UNIVERSITY OF JOHANNESBURG

CENTRE FOR AFRICA-CHINA STUDIES

Policy Brief

1

China's Digital Security Law: Prospects and Recommendations

Edmund Terem Ugar and
Emmanuel Matambo

September 2022

POLICY BRIEF 1

Centre for Africa-China Studies
University of Johannesburg

Policy Brief No 1

China's Digital Security Law: Prospects and Recommendations

Edmund Terem Ugar and Emmanuel Matambo

Published in September 2022 by:
The Centre for Africa-China Studies (CACS)
at the University of Johannesburg
9 Molesey Avenue
Auckland Park
Johannesburg
South Africa
www.cacs.org.za

For enquiries, contact:
Dr. Emmanuel Matambo
– Research Director, CACS
Tel: +27 11 559 7675
Email: ematambo@uj.ac.za

POLICY BRIEF 1

China's Digital Security Law: Prospects and Recommendations

Edmund Terem Ugar and Emmanuel Matambo

1. Introduction and Background

In June 2021, China passed the new Data Security Law (DSL) two months after the release of the second draft of the law. The DSL was effective on September 1, 2021 (Sheng, Xu, and Tao, 2021; Haldane, 2021). The DSL is one of three fundamental data laws and policies of the Chinese government to maintain its data sovereignty. The other two are the Cybersecurity Law and the Personal Information Protection Law. Hitherto, China's data policies were porous, so the data extraction, usage, and marketing regulations were not strong enough to protect the data subjects. Currently, China's population of over 1.4 billion people has a significant data market for its digital economy and technological research and development. With the importance of data in terms of political and social stabilities, the necessity of the new DSL is that Chinese citizens now have a robust law that they can rely on whenever there is a threat to data theft or illegal extraction, usage, and marketing of data by local or international organisations and corporations.

With the emergence of the DSL, the Cybersecurity Law and the Personal Information Protection Law, China has gained data sovereignty. This implies that businesses operating within China must familiarise themselves with the new policies and measures of processing and using the data of Chinese citizens. Thus, the Chinese government can now control data security at home with the same logic used by data sovereign states in America and Europe against companies that belong to Chinese entrepreneurs. The DSL takes a top-down approach because the law allows government departments and provinces to set their data classifications and protective measures. However, this paper makes further recommendations China should create Pan-Asian data regulation laws similar to the General Data Protection Regulation (GDPR) of the European Union to enable the country to situate itself as the biggest and most powerful data market structure in the world.

The first section of this paper outlines the meaning of data sovereignty. The second section discusses China's DSL. The third section engages with other avenues China can benefit tremendously in the data market. The fourth section makes recommendations and concludes the paper.

2. Data Sovereignty

The United Nations Conference on Trade and Development (UNCTAD) (2021) noted that data sovereignty had become important for many nation-states. 128 nation-states have legislation on data protection, while 20 countries have drafted their legislation and are waiting for implementation. Research conducted by Couture and Toupin (2019) showed that, before 2010, the frequency of the term data sovereignty was not common in academic and non-academic papers. On the one hand, prior to 2011, the term was non-existing in academic literature; between 2011-2014, the term appeared 14 times; between 2015-2018, the term appeared 89 times. On the other hand, in non-academic papers, the term appeared 23 times prior to 2011; between 2011-2015, it appeared 794 times; in 2015-2018, it appeared 2459 times (Couture and Toupin, 2019).

Furthermore, in a study by Hummels and friends (2021), the term data sovereignty had the highest appearances of the total terms such as digital sovereignty, internet sovereignty, data sovereignty, and cyber sovereignty in the 341 academic publications surveyed. This indicates that nation-states are actively participating in ensuring the data security of their states by enacting policies and regulations for data governance. However, what does data sovereignty mean?

