China Leadership Monitor

China's 2021 Data Security Law: Grand Data Strategy with Looming Implementation Challenges

Aynne Kokas

China Leadership Monitor, Winter 2021 Issue 70
Wednesday, December 1, 2021

China's 2021 Data Security Law (DSL) presents a transformative vision of the country's data management practices to intensify domestic oversight and expand international influence. However, the law's limitations with respect to implementation present a challenge for both domestic regulators and multinational corporations. The law's requirement that individual regions and industrial sectors determine their own data security enforcement measures sets up the potential for competition among agencies. At the same time, its international scope raises questions for domestically focused agencies charged with enforcement and multinational firms seeking to comply with the law. This article argues that understanding the law's broader implications will require tracing the implementation practices of regions and industrial sectors based on a case study of the automotive sector.

In his September 26, 2021, letter to the participants at the Wuzhen World Internet Forum (世界互联网大会) , Chinese President Xi Jinping articulated a vision of digital civilization (数字文明), a world in which digital spaces create a "community of common destiny" (命运共同体).[1] Just weeks later at an October 19, 2021 Politburo meeting, Xi reasserted the importance of the digital economy to China's growth.[2] Both instances reiterate the importance of data to President Xi's larger ambitions. The 2021 Data Security Law (DSL) (数据安全法), which took effect on September 1, 2021, offers a legal framework that articulates this vision.[3] The DSL is a

---

[1] 习近平向2021年世界互联网大会乌镇峰会致贺信_世界互联网大会官网," 年世界互联网大会, updated September 26, 2021, http://www.wicwuzhen.cn/web21/information/Release/202109/t20210926_23146429.shtml

[2] 习近平主持中央政治局第三十四次集体学习：把握数字经济发展趋势和规律 推动我国数字经济健康发展_滚动新闻_中国政府网," 中华人民共和国政府, updated October 19, 2021, 2021, accessed November 5, 2021, http://www.gov.cn/xinwen/2021-10/19/content_5643653.htm.

[3] Ministry of Foreign Affairs of the People's Republic of China 中华人民共和国外交部, "“Quanqiu shuju anquan changyi” 全球数据安全倡议 [Global Initiative on Data Security]," (Beijing, China, September 8, 2020). https://www.fmprc.gov.cn/web/wjbzhd/t1812949.shtml; China Law Translate, "中华人民共和国数据安全法(草案) (二次审议稿)," *China Law Translate*, 2021, https://www.chinalawtranslate.com/data-security-law-draft-2/

https://www.chinalawtranslate.com/en/data-security-law-draft-2/; "Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)," *DigiChina*, 2021, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-

constellation of principles for data regulation, data security, and data-driven industries. The law has received much attention for being a vehicle for advancing both the domestic growth and international influence of China's tech industry.[4] It asserts and protects the rights and interests of citizens and organizations relative to their data. More profoundly, it establishes a direct link between data security, national sovereignty, and national security. The DSL provides a framework for a system through which China expands its sphere of influence in domestic and international data-management practices. However, what the law does not do is provide detailed guidance on implementation. Instead, execution of the law depends on implementation by regions and agencies with varying technical capacities and relative power within the nation. As such, the DSL also lays a foundation for intensive competition over data within China.

This article describes China's DSL and its larger implications. Next, it traces several of the key laws and policies that set the stage for the DSL. It then outlines the conceptual frameworks from which the law emerged. The article then maps the structure of the DSL, including the key terms that shape the law. It then examines related laws that provide additional granularity concerning how government agencies will implement the law. This article will explain how the DSL is one feature of China's longstanding progression toward controlling data generated within China by Chinese nationals, and by firms with operations in China. It is a culmination of over a decade of progressive regulatory expansion that broadly defines the Internet in China beyond the territorial scope of the PRC. Finally, the article examines the policy implications of the law both domestically in China and for businesses and organizations around the world. The article does this by examining sector-based standards from the automotive industry, one of the first industries to have its own data security provisions, to underscore the complexity of implementation. Ultimately, while the DSL offers broadly defined strategic parameters for advancing China's data-sovereignty claims, the implementation practices of regions and industrial sectors will be central to shaping the reality of China's data security landscape.

