the prediction accuracy of the algorithms. Machine learning (ML) techniques like back-propagation cannot work without this crucial data set. **111**

> *'My team cannot train useful machine-learning models because we don't have the data on loan paybacks from the Central Bank's Qingdao branch. Without that data we cannot label our algorithmic predictions as good or bad.'*[162]

The access to credit payment data was expected to be done by negotiation between the Qingdao's municipal (horizontal state) and the local central bank (vertical state). However respondent C was uncertain about the progress during the time of the interview. **112**

Respondent C also mentioned that other important public data like financial reports, tax, and payment for employees' social insurance, all needed negotiation with powerful local governmental agencies like the SAMR, tax agency, and the social security agency. **113**

---

[158] 百行征信僵局，腾讯阿里困兽之斗, available at https://www.jiemian.com/article/3542916.html (last accessed 16 December 2022).

[159] 央行发放第二张个人征信业务许可 2020, available at http://www.xinhuanet.com/fortune/2020-12/25/c_1126908900.htm (last accessed 16 December 2022).

[160] 朴道征信错位发展，采集信贷之外的信用数据) 2021, https://www.163.com/dy/article/GC2OIQ6F053257CG.html (last accessed 16 December 2022).

[161] Government official X, Shanghai, 2021.3.

[162] Manager C, Qingdao, 2021.2.

Meanwhile accessing electricity usage data was expensive because large state owned enterprises (SOEs) like the State Grid Corporation of China already charges fees based on data access entries.[163]

114 There were also greater uncertainties of data ownership as well as data protection by the time of the interviews before PIPL 2021 was passed in August 2021 (but still left the data ownership problem unanswered).

> *'Without clear ownership arrangements and data protection rules how do we access public data? Can we keep the data we used in our hard drives?'*[164]

115 In spite of these difficulties, this state-affiliated credit-reporting company took an innovative method called 'use without retaining the data'. The technical team basically goes to different local branches of the ministries, accesses their public data and finish the calculation in their office, and takes away the software product/algorithms with some predictive capacities without taking the data away. But the problem was that they need to go to the offices and update the algorithms quite often.[165]

116 The above interview evidence only reveals the data fragmentation experienced by this particular firm in relation to public information access in Qingdao. However, Respondent C claimed that they have extensively consulted and learnt from practices in other cities like Hangzhou and Shanghai. There has been active informal knowledge exchange between local state and firms on how to access and trade data.[166]

117 Respondents at an internal discussion in Shanghai also showed their burning concerns on how to define data property and transaction under uncertain compliance regimes, especially concerning the Shanghai's big-data centre and the pilot of *Lingang* free trade zone with the aim to be a data harbour (Shanghai, 2021.3).[167] Interviews with officials at Hefei's big-data centre also show similar questions regarding data ownership and data protection (Hefei, 2021.3). The reported rise of China's big-data centres and companies also evidence the local attempts to 'activate' data use when data is actually fragmented without clear legal coding on data ownership and protection.[168]

118 Beijing and Shenzhen are two poles within these myriads of local activation experiments. Beijing adopts a commons approach to data access, while Shenzhen tried to formally establish data property right and interest in its legislation (yet without success).

2. Beijing: 'Use without Retaining'– a Data Pooling Approach

119 The Beijing International Data Exchange (BIDE) was established in March 2021 under the Beijing Municipality.[169] It partly functions as a traditional trading centre for big-data products like analytics instruments, their future financial gains, i.e. securitised data assets, and cross border data transactions (Art. 5 sec. 2).[170]

---

[163] Manager C, Qingdao. 2021.2.
[164] Manager C, Qingdao, 2021.2.
[165] Manager C, Qingdao, 2021.2.
[166] Manager C, Qingdao, 2021.2.
[167] Also see Shanghai Data Regulation (Draft for comments) 2021.
[168] 大数据中心互联网时代的"粮仓", available at http://www.cac.gov.cn/2020-03/18/c_1586070965007725.htm (last accessed 16 December 2022); 关于加快构建全国一体化大数据中心协同创新体系的指导意见 (发改高技〔2020〕1922号), available at https://www.ndrc.gov.cn/xxgk/zcfb/tz/202012/t20201228_1260496.html?code=&state=123 (last accessed 16 December 2022).
[169] 北京国际大数据交易所 (bjidex.com).
[170] 北京市地方金融监督管理局　北京市经济和信息化局关于印发北京国际大数据交易所设立工作实施方案的通知 2020.9.29, 2020.9.29, available at http://www.beijing.gov.cn/zhengce/gfxwj/202103/t20210331_2341258.html (last accessed 16 December 2022).