The Data Security Law Builds on Extensive Preexisting Frameworks

China's 2021 DSL sits atop over a decade of Chinese efforts in the country's digital realm. China has long had a policy of controlling information that enters the country. Since the 2010 introduction of the landmark "White Paper on the Internet in China," which asserted the concept

china/; Council of Chairman 委员长会议, "Zhonghua renmin gongheguo shuju anquanfa caoan" 中华人民共和国数据安全法（草案） [Data Security Law of the People's Republic of China (Draft)], (China: Zhongguo rendawang 中国人大网, 2020). Council of Chairman 委员长会议, Short "Zhonghua renmin gongheguo shuju anquanfa caoan" 中华人民共和国数据安全法（草案） [Data Security Law of the People's Republic of China (Draft)].. https://npcobserver.files.wordpress.com/2020/07/data-security-law-draft.pdf

[4] Цзяньвэнь Чжан and Хуань Ян, "Обеспечение безопасности данных в электронном виде (о законопроекте КНР "О безопасности данных")," *Юридическая Наука В Китае И России*, no. 4 (2021 2021), https://doi.org/10.17803/2587-9723.2021.4.074-081, https://elibrary.ru/item.asp?id=46542049.

of “Internet sovereignty,” or “cybersovereignty” （网络主权） in the Chinese context,[5] the Chinese government has developed increasingly robust mechanisms for control over data not only within the country’s territorial borders but beyond. Three major gateways structure Internet communications into China.[6] Each connects to a major city. BJ, SH, and GZ refer to the gateways in Beijing, Shanghai, and Guangzhou.[7] There are also network access points, which other gatekeepers control.[8] These network access points control access to the following government backbone networks: ChinaNet, CERNet, GBNet, and CSTNet.[9] Several new government frameworks have expanded both the legal and technical specifications for cybersecurity. The foundations of China’s DSL rely on earlier policy guidance to establish data security infrastructure in China. In the following section, I will describe these approaches, which range from legal frameworks for data security and national security to technical specifications, and beyond.

In 2017, China’s Cybersecurity Law (中华人民共和国网络安全法) entered into effect.[10] The law, which centers on data localization, requires that all "critical information infrastructure" (关键信息基础设施), including private-sector data, should be controlled by Chinese state-owned entities.[11] The Cybersecurity Law structures China's critical-information infrastructures as a fixture of its national-security apparatus. It establishes that the government's role in the governance and control of important national data requires transferring all such data, both government and commercial, to Chinese government-run servers. Article 37 of the 2017 Cybersecurity Law discourages data transfer from the country by creating difficult transfer conditions.[12] These conditions stipulate that such transfers of information can only occur when the business has a specific need for the information. In response to the law, Qualcomm set up data storage facilities in Guiyang.[13] Apple established its own data center in China following

---

[5] "《中国互联网状况》白皮书（全文）," http://www.scio.gov.cn/tt/Document/1011194/1011194.htm.

[6] Lyombe Eko, Anup Kumar, and Qingjiang Yao, "Google This: The Great Firewall of China, the II Wheel of India, Google Inc., and Internet Regulation," *Internet Journal of Law* 15, no. 3 (January 2011): 3–14. https://search.lib.virginia.edu/articles/article?id=bth%3A65287912.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Standing Committee of the National People's Congress 全国人民代表大会常务委员会, “Zhonghua renmin gongheguo wangluo anquanfa” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], (Beijing, PRC: "Zhongguo rendawang" 中国人大网 [China National People's Congress Network], 2016). http://www.cac.gov.cn/2016-11/07/c_1119867116.htm..

[11] Ibid

[12] Ibid.

[13] Aynne Kokas, "Platform Patrol: China, the United States, and the Global Battle for Data Security," *The Journal of Asian Studies* 77, no. 4 (2018),

implementation of the law.[14] The Cybersecurity Law enforces the claim that all data generated in China should be subject to government oversight.

Building on cybersecurity standards that establish where the digital borders of the nation begin and ends, the Chinese government has launched a series of national standards that dictate how information must flow within the country. A key step was to enact the Cryptography Law of the PRC (人民共和国密码法) in 2019.[15] The law established standards for government cryptographic transfers to protect national security.[16]

The law defines a new framework for national security concerning data through its guidance for commercial cryptography. It makes hacking and cryptography illegal in activities that harm state, individual, or organizational interests. This approach transforms commercial cryptography into an area of national-security scrutiny. Specifically, it makes the practice of private entities encrypting themselves to prevent government access an area of unclear legality due to data-protection principles that protect users and corporations, but it stipulates government access to the data. The 2020 Personal Information Security Specifications further contribute to China's data security legal apparatus.

Domestically, China's Personal Information Security Standards（个人信息安全规范）entered into effect on October 1, 2020.[17] The specifications, designed to refine and explain the 2017 Cybersecurity Law, articulate how companies can share individual personal information (though not generalized data). Like the Cryptography Law, in a move that foreshadowed the DSL, the specifications do not restrict government access to data.

Regulators designed the specifications' data standards to support a data-driven economy. They prevent the bundling of individual personal information into multiple business functions, a protection that evades U.S. consumers.[18] Users must be able to consent to the use of personal

---

https://www.cambridge.org/core/journals/journal-of-asian-studies/article/platform-patrol-china-the-united-states-and-the-global-battle-for-data-security/826A11255871A1D90B5B74960A5620F7.

[14] Xinhua, "Apple speeds up construction of first China data center," *China Daily*, April 27, 2019, https://www.chinadaily.com.cn/a/201904/27/WS5cc3e5afa3104842260b8ba0.html.

[15] The Chinese People's Congress 中国人民代表大会, "“Zhonghua renmin gongheguo mimafa” 中华人民共和国密码法 [Code Law of the People's Republic of China]," Government, *"Zhongguo rendawang" 中国人大网 [China National People's Congress Network]* (October 2019), http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml.

[16] Ibid.

[17] Xinhua, "Apple speeds up construction of first China data center."

[18] Tom Miles, "U.S. asks China not to enforce cyber security law," *Reuters* (September 26, 2017), https://www.reuters.com/article/us-usa-china-cyber-trade-idUSKCN1C11D1; Ryder, "China's Personal Information Specifications: Revised," *Harris Bricken*, July 15, 2020, http://harrisbricken.com/chinalawblog/chinas-personal-information-specifications-revised/; State

information for a specific business function. If the company ceases to need the consumer data for that business function, it must discontinue its collection.[19] For any sensitive data, the controllers of data (typically corporations) must obtain explicit consent.[20] The Personal Information Security Standards assert the Chinese government's control over personal information (and related data). The 2020 specifications reinforce that the transfer of personal information outside of China must comply with all relevant national standards. According to the standards, corporate data would remain subject to continued government access for national-security review.

The 2020 Personal Information Security Specifications grant Chinese consumers greater control over how corporations use their data. They reinforce the Chinese government's role as arbiter of information flows into and out of the country. Further, the lack of clarity about national-security concerns related to specific data or cryptographic techniques makes it difficult to move data out of China.

Data oversight practices like the Cybersecurity Law, Cryptography Law, and Personal Information Security Specifications extend China's data security oversight outside the physical bounds of the nation. The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region establishes a legal precedent for extraterritorial enforcement of a wide range of laws for national-security purposes. The law, drafted and legislated in Beijing, took effect in Hong Kong on July 1, 2020.[21] It offers a broad definition of national security. In Article 1, the law notes it safeguards "national security" 'preventing, suppressing, and imposing punishment for the offences of secession, subversion, organization and perpetration of terrorist activities, and collusion with a foreign country or with external elements to endanger national security in relation to the Hong Kong Special Administrative Region."[22] "National security" in the context of the DSL is closely tied to data security. Although the law applies to the Hong Kong Special Administrative Region, its origins in Beijing underscore the breadth of the Chinese government's conception of national security. The broad framing of national security then pairs with expansive extraterritorial jurisdiction.

Administration for Market Regulation 国家市场监管总局 and Standardization Administration of China 国家标准委, "Guojia biaozhun geren xinxi anquan guifan 2020 ban zhengshi fabu" 国家标准《个人信息安全规范》2020 版正式发布 [The 2020 version of the national standard "Personal Information Security Standards" was officially released], (2020). https://www.secrss.com/articles/17713.

[19] Lauren Maranto, "Who Benefits from China's Cybersecurity Laws?," *Center for Strategic and International Studies (CSIS)*, June 25, 2020, https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws.

[20] 标准委, "Guojia biaozhun geren xinxi anquan guifan 2020 ban zhengshi fabu" 国家标准《个人信息安全规范》2020 版正式发布 [The 2020 version of the national standard "Personal Information Security Standards" was officially released].

[21] "English translation of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region," http://www.xinhuanet.com/english/2020-07/01/c_139178753.htm.

[22] Ibid.