But more importantly, BIDE features the 'use without retaining' approach to data access (Art. 5 sec. 2) that is similar to the informally adopted method in Qingdao.[171] The difference is that in Beijing the BIDE is expected to functions as a 'pool' that helps gather data from different data handlers, while in Qingdao's case the data scientist had to go to each different branches of the government to 'use without retaining' the data[172]. **120**

Experts have commented that BIDE is better than previous data trading centres (e.g. in Guizhou) because the 'use without retaining' method circumvents the ownership question and replaces it with the 'right to use' question. It also creates a safe environment for public and private actors to access data and run their computer programs based on specific needs. The fees charged are based on the entries of data access and quantity. It is safe both in terms of data security and data protection, which adopts a 'regulatory sandbox' approach inspired by the UK's financial regulations. The sandbox environment creates a virtual space to experiment the release of data or financial instruments before taking these practices into the real market environment.[173] **121**

This chapter calls these BIDE's practices attempts towards 'data pooling', where data are being collectively governed by data communities who regularly contribute and use such data commons, with the state backing its security and compliance regimes. This categorisation is inspired by Ostrom's polycentric governance of common-pool resources (CPR), which defies a dichotomy of state v privatisation on the governance of commons like forests or fisheries.[174] **122**

The effects of Beijing's data pooling practices, however, still need to be observed in the long-run. Like Qingdao, the 'use without retaining' practices can also face the problems of regular data updates and data fragmentation when critical data providers like the Central Bank refuse to share data. **123**

3. Shenzhen: Data Property Right and Interest?

Beijing's 'use without retention' is in contrast to Shenzhen's (unsuccessful) attempt to code 'data rights' into its local legislation, which leaned towards a property rights approach. In October 2020, the central Party-state issued an implementing plan (2020–2025) which instructed Shenzhen to start piloting data property and transaction institutions, and data protection mechanisms.[175] **124**

As a result, in July 2020, Shenzhen proposed its first draft of *Shenzhen Data Regulations (2020)*. It was the first time in China a formal legislation draft that tried to stipulate 'data right' articles. They include Art. 4 on a personal data right to 'self-determination, control, processing/disposal, benefit and redress', and Art. 52 which protects 'data rights' that are exclusive to its collector or generators.[176] This triggered constitutional debates on whether the local laws could establish such data rights even before higher national laws allowed, and on whether this 'data right' would prevent the flow of data.[177] It was also argued that in the 'Wechat unfair competition case' (2020) **125**

[171] Manager C, Qingdao, 2021.2.

[172] *Ibid.*

[173] Expert opinions in 2021 news article; http://jrj.beijing.gov.cn/jrgzdt/202104/t20210401_2342064.html 2021.4.1 北京国际大数据交易所成立.

[174] See e.g. Ostrom, *American Economic Review* 100.3 (2010): 641-72.

[175] http://www.gov.cn/zhengce/2020-10/11/content_5550408.htm 中共中央办公厅 国务院办公厅印发《深圳建设中国特色社会主义先行示范区综合改革试点实施方案20202025年）》.

[176] 深圳市司法局关于公开征求《深圳经济特区数据条例征求意见稿）》意见的通告, available at http://sf.sz.gov.cn/hdjlpt/yjzj/answer/5748 (last accessed 16 December 2022).

[177] 地方无权对"数据权"立法深圳数据条例意见稿引专家热议. (2020), available at https://www.xuehua.us/a/5f15cb4ce3809536eb95207b?lang=zh-cn (last accessed 16 December 2022).

the Hangzhou Internet Court decided that personal data is protected as a 'right of control' at the individual level, but the corporations only have competition rights with regards to the 'data pool'[178]. This was used by legal scholars as evidence against writing 'data rights' into the latter two versions of the *Shenzhen Data Regulation (2021)*.[179]

126 In July 2021, Shenzhen passed its final version of the *Data Regulation* (effective January 2022) after the second draft (May 2021). It deleted all articles regarding data rights, and explained in a companion legislative note that there has been 'no consensus on data rights', and it is difficult to create this 'new right category' in local legislation. However, in Article 4 it does recognise the property right of data products and services made by natural and legal persons, which is not controversial in the existing legal framework.[180]

127 Shenzhen's data legislation saga is to some extent similar to the Central Bank's 2015–2018 private licenses, though Shenzhen's early efforts were rejected in later drafts. The state started by proposing privatised legal arrangements that incentivised corporations to innovate new ways of using their data, but later challenged by needs of better data access and flow. In contrast, the data pooling idea also appeared in both the Central Bank's post-2018 approach on consumer credit information and the Beijing 'use without retaining' cases.

III. Tianjin: 'Party manages data'

128 A final form of the activation strategy is by resorting to the Party's leadership. It is more politically flexible than the Central Bank's licensing and the experiments on data access or ownership (Beijing v Shenzhen).

129 In Tianjin Municipality, the party-vanguard raised the idea of 'Party manages data' (*dangguan shuju*) since 2019, which so far only focuses on facilitating the use of public information collected by local government agencies.[181] News reported that this strategy is crucial for data security and improving governance performances. For example, it was reported to be very useful in the COVID-19 pandemic governance. Public big data were used in conjunction with the 'grid management' in streets and neighbourhoods. The 'red, orange and green QR code' system was claimed to be effective where civil servants and community workers use these systems in respective 'grids' (streets) to help identify risks.[182]

130 Wang Yun, the chief officer of the Tianjin Big Data Centre (a public department in Tianjin government) argued in a news report that 'Party members should have some spaces and immunity to trial and error in their innovative use of data for the public good'.[183] In 2020 the Tianjin Big Data Centre passed an *Implementation Measure* (2020)

---

[178] (2019) 浙8601民初1987号 [2019, Zhejiang, 8601 Civil first instance case no. 1987] 2020）浙01民终5889号 [2020, Zhejiang, 01 Civil appeal case no. 5889].

[179] 地方无权对"数据权"立法深圳数据条例意见稿引专家热议, available at https://www.xuehua.us/a/5f15cb4ce3809536eb95207b?lang=zh-cn (last accessed 16 December 2022).