Article 38 of the law creates legal liability in Hong Kong for anyone from any national background who violates Hong Kong's national security anywhere in the world.[23] Article 43 extends the extraterritorial control of the Chinese government to corporate resources, which can include search and seizure of corporate data on critical infrastructure.[24]

The DSL emerged after over ten years of Chinese government laws and policies that enforce national data oversight. Earlier frameworks established sovereign control of data; consumer protection from corporate, but not government, data access; and extraterritorial jurisdiction. Thus, when the DSL was enacted, many of its core principles were already present in earlier laws, policies, and standards. However, the DSL played an essential role by weaving together these disparate pieces into a larger vision.

Key Features of the Data Security Law

The focus of the DSL is on regulating data, with a focus on data handling, data security, protecting the rights of users and organizations, and perhaps most notably, preserving state sovereignty and national security. Article 4 of the DSL closely links China's data security regulatory framework with the broader scope of national security.[25] This explicit linkage of data security with the more expansive concept of national security is one of the central implications of this law. By connecting data security explicitly with national security, regulators have expanded the scope of the DSL to include a much wider range of issues than mere data security.

The law focuses on developing the data security industry, national-security protocols for data protection, data-handling practices for organizations and individuals, and e-governance practices.[26] It bolsters China's domestic data security by offering support for a comprehensive Chinese big data strategy, development of domestic data standards, and data-driven industrial products. It establishes the government's authority in data security risk assessment and activities that affect national security (broadly defined).[27]

In addition to establishing a roadmap for China's larger data security strategy, a framework for state oversight of data, and broad responsibilities for organizations and individuals within the scope of data-handling, the DSL offers definitions of key terms related to data security in China. The DSL provides broad definitions of the terms "data" (数据), "data processing" (数据处理), and "data security" (数据安全) in Article 3 as a framework for understanding the law. The broad definition of these terms expands the scope of China's data security regulations. "Data,"

---

[23] Ibid.

[24] Ibid.

[25] Council of Chairman 委员长会议, Short "Zhonghua renmin gongheguo shuju anquanfa caoan" 中华人民共和国数据安全法（草案） [Data Security Law of the People's Republic of China (Draft)]. https://npcobserver.files.wordpress.com/2020/07/data-security-law-draft.pdf

[26] Ibid.

[27] Ibid.

according to the law, refers to "any record of information in electronic or other forms."[28] "Data handling" can encompass any information management, transmission, or disclosure practice. Similarly, "data security" can encompass any information security–related terms.

Critical-information infrastructure is an animating concept within the DSL, as it is in the Cybersecurity Law. Article 31 refers to the law's oversight over the export of critical-information infrastructure operators located inside the PRC (mainland). However, the law fails to define what constitutes critical-information infrastructure. The 2017 Cybersecurity Law calls for the protection of critical-information infrastructure, defining critical-information infrastructure to "public communication and information services, power, traffic, water, finance, public services, electronic governance, and other critical information infrastructure that if destroyed, lose its function, or leak data might seriously endanger national security, national welfare, and the people's livelihood, or the public interest, on the basis of their tiered protection system."[29] Notably, also entering into effect on September 1, 2021 were the "Regulations on Critical-Information Infrastructure Security Protections" (关键信息基础设施安全保护条例).[30] The protections retain most of the earlier definition of critical-information infrastructure from the Cybersecurity Law. However, there is one crucial shift that is particularly relevant to the DSL. The 2021 regulations carve out network facilities and information systems as key parts of the national critical-information infrastructure. While the 2017 law's definition of critical-information infrastructure was expansive enough to include network facilities and information systems, the 2021 regulations make this claim explicit in anticipation of the release of the DSL.

In addition to its expansive framing of "data" and "critical-information infrastructure," the DSL also offers expanded extraterritorial data governance, evoking what foreign policy scholar Gerard Toal describes as "certain technological paradigms and systems [that] enable new forms of territorialization and territoriality,"[31] Communications scholar Lisa Parks argues that technology (and technology regulations) can function as a "territorializing gesture" that extends "the power to regulate."[32] As Chinese data-driven firms grow and the Chinese market remains central to the growth aspirations of multinational corporations that retain access to doing business in China, the DSL's influence grows in parallel. Foregrounded in Article 2 of the law is

---

[28] Ibid.

[29] National People's Congress of the People's Republic of China, 中华人民共和国网络安全法, (Beijing: National People's Congress of the People's Republic of China, 2016).

[30] "关键信息基础设施安全保护条例（国令第 745 号）_政府信息公开专栏," http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm. English translation at https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/.

[31] Gerald Toal, *Geopolitical Structures and Cultures: Towards Conceptual Clarity in the Critical Study of Geopolitics*, ed. Lasha Tchantouridze, Geopolitics: Global Problems and Regional Concerns, (Winnipeg, Manitoba, Canada: Center for Defence and Security Studies, 2004). https://gerardtoal.files.wordpress.com/2011/01/toal_geopoliticalcultures2003.pdf.

[32] Lisa Parks, "Signals and Oil: Satellite Footprints and Post-communist Territories in Central Asia," *European Journal of Cultural Studies* 12, no. 2 (2009): 141..

the claim that data-handling activities outside the People's Republic of China deemed to violate the PRC's national security, public interest, or the rights of citizens are subject to the law.[33] Article 35 and Article 46 forbid and impose financial punishments for transferring data extra-territorially according to legal requests from other countries without appropriate authority.[34] In addition to limitations on data exports relative to foreign government requests, Article 24 of the DSL asserts the need for data export controls for national security.[35] Articles 2, 24, 35, and 46 closely tie broader Chinese government assessments of "national security" to control of data not only within China but also to the control of data that is gathered or may be exported extraterritorially.[36]

The law leverages a national-security justification to assert broad authority over all data-gathering practices, including a national-security review process. However, the DSL fails to outline what constitutes a national-security interest. Indeed, the DSL echoes the Hong Kong National Security Law by deliberately leaving vague the question of national-security interest to extend the potential range of the law. The DSL also includes no specific description of what the national-security audit process would constitute. While the law notes that departments and regions would be responsible for identifying their respective categories of sensitive data, the law does not specify if the national-security review system falls under the discretion of individual departments or regions. This creates uncertainty regarding how national-security reviews might be conducted, which has significant long-term implications for businesses seeking to operate in China. As a result, industry-specific, regional, and local governments have a mandate to develop their own laws concerning data security. The DSL is significant in that it unites earlier laws and policies. It reaffirms the principles of consumer protection, government access to data, and extraterritorial enforcement of China's cyber-sovereignty.

Policy Implications

Three broad policy implications emerge from the DSL. The law creates a competitive landscape for data-protection practices among government agencies. It generates complex international enforcement requirements without an international enforcement infrastructure. Finally, successful implementation hinges on clear implementation strategies both at an agency level and a regional level.

The DSL creates complexity for Chinese government regulators across different agencies. First, the DSL provides very little granularity with respect to how to execute the document's broad-ranging requirements, including technical standards to national-security reviews of data security practices with the potential to impact national security. Individual organizations are developing

---

[33] "Zhonghua renmin gongheguo shuju anquanfa caoan" 中华人民共和国数据安全法（草案） [Data Security Law of the People's Republic of China (Draft)]. https://npcobserver.files.wordpress.com/2020/07/data-security-law-draft.pdf.

[34] Ibid.

[35] Ibid.

[36] Ibid

their own standards for data protection. Competing approaches pose challenges for regulators in the data security context, particularly with respect to regulatory efficiency and the allocation of data as a resource. Agency-determined data security regulations pose the potential for internal Chinese government turf wars over control of data. Certain organizations are more well-endowed than others, and thus they more capable of introducing technical standards. For example, early movement regarding automotive data collection offered automotive regulators firsthand access to data that other regulatory agencies could use. In response to the law's second draft version, Huang Daoli and Hu Wenhua from the Third Research Institute of the Ministry Public Security in Shanghai critique the lack of clarity surrounding how the law deals with data security issues among agencies.[37]

Each regulator overseeing his own data creates the challenge of coordinating national-security reviews among agencies and localities. Patronage networks, factions, or cliques hold an important place in Chinese bureaucratic life for distributing various resources. Instituting data-security regulations offer another pathway for the control and distribution of resources.[38] In addition to its national-security importance in China, data-gathering has clear financial benefits, but it threatens to privilege the already well-endowed agencies and regions. The massive data resources generated by Chinese tech firms and adjacent industries that gather user data or industrial data present an opportunity for the development of products and resources. While some governments and regions are poised to take advantage of massive data resources, devolving authority to regional governments also poses a resource challenge for organizations without the financial or IT capacity to execute the extensive requirements of the DSL. What this already means in practice is that certain wealthy, technically oriented industries (like the automotive industry) have standards in place to manage user data. Other industries without those same financial and technical resources face a more uncertain regulatory landscape.