[180] 深圳市第七届人民代表大会常务委员会公告第十号）(2021), available at http://www.sz.gov.cn/zfgb/2021/gb1218/content/post_9307139.html (last accessed 8 February 2023) [Shenzhen 7th People's Congress Plenary Committee Report No. 10. On passing the Shenzhen Economic Special Zone's Data Regulation, 2021. Effective 2022.1.1].

[181] 坚持党管数据建设数字天津 [Insist on the Party manages data method to build digital Tianjin, www.cac.gov.cn, last accessed 15 April 2019].

[182] http://stdaily.com/index/kejixinwen/2021-09/08/content_1218450.shtml "党管数据"是保证数据安全的必由之路; http://www.xinhuanet.com/2021-01/05/c_1126949362.htm "党管数据"天津样本——专访天津市委宣传部副部长、市委网信办主任王芸.

[183] http://www.xinhuanet.com/2021-01/05/c_1126949362.htm "党管数据"天津样本——专访天津市委宣传部副部长、市委网信办主任王芸.

to list certain immunity measures to promote the local party cadres to take more responsibilities and adopt new technologies in governance. This is a follow-up policy of the Tianjin Municipality's 2018 *Action Plan (2018-2020)* which aimed to tackle the problem of party members' 'inaction and not taking responsibilities'.[184]

Wang also claimed that Party's leadership is important to break 'information islands' and 'data chimneys', and big data is crucial to the Party's governance capacity and performance. She categorised the major achievements of this strategy since 2019 as enhancing top-level designs of governmental data, 'promoting the development of digital economy' and 'services to the people'. Wang provided some examples. (1) Governmental data sharing with national and ministerial agencies to coordinate financial and market regulations and building risk-models and emergency management systems. (2) Using data to help with economic recovery after the COVID-19 pandemic in 2020 by analysing economic data (e.g. on tax) to help private companies decide when to get back to work and alleviate their pressures on cash-flow and loan payback. The Tianjin Big Data Centre also designed a technology called 'code for frozen food'. It traces the supply of frozen food from sea ports to the serving tables, as COVID-19 virus proved to survive in frozen environments via the supply chain. (3) Providing public information to the local communities on daily life, including municipal construction plans, environment concerns, fire safety, noise pollution, police alerts, community disputes and so on.[185] **131**

Outside of Tianjin, this 'Party manages data' approach has also been advocated, for example by large state-owned enterprises in their data security compliance work in general.[186] **132**

Despite its emphasis on a political and flexible handling of data, Tianjin's 'Party manages data' strategy still need to comply with data laws including the PIPL 2021 that regulates both public and private 'data handlers'. The party-state most likely can only legally access and use public information collected by state agencies themselves under legal procedures. Against private actors, Tianjin is actually one of the first few cities that passed a local legislation (effective January 2021) that bans the private collection of biometric data including facial data (Art. 16).[187] Government news also claim that the city is at the forefront of personal data protection practices against abusive private information collection and processing.[188] Nevertheless, there is rather limited information on the protection against public abuse. The empirical and normative aspects of Tianjin's 'Party manages data' practices still require further fieldwork and long-term observations. **133**

Sectional conclusion – Legal coding/pooling of data assets via activation: Attempts have been made to 'code' data with legal arrangement in China, yet without conclusive agreements among stakeholders. Data fragmentation is revealed at different ministerial (vertical), regional (horizontal) and corporate levels. To cope with data fragmentation, **134**

[184] http://www.gov.cn/xinwen/2018-04/03/content_5279425.htm 关于深入开展不作为不担当问题专项治理三年行动方案2018—2020年）.

[185] http://www.cac.gov.cn/2021-08/18/c_1630875756964401.htm 党管数据的津门"智"理，光明日报, last accessed 18 August 2021.

[186] http://theory.people.com.cn/n1/2021/0830/c40531-32212137.html 坚持党管数据 保障数据安全.

[187] 天津市社会信用条例天津市第十七届人民代表大会常务委员会公告，第63号）available at https://flk.npc.gov.cn/detail2.html?ZmY4MDgwODE3NTI2NWRkNDAxNzYzYzc1Zjg0ZTU3MWY%3D (last accessed 5 May 2023) [Tianjin Social Credit Regulations, Tianjin 17th People's Congress Plenary Committee Report, No 63. Effective on 1 January 2021].

[188] 天津扎实开展数据安全和个人信息保护工作 [Tianjin steadily develops work on data security and personal information protection, www.tjcac.gov.cn, last accessed 20 August 2020]; 天津市开展APP违法采集个人信息集中整治 [Tianjin works on regulating APP illegal collections of personal information, www.gov.cn, last accessed 23 November 2019].

the Chinese party-state adopted different forms of activation strategies as shown in case studies. These include the cases of Central Bank v Ant Group, Beijing v Shenzhen and Tianjin's 'Party manages data'.

135 In these three case studies the state provided legal and policy spaces for the coding and contestation of data's ownership and access. If we borrow Roman law's concept, data so far, in its individual form, seems to be *res nullius* – physical things that have not or have never had an owner. This legal category includes the individual 'wild animal', or *ferae naturae*, which will not become property until being captured/killed.

136 Following this metaphor, the activation strategy allows individual units of data, i.e. the new 'wild animal', to be captured in a window period by public and private 'hunters'. The strategy allows them to try ways that best use the captured data in privatised or collective ways. The competition between ministerial (vertical), regional (horizontal) and corporate interests jointly contest the technical-legal arrangements of data access and use, with informal knowledge exchange happening in data governance communities including scholars, lawyers, and social groups across geographic or administrative regions.