Beyond the turf challenges within agencies focusing on civilian data regulation, there is also competition between military data security demands and the requirements of the DSL. The law clearly carves out military data security regulations as separate from the civilian regulations covered under the DSL in Article 52, despite the clear prioritization of national security within the context of the law.[39] How to balance civilian and military interests with respect to user data is not included in the scope of the law, despite certain types of data having both clear civilian and military uses, as in the case of satellite weather data.

---

[37] Huang Daoli and Hu Wenhua, "Situation, Dilemma and Countermeasures of China's Data Security Legislation: Comment on the Data Security Law of the People's Republic of China (Draft)," *Journal of Beijing University of Aeronautics and Astronautics Social Sciences Edition* 33, no. 6 (October 2, 2020 2020), https://doi.org/10.13766/j.bhsk.1008-2204.2020.0475, https://bhxb.buaa.edu.cn/Jwk3_bhsk/EN/10.13766/j.bhsk.1008-2204.2020.0475.

[38] Ben Hillman, *Patronage and Power: Local State Networks and Party-State Resilience in Rural China* (Stanford, CA: Stanford University Press, 2014/05/14/, 2014). https://www.degruyter.com/document/doi/10.1515/9780804791618/html.

[39] Council of Chairman 委员长会议, Short "Zhonghua renmin gongheguo shuju anquanfa caoan" 中华人民共和国数据安全法（草案） [Data Security Law of the People's Republic of China (Draft)].

In addition to the internal logistical challenges for intra-government implementation, the law's international-enforcement provisions present distinct enforcement issues. The law fails to identify mechanisms for coordination between security agencies and export control regulations, foreign investment law, and civil code. The DSL requires developing a system that integrates these wide-ranging interests in the Chinese government, from technical to foreign affairs. The unclear environment for international enforcement paired with a clear mandate for international oversight over data-handling activities outside China, as noted in Article 2, presents a cloud of uncertainty over how multinational corporations could face reprisal for their international activities.[40] Asymmetrical responses to corporate violations in recent years have included everything from increased taxation to exclusion from the market to exit bans for employees and beyond. The DSL only magnifies this already challenging and uncertain business environment. Similarly complex is the challenge presented by the national-security data reviews outlined in Article 23 of the DSL.[41] The DSL offers a useful framework for understanding how the Chinese government broadly conceives the role of data management in national security. However, it offers little detail on how to approach data security and management among government agencies, and this lack of clarity presents a challenge to regulators.

Another key policy challenge presented by the DSL is its comparatively vague implementation guidance, even excluding the challenge of intra-governmental division of oversight. One of the first industries with its own data security framework is the automotive sector. Order No. 7 of the Cyberspace Administration of China (CAC), the National Development and Reform Commission, and the Ministry of Industry and Information Technology, the Ministry of Public Security, "Several Provisions on the Management of Automobile Data Security" (汽车数据安全管理若干规定) was deliberated and adopted at the tenth executive meeting of the CAC and it entered into effect on October 1, 2021.[42] Although issued by the CAC, the provisions also received support from the National Development and Reform Commission, and the ministries of Transport, Industry and Information Technology, and Public Security.[43]

The provisions relate to automotive data-processing activities. The provisions help to clarify the DSL's broader definition of "data." In the case of the provisions, "automotive data" refer to personal and important data involved in automotive design, production, sales, use, operations, and maintenance.[44] The law still leaves a carve-out for other types of data, but it provides more detail about what constitutes protected data within the automotive context than the DSL does about data security.

---

[40] Ibid.

[41] Ibid.

[42] National Internet Information Office 国家互联网信息办公室 et al., "汽车数据安全管理若干规定," 中华人民共和国互联网信息办公室, http://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm.

[43] Ibid.

[44] Ibid

Notably, the provisions also define "personal information" (个人信息) for automotive data, a term the DSL uses but does not define. While the term maintains the wide-ranging scope of the means for recording information (electronic or otherwise) present in the DSL, it does narrow the definition of data to distinguishable details about the owner, rider, driver, or individuals outside of the vehicle. The law goes on to define "sensitive personal information" (敏感个人信息) as that, when leaked or used illegally, could harm vehicle owners, drivers, passengers, and people outside vehicles.[45] The provisions clarify what constitutes personal and sensitive information, offering a framework for compartmentalizing information for user safety and demonstrating what type of personal data might be subject to consumer data protection.