137 While the activation strategy provides dynamic periods of state-market co-production of new practices and knowledge, this paper also observes an emerging 'data pooling' approach from these practices. Instead of hunting 'wild animals', China's data governance in practice may lead towards a common-pool resources (CPR) governance approach, similar to the governance of forestry or fisheries studied by Ostrom. If so, activation may transit into institutionalisation which could solidify a CPR-based practice of data governance.

E. Layering: Data Cycles, Local Habitats, and Sustainable Design

138 As required in the party-state's top-level data policies, data security, data markets, access and transaction are all foundations for the ultimate goal to 'increase the values of data resources'[189]. Evidence however finds a lack of valuable and sustainable use of data in governance settings, which the local public actors try to address.

139 This chapter 'Layering' describes the local state actors' attempts to build sustainable data cycles and habitats with in-depth understanding of data's local institutional contexts. This can be seen as a data strategy that is concerned with better designs of laws and technologies in order to achieve valuable and sustainable data use in governance. The strategy provides an insight that data cycles are generated locally and data scaling is limited by institutional layering. Evidence is mainly drawn from empirical observations of China's smart court and the social/financial credit risk-assessment projects.

I. Smart Court: National v Local Practices

140 The 'Smart Court' project in China has experienced difficulties when applying data-driven technologies to the court's daily operations. Not only did such difficulties happen

[189] 中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见 [CPC Central Committee and State Council: Instruction on Improving the Market Mechanism for Allocating Essential Factors, 2020.3.30.], available at http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm (last accessed 16 December 2022).

at the Supreme People's Court's (SPC) national case recommendation system, but also many provincial High Courts' databases and models. Evidence shows limitations in these efforts that use China's judicial big-data with the goal to help judges make consistent judgements and accelerate the proceedings.

More specifically, the national (SPC) and provincial (High Court) case recommenda- **141**
tion systems are not effective enough to gain popularity among judges because the recommended cases were not always very relevant. This low relevance in matches can be partly due to the insufficiency of digitised court judgments before the 1990s/2000s to form long-term time series, and sometimes the concentrated caseloads in certain years or regions that were weighted over-heavily in the algorithmic models.[190] Respondent B, a judge and court administrator in a Shanghai Intermediary Court, said:

> *'While technology can improve efficiency of the court, the quality of judgments cannot be rushed in the Smart Court progress.'*[191]

The judges in this Shanghai court use another locally designed 'typical case' system, **142**
instead of the national system, Respondent B also mentioned. This local system is built by more traditional ways of human-selection, i.e. senior judges come together to discuss what new cases can be seen as important and typical, and circulate these cases to the entire court and lower courts.[192]

These 'typical cases', without any high-tech involved, are claimed to be more helpful **143**
in the long-term. It alludes to the temporal aspects of layering – data and its knowledge accumulated through time within institutions with path-dependency. Local courts can have their own concerns and ways of generating judicial data which can be difficult when scaling to the national level. This means data-driven technologies in governance contexts might be more effective at local level with longer time-scales.

Another example is the 'algorithmic case allocation' system used in this Shanghai **144**
intermediary court to automate the process of case assignment. It claims to help prevent judges from arbitrarily picking cases they wish to decide, and also makes more efficient division of labour by sending simple cases to junior judges while the complex ones to senior judges.[193] This local court practice gained much support by judges at the court, which is largely due to the active participation of judges in the design and updates of this algorithmic system. At the initial design of this system, data scientists and judges sit together to discuss the data categories and the labelling of the cases' cause of actions. Periodically the senior judges come back to evaluate the system's performance, following the operational cycles of the court and the time when legal institutions change. For example, when new types of cases emerge due to legal amendments or new judicial interpretations, the senior judges would make decisions on how to change data categories in terms of the cause of actions, and ask the court's information team (with computer scientists) to update the system. This also follow the court's own judgement cycles which determine the data lifecycle of generation, processing and use.[194]

The smart court cases show that legal institutions operated at the local level are coded **145**
into the data cycle construction and modelling. These legally and historically embedded technologies retain shared knowledge and practices, like the 'sediments of time', shaped by interactions between lawyers, judges, administrators and the wider legal epistemic

[190] 左卫民，如何通过人工智能实现类案类判，《中国法律评论》，2018年第2期。[Zuo, Weimin, *Chinese Legal Commentaries,* 2018 (2).]
[191] Judge and Court Administrator B, Shanghai, 2021.
[192] *Ibid.*
[193] Judge and Court Administrator B, Shanghai, 2021.3.
[194] Judge and Court Administrator B, Shanghai 2021.3.

community.[195] These technologies, like laws, thus require timely updates and alignments to the changes of external environments, including their legal institutional context and the court's own operational environments. Both legal and tech epistemic communities are crucial in such law-tech co-evolution process.

II. Social/Financial Credit: Public Information for Risk-assessment

146 'Data sediments' were first referred to in official documents in the State Council's E-Government instructions 2017. In that context, data sediments mean the long-term accumulation of public data in government practices. This temporal strategy is important in the use of public information for risk-assessment in the state project of social and financial credit systems. Cases in Shanghai and Qingdao are discussed below. Respondent D, a civil servant in Shanghai, made an illuminating point on the state's layering practice as building 'data habitats' when discussing the ways forward for the Shanghai's use of public credit information:

> *'We need to build a habitat for data, like raising fish in a garden pond. It takes time for the fish to grow and then you can draw useful information from this data.'*[196]

147 The fish pond analogy interestingly echoes with Ostrom's case studies on the governance of fisheries, i.e. the common-pool resources (CPR). The data habitat analogy reveals the commons or pooling aspects of data, which has sustainability and time concerns with regards to its own data cycles in its long-term institutional environments (similar to CPR regeneration cycles in polycentric governance)[197].

148 This idea of data habitat was raised when discussing the challenges in some of the risk-assessment practices in Shanghai. Respondent D said that the risk scores generated for businesses sometimes are not very useful for an experienced regulator when deciding how to allocate inspection resources.

> *'[… The regulators] don't need our risk models that much data because they already have a deep understanding of the places to safeguard the market order. Our public credit information is not that often useful for them'.*[198]

149 Respondent D also mentioned that the depth of the data requires understanding of the data habitat, because data interpretation has different layers through time.

> *'You also need a habitat to understand the depth of the data. If someone has a criminal record, but because of over-defending himself or others in a violent crime, then maybe he can be seen as brave. To understand him you need more data over a period of time and context.'*[199]

150 The standardisation of data meant the losing of certain depth of understanding of the data which should be interpreted in its context. Data layering means to understand data not just as numbers or digits, but also the embedded meaning of those data in the environments where it was generated and construed. In this way the data applica-

---

[195] A concept borrowed from Koselleck, 2018. Also see Zuo, Zhenbin, *Governance by Algorithm: China's Social Credit System* (working paper), 2020, available at https://www.finance.group.cam.ac.uk/system/files/documents/GovernancebyAlgorithm_CERF_Zhenbin6.16.2020.pdf (last accessed 16 December 2022).

[196] Civil servant D, Shanghai, 2021.3.

[197] See e.g. Ostrom, *American Economic Review* 100.3 (2010), 641-72.

[198] Civil servant D, Shanghai, 2021.

[199] *Ibid.*

tions can provide more accurate and helpful use in the long-run without being locked-in its path-dependency.

To achieve deeper knowledge in the field and in its context, human expertise or tacit knowledge is also required to pass on informal knowledge alongside formalised institutional knowledge. Respondent D mentioned that: **151**

> *'In market regulations, the local authorities usually are already quite familiar with the business situation because they have been there for years. They know who the major players are and how to regulate them, while smaller shops come and go (…).'*[200]

Layering thus requires human expertise to pass on informal knowledge and provide a larger picture of the data contexts. This hybrid between human expertise (regulators' informal knowledge) and formal data support (institutionalised public credit-reporting) together shapes the technology and their actual use in Shanghai's public credit information centre. Moving from Shanghai to Qingdao, Respondent C who works at a state-affiliated credit-reporting company in Qingdao also described the rooms for improvements on their risk-prediction products in the longer term: **152**

> *'Each commercial bank has its own way of collecting and accumulating data. They have their own risk models for lending decisions built after for a long time, and often use our data analytics products as an auxiliary that often needs to be recalibrated according to their own understanding (…) They have been in the field for much longer, and knows how to recalibrate polluted or distorted data. What we could do is to provide more comprehensive data models for them, and their own insights acquired through time can correct our models and predictions.'*[201]

This shows that even at local levels, useful data applications are hard to achieve without understanding the specific needs and tacit context over time. Informal knowledge retained and exchanged in private actors like banks thus are crucial for the in-depth application of standardised and large-scale data in the long run. They are epistemic communities that help retain the embedded cognition/knowledge through time. **153**

Data cycles and their path-dependence on the legal institutions was also discussed by Respondent C: **154**

> *'The data on quarterly financial reports is not helpful because many small businesses don't even survive that long. The data disclosure cycle follows certain administrative practices established in the past. You need to changes those then we can extract useful information.'*[202]

This highlights the importance of legal institutions like financial disclosure rules on the generation and update of data in its habitat. The data cycles are path-dependent on how law regulates the periodical publication of for example the firm's financial reports. This could be extended to other situations where public data are restrained by each regulatory agency's own mandate, such as tax, social insurance paid for the employees, electricity usage etc. These different institutions and organisational operations create various time frames at local levels and thus diverse data cycles. **155**

[200] *Ibid.*
[201] Staff C, Qingdao, 2021.2.
[202] Staff C, Qingdao, 2021.2.

III. Law-tech Co-Evolution and Layering in Design

156 The above qualitative evidence reveals aspects of the practical hurdles that need to be surpassed before achieving sustainable data governance for data applications. Compared to industrial big-data, the massive amount of public information (including court judgements) and personal information may not be as easy to use for example in judicial and social/financial governance settings.

157 As a result, data assets are hard to evaluate, especially when the legal contestation on data property and commons are still ongoing. Alibaba and Deloitte's joint report (2019) also pointed out that data is not yet deemed as assets in accounting, and thus cannot be represented in financial reports.[203]

158 Some secondary grey sources also reveal emerging trends to make use of the public 'data sediments'. Huawei for example claimed that 'we help government have its data assets sedimented'.[204] It also tries to provide services on big data ecosystems.[205] Various businesses and reports also actively use terms like 'awakeing the sleeping data sediments'.[206] Although these slogans can be corporate marketing strategies, they share common themes of releasing the value of long-term accumulated public information in governance, which requires building a better data habitat.