The provisions define the term "important data" (重要数据) as "any data that may endanger national security, the public interest, or the lawful rights of individuals or organizations."[46] This clarifies auto industry data oversight, but it also suggests how provisions for other industries may operate with respect to the DSL. According to the automobile data security provisions, important data constitute the following:

> (1) geographical information, personnel flows, vehicle flows, and other data in important sensitive areas, such as military management zones, national defense science and industry entities, and party and government offices at or above the county level.
>
> (2) data reflecting economic operations, such as vehicle flows and logistics.
>
> (3) operating data on vehicle-charging networks.
>
> (4) video and image data outside of vehicles, including face information and license plate information, among others.
>
> (5) personal information involving more than 100,000 personal information subjects; and other data that may endanger national security, the public interest, or the lawful rights and interests of individuals or organizations as determined by the Cyberspace Administration of China, the National Development and Reform Commission, the Ministry of Industry and Information Technology, the Ministry of Public Security, the Ministry of Transport, and other relevant departments of the State Council.[47]

Whereas Article 6 of the automotive industry provisions evokes the existing DSL language about data and national security, the other provisions offer helpful insight into what specifically constitutes data related to national-security concerns. Several articles are not specific to automotive data, namely personal information involving more than 100,000 subjects, information about economic operations, geographic information, personnel information, and

[45] Ibid.

[46] Ibid.

[47] Ibid.

information about government or military facilities at or above the county level.[48] More broadly, the provisions demonstrate how the DSL, while important for setting China's larger data security agenda, relies on individual industries' standards to clarify the law's scope and priorities.[49] The provisions also provide additional details about the types of data that might be included in national-security data reviews or export controls.

The automotive industry provisions have received widespread attention because they connect with the May 2021 decision of electric carmaker Tesla to set up data centers and research facilities in China to avoid cross-border data transfers[50] as well as a March 2021 Chinese government ban of Tesla vehicles on the premises of Chinese military facilities.[51] As the Tesla case demonstrates, DSL enforcement exists at the nexus of ministry-level provisions for enforcement, government norms, corporate public-relations challenges, and nebulous definitions of terms that guide business operations.

The case of the automotive industry offers a picture of comparatively sophisticated DSL enforcement provisions. It is a high-tech sector that already must incorporate robust security protocols into all its products. However, the early promulgation of the automotive industry requirements underscores the uneven access to technical expertise and resources in different regions and industries. How the devolution of data security oversight plays out will be a crucial area to watch in the coming years as implementation of the law comes online.

Conclusion

Ultimately, the DSL offers a framework for linking data security with national security. The breadth of the DSL means that the concept of "data security," like the concept of "national security," can encompass a wider range of information, processes, and organizations than its title suggests. However, the financial incentives of data exploitation for individual government agencies encourage competitive approaches to data management among regions and agencies. Sectoral and regional enforcement of the law can leave certain sectors and regions behind, creating a further digital divide between more and less privileged regions and industries and undermining the larger ambitions of the law.

About the Author

Aynne Kokas is an associate professor of media studies at the University of Virginia and a senior faculty fellow at the Miller Center for Public Affairs. Her multiple-award-winning first book,

[48] Ibid.

[49] Ibid.

[50] Trefor Moss, "Tesla to Store China Data Locally in New Data Center," *The Wall Street Journal*, May 23, 2021, 2021, https://www.wsj.com/articles/tesla-to-store-china-data-locally-in-new-data-center-11622015001.

[51] Reuters Staff, "Tesla cars banned from China's military complexes on security concerns," *Reuters*, March 19, 2021 2021, Autos, https://www.reuters.com/article/us-tesla-china-idUSKBN2BB18R, www.reuters.com.

Hollywood Made in China (University of California Press, 2017) argues that Chinese investment and regulations have transformed the US commercial media industry. Forthcoming from Oxford University Press in 2022, her next book, *Trafficking Data: Networked Sovereignty in the Age of US-China Tech Competition*, examines the policy implications of consumer data transfer between the United States and China. She has testified in front of both chambers of Congress on US-China relations. Dr. Kokas is currently a Wilson China Fellow, an SSRC Abe Fellow, and a life member of the Council on Foreign Relations.

Photo credit: Blogtrepreneur, CC BY 2.0 <https://creativecommons.org/licenses/by/2.0>, via Wikimedia Commons