159 Moreover, Shi's research on COVID prediction puts 'emphasis on heterogeneous, unstructured data (…) and let unfiltered data become sediments.' He explained that medical and socio-economic data need to be accumulated over time to achieve a good prediction of COVID-19 cases. 'Only high quality data can have good results'.[207] The big-data predictions in turn shapes laws and policies on COVID governance. This can also be seen as data layering practices that utilise long-term institutional data for governance and shape new data cycles of generation and use.

160 Attempts have been made to layer data institutions and build data habitats in Smart Court, social and financial credit systems, and some corporate or research use of public data. These emerging cases demonstrate a law-tech co-evolution process where layering is a key strategy to the timely adjustment between institutions and the technological design and prevent pathological path-dependencies. For example, data cycles can be co-designed and updated by judges, regulators and data scientists in areas like market regulations and disclosure cycles. In specific industries like banking for instance, market regulators and commercial banks can be involved in the design of public data infrastructures that helps update data cycles and bank's lending decisions and financial regulations.

---

[203] Deloitte and Alibaba Research Institute, Path towards data assetization, 2019. 德勤携手阿里研究院联合发布《数据资产化之路——数据资产的估值与行业实践》报告 (deloitte.com).

[204] 田林一: 沉淀政府数据资产，实现数据随需共享 – 华为期刊 (huawei.com) [Tian, Linyi. Sediments of government data assets, realising data sharing upon demands. Huawe.com] (last accessed 16 December 2022).

[205] 大数据生态系统-华为云 (huaweicloud.com) [Theme on Big data ecosystem, see Huawei Cloud website] (last accessed 16 December 2022).

[206] See e.g. WakeData惟客数据-唤醒沉睡的数据 (wakecloud.com) [Awake the sleeping data, wakecloud.com]; 我国大数据快速发展，唤醒"沉睡"的数据赋能各行各业(ruiec.com) [Rapid development in big-data, awakening the 'sleeping' data to empower all industries, ruiec.com] (last accessed 16 December 2022); 数据"沉睡"制约大数据产业发展 _ 经济参考网 (jjckb.cn) [Wu, Shuaishuai, jjckb.cn, 2017.3.23].

[207] 任芳言让数据沉淀的人—新闻—科学网 (sciencenet.cn) [Ren, Fangyan: a person that lets data precipitate. 2021.1.5.] Reporting on Shi Yong's work in predicting COVID case growth in Wuhan (last accessed 16 December 2022).

Public and private epistemic communities in this sense can generate new knowledge and practices for valuable data use. They can help provide a deeper understanding of how past data is locally layered through time and shaped by law-tech co-evolution. With emerging evidence of layering, this chapter conceptualises it as a strategy that helps better design institutional data habitats/ecosystems. **161**

F. Conclusion

The chapter conceptualises three data strategies of the Chinese party-state in practices: institutionalisation, activation and layering. It concludes that the Chinese party-state uses these strategies to co-produce a data-driven regulatory state and a national digital market. It contributes to the more general theoretical debate on state-market relationship, and argues that a rising rule-of-law state in China co-produces the digital economy, shapes data 'property' and commons, and co-evolves with new technologies. More specifically, the three state strategies are conceptualised based on institutionalist theories of law and economics, and are examined by doctrinal and qualitative evidence drawn from China's recent developments since 2010s. **162**

Institutionalisation is shown to works as a stabilising strategy. It facilitates state-market co-production of common knowledge by stabilising formal institutions that deal with data security, data protection and antitrust concerns. Cases are drawn from DiDi's IPO security review, the legislative process of PIPL featuring gatekeeper and managerial liabilities, and the antitrust actions on Ant Group, Alibaba, Meituan and other big-techs. These cases together show the rise of stabilising legal institutions and a knowledge-based regulatory state co-produced with a national digital market. They also reinforce a public-private divide that facilitates division of labours between state and market actors in co-producing security, data protection and market order facing a rapidly evolving digital society. **163**

Activation is observed to serve as a contestation strategy. It triggers co-production of epistemic communities which experiment data commons, ownership, or political leadership approaches to tackle data fragmentation. Activation allows for dynamic and provisional ways of activating the data market and use, while also exhibiting tendencies to be later institutionalised into stabilised common knowledge and coded into formal laws. Cases of the Central Bank v Ant Group, Beijing v Shenzhen, and the Tianjin's 'Party manages data' were provided. They demonstrate a dynamic data commons/pooling approach is emerging, while data property is highly contested. These cases also show that data property or commons thus do not emerge by themselves, but require legal-political contestations. **164**

Layering is evidenced to function as a sustainable development strategy. It only recently emerged as a strategy to build data cycles and long-term habitats that facilitate the in-depth understanding of data and the use of valuable data. It reveals that while big data is useful in large-scale governance projects, news data technologies are layered, i.e. path-dependent on existing socio-legal institutions. Cases of China's Smart Court, the social and financial credit systems, and other grey resources provide initial evidence on the state's layering approach towards co-design of data cycles and habitats for more valuable applications and deployments of data technologies. **165**

The conceptual model of institutionalisation, activation and layering contributes to an institutionalist understanding of China's data law, policy and practices in relation to China's digital market and data-driven technologies. It is also intended as a common **166**

theoretical framework that can be applied beyond its data context and to analyse other countries' legal systems and practices. This strategy model and its theoretical foregrounding pave the way for more comparative studies and empirical research which is beyond the scope of this chapter. The normative implications of these strategies and data governance practices also requires further examination, ideally based on more empirical evidence.

Bibliography

I. Major books and articles

167 Aoki, *Corporations in evolving diversity: Cognition, governance, and institutions*, 2010

Chen/Deakin/Siems/Wang, Law, trust and institutional change in China: evidence from qualitative fieldwork, 17(2) *Journal of Corporate Law Studies* 257 (2017)

Chen/Deakin, On Heaven's lathe: state, rule of law, and economic development, 8(1) *Law and Development Review* 123 (2015)

Dai, Toward A Reputation State: A Comprehensive View of China's Social Credit System Project, *Social Credit Rating: Reputation und Vertrauen beurteilen* 139 (2020)

Davis/Ostrom, A public economy approach to education: Choice and co-production, 12(4) *International Political Science Review* 313 (1991)

Deakin/Gindis/Hodgson/Kainan/Pistor, Legal institutionalism: Capitalism and the constitutive role of law, 45(1) *Journal of Comparative Economics* 188 (2017)

Deakin, Evolution for Our Time: A Theory of Legal Memetics, 55 *Current Legal Problems* (2002)

Deakin, Juridical ontology: the evolution of legal form, *Historical Social Research/Historische Sozialforschung* 170 (2015)

Deakin, Legal Evolution: Integrating Economic and Systemic Approaches, 7 *Review of Law and Economics* (2011)

Deakin/Markou, Evolutionary Law and Economics: Theory and Method, *Northern Ireland Legal Quarterly* 72.4 (2021)

Deakin/Meng, Resolving Douglass C. North's 'puzzle' concerning China's household responsibility system, *Journal of Institutional Economics* 1 (2021)

Deakin/Meng, The Governance of Covid-19: Anthropogenic Risk, Evolutionary Learning, and the Future of the Social State, 49(4) *Industrial Law Journal* 539 (2020)

Deakin/Wilkinson, *The Law of the Labour Market: Industrialisation, Employment, and Legal Evolution*, 2005

Griffin, CFIUS in the Age of Chinese Investment, 85 *Fordham L. Rev.* 1757 (2016)

Hildebrandt, Code Driven Law. Scaling the Past and Freezing the Future, in: Markou/Deakin (eds.), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence,* 2020

Hildebrandt, Law as Information in the Era of Data-Driven Agency, 79(1) *The Modern Law Review* 1 (2016)

Hildebrandt, The adaptive nature of text-driven law, 1(1) *Journal of Cross-disciplinary Research in Computational Law* (2021)

Koselleck, Sediments of Time on possible histories, 2018

Markou/Deakin, Ex Machina Lex: Exploring the Limits of Legal Computability, in: Markou/Deakin (eds.), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence,* 2020

Ostrom, Beyond markets and states: polycentric governance of complex economic systems, 100(3) *American Economic Review* 641 (2010)

Ostrom, Crossing the great divide: Coproduction, synergy, and development, 24(6) *World development* 1073 (1996)

Ostrom/Whitaker, Community control and governmental responsiveness: The case of police in black neighborhoods, 10(4) *Improving the quality of urban management* 303 (1974)

Ostrom/Whitaker, Does local community control of police make a difference? Some preliminary findings, *American Journal of Political Science* 48 (1973)

Parks/Baker/Kiser/Oakerson/Ostrom/Ostrom/Percy/Vandivort/Whitaker/Wilson, Consumers as coproducers of public services: Some economic and institutional considerations, 9(7) *Policy studies journal* 1001 (1981)

Peters, Optimal leverage from non-ergodicity, 11(11) *Quantitative Finance* 1593 (2011)

Peters, The ergodicity problem in economics, 15(12) *Nature Physics* 1216 (2019)

Pistor, The code of capital, 2019

Supiot, *Governance by numbers: The making of a legal model of allegiance*, 2017

Victor, The EU general data protection regulation: Toward a property regime for protecting data privacy, 123 *Yale LJ* 513 (2013)

Zuo, Governance by Algorithm: China's Social Credit System (working paper), 2020, Governance by Algorithm_CERF_Zhenbin 6.12.2020.docx (cam.ac.uk), available at https://www.finance.group.cam.ac.uk/system/files/documents/GovernancebyAlgorithm_CERF_Zhenbin6.16.2020.pdf (last accessed 16 December 2022)

坚持党管数据建设数字天津 [Insist on the Party manages data method to build digital Tianjin, 2019.4.15]

淘宝11.8亿条用户隐私被泄露 两男子被判刑 [Taobao 1.18 billion pieces of user information leaked, two men sentenced. Sina news, 2021.6.17]

天津市开展APP违法采集个人信息集中整治 (2021), available at http://www.gov.cn/xinwen/2019-11/23/content_5454795.htm (last accessed 8 February 2023) [Tianjin works on regulating APP illegal collections of personal information, www.gov.cn, 2019.11.23]

天津扎实开展数据安全和个人信息保护工作 [Tianjin steadily develops work on data security and personal information protection, www.tjcac.gov.cn, 2020.8.20]

王锡锌个人信息国家保护义务及展开，《中国法学》，2021年第1期。[Wang Xixin, "Personal information's state protection obligations and its implications." *China Legal Science*. 2021 (1).]

张新宝互联网生态"守门人"个人信息保护特别义务设置研究，《比较法研究》，2021年第3期。[Zhang Xinbao. "Research on Internet ecosystem's Gatekeepers special protection obligations to personal information." Comparative Law Journal. 2021 (3)

左卫民如何通过人工智能实现类案类判，《中国法律评论》，2018年第2期。 [Zuo, Weimin. 2018. "How to achieve similar case with similar judgements by AI". *Chinese Legal Commentaries*. 2018 (2).]

II. Laws, policies and cases

1. Major Laws and regulations (including drafts)

COM (2020) 842: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act) Procedure 2020/0374/COD

COM (2020) 825: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Procedure 2020/0361/COD

中华人民共和国民法典 [Civil Code of the People's Republic of China 2021], available at http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml (last accessed 16 December 2022)

中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China, 2021], available at http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (last accessed 16 December 2022)

中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China 2017], available at http://www.npc.gov.cn/ (last accessed 16 December 2022)

中华人民共和国数据安全法 [Data Security Law of the People's Republic of China 2021], available at http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml (last accessed 16 December 2022)

信息安全技术—个人信息安全影响评估指南(GB/T 39335-2020) [Information security technology – Guidance for personal information security impact assessment (GB/T 39335-2020)]

国务院征信业管理条例 国务院令631号）State Council's Regulation on Credit-reporting Industry 2013. No.631, available at http://www.gov.cn/zwgk/2013-01/29/content_2322231.htm (last accessed 16 December 2022)

国务院反垄断委员会关于平台经济领域的反垄断指南 [State Council Antitrust Committee [2021] 1, Antitrust Guideline on Platform Economy (2021.2.7)], available at http://www.gov.cn/xinwen/2021-02/07/content_5585758.htm (last accessed 16 December 2022)

公开征求对《移动互联网应用程序个人信息保护管理暂行规定征求意见稿）》的意见 [MIIT Mobile Internet Application Personal Information Protection Provisional Regulations (Draft for Comments), 2021.4.26], available at http://www.gov.cn/hudong/2021-04/26/content_5602780.htm (last accessed 16 December 2022)

天津市社会信用条例天津市第十七届人民代表大会常务委员会公告，第63号 2020） [Tianjin Social Credit Regulations, Tianjin 17th People's Congress Plenary Committee Report, No 63. Effective on 1st January 2021], available at http://credit.sc.gov.cn/xysc/c100016/202205/fa2757b27c104200a868f49cca46f7d6.shtml (last accessed 8 February 2023)

深圳市第七届人民代表大会常务委员会公告第十号）[Shenzhen 7th People's Congress Plenary Committee Report No. 10. On passing the Shenzhen Economic Special Zone's Data Regulation, 2021. Effective 2022.1.1], available at http://www.sz.gov.cn/zfgb/2021/gb1218/content/post_9307139.html (last accessed 8 February 2023)

2. Policies

习近平决胜全面建成小康社会 夺取新时代中国特色社会主义伟大胜利——在中国共产党第十九次全国代表大会上的报告 [Xi Jinping: Report Delivered at the 19th National Congress of the Communist Party of China – Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era, 2017.10.18], available at http://www.gov.cn/zhuanti/2017-10/27/content_5234876.htm (last accessed 16 December 2022)

中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见 [CPC central committee and State Council: Instruction on Improving the Market Mechanism for Allocating Essential Factors, 2020.3.30.], available at http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm (last accessed 16 December 2022)

授权发布:中国共产党第十八届中央委员会第五次全体会议公报-新华网 (xinhuanet.com) [Report of the Fifth Plenary Session of the 18th Communist Party of China (CPC) Central Committee. 2015.]

中华人民共和国国民经济和社会发展第十三个五年规划纲要，available at http://gov/cn/xinwen/2016-03/17/consent_5054992.htm (last accessed 8 February 2023 [The 13th Five-Year Plan of the People's Republic of China on economic and social development, 2016]

国务院关于印发促进大数据发展行动纲要的通知国发〔2015〕50号 2015, available at http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm (last accessed 8 February 2023) [State Council's instructions on the action plans for promoting big-data development, 2015. SC [2015] 50.]

国务院关于印发政务信息资源共享管理暂行办法的通知国发〔2016〕51号） [State Council on the provisional measures to government information resources sharing and management. 2016. SC [2016] 51.], available at http://www.gov.cn/zhengce/content/2016-09/19/content_5109486.htm (last accessed 16 December 2022)

工业和信息化部关于印发大数据产业发展规划20162020年）的通知 [MIIT on issuing the Big-data Industry Development Plan. MIIT [2016) 412.], available at http://www.cac.gov.cn/2017-01/17/c_1120330820.htm (last accessed 16 December 2022)

外交部全球数据安全倡议 [Foreign Ministry: Global Data Security Initiative (2020)], available at http://www.xinhuanet.com/world/2020-09/08/c_1126466972.htm (last accessed 16 December 2022)

Obama administration unveils "big data" initiative: announces $200 million in new r&d investments (Executive Office of the President, 2012), available at https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf (last accessed 16 December 2022)

3. Cases and administrative actions

United States v. Facebook, Inc., No. 19-2184 (TJK), 2020 WL 1975785 (D.D.C. April 23, 2020)

2019）浙8601民初1987号 [2019, Zhejiang, 8601 Civil Court, First instance case no 1987]

2020）浙01民终5889号 [2020, Zhejiang, 01 Civil appeal case no. 5889]

2020）浙0106刑初437号 [2020, Zhejiang, 0106, Criminal Court, first instance case no. 437]