Data sovereignty involves managing information in line with the rules and regulations of a state where the information is gained (Snipp, 2016). Its importance is necessitated by the ubiquity and proliferation of internet access and electronic devices. In addition, data has also become a source of economic and security importance in our current social epoch. Only 213 computers had access to the internet in 1981. At the beginning of the 21st century, the figure increased to 72.39 million computers that were connected to the internet in 2000. In 2014, the figure reached a billion (Comer, 2020:90). The dawn of high internet access implied that states needed to take precautionary measures due to the implication data has to the economy and security of a state (Mueller, 2018). One of the reasons for data sovereignty and a call for states to take responsibility for ensuring the security of personal information and non-personal information in their locale was that, hitherto, most states, if not all, had left the management of personal and non-personal information to the private sector (Barlow, 1996; Wu, 1997; Perrit, 1998). The ethical implication with private companies managing data was that the state lacked control of the information of its citizens. However, states are now scrambling for data control to enable and enhance security, political, and economic capabilities (Himbert, 2009). China is one of the countries that has implemented strong data laws.

3. China's Data Laws

China's Personal Information Protection Law (PIPL) defines data in broad terms as whatever information, be it recorded information, electronic document, or cyber information, which can or cannot identify a data subject as long as such information

relates to an "identified or identifiable natural person" (Sheng, Xu, and Tao, 2021). In line with the PIPL, the Chinese Data Security Law (DSL) further defines data activities as "data collection, storage, processing, use, provision, transaction, publication, and other activities" (Article 3). The law defines data security as the "ability to adopt necessary measures to ensure data is effectively protected and lawfully used and remains continually secure in the state." Data security, as defined here, entails that organisations and individuals within the Chinese territory cannot transfer information to any foreign department without the approval of the designated Chinese department – the National Data Security Work Coordination Mechanism (NDSWCM). The DSL does not only regulate data within the jurisdiction of China but beyond. Article 2, paragraph 2 states that individuals and organisations outside of China must ensure that they engage in data activities that do not harm the national security and public interest of Chinese citizens. Failure of individuals and organisations to oblige with the laws will result in economic and political implications, such as the payment of fines, condemnation, and sanctions that the organisation must choose from (Sheng, Xu, and Tao, 2021; Haldane, 2021)

The DSL categorises data into three forms: core data, important data, and general data. While the state's core data is clearly defined as data that relates to national security, national economy, the livelihood of people, and the public interest (Sheng, Xu, and Tao, 2021; Haldane, 2021), important data is not clearly defined. The DSL reserves the definition of important data and the steps to ensure the protection of important data to the discretion of organisations, government departments, and provinces under article 4.

4. Territorial and Extraterritorial Data Transfer

The DSL differentiates important data that it conceives as critical information infrastructure (CII) from those that are non-CII data. CII data are information infrastructures that are important to sectors such as information service, energy, transportation, finance, egovernment, public communications, water conservancy, or other information infrastructure that has an impact on the national security, national economy, and public interest (Sheng, Xu, and Tao, 2021). For CII data to be transferred outside the territory of China, the operators or actors in the data processing must comply with the rules that are clearly established in the Cybersecurity Law. The Cybersecurity Law articulates that CII data can only be transferred outside of the Chinese territory if and only if the data is necessary for business; if so, operators of the CII must collaborate closely with the Cyberspace Administration of China (CAC) and other government bodies that are charged with the responsibility of data protection. Regarding non-CII documents, the DSL allows the formulation of laws at the discretion of the CAC and other relevant bodies.

Furthermore, the DSL does not allow the transfer of data for legal proceedings stored in China to any legal enforcement authorities outside of China without the prior approval of the Chinese government. Failure to obtain government authorisation may lead to a fine of US$156,000. In cases where there are severe impacts on the data subject if data is illegally transferred, there are additional fines of US$1.56 million, revocation of business license and suspension. In addition, data collected from China must be used lawfully, must be used in line with the purpose in which the data was collected, and must not be stolen (Article 27-32).

5. Analysis of the DSL: Lessons from Germany and Europe

China's DSL is an important data protection law that can significantly impact neighbouring Asian countries if China can move for Pan-Asian data regulations. This is because data sovereignty is more robust when national and continental policies are in place. For instance, Germany, which passed its data laws in 2017, has robust data policies and regulations that allow the supervised processing of data by the government. At the same time, the country works in close relationship with other European Union (EU) countries to ensure a sustainable continental data policy. The reason for such partnership is because whatever happens within the EU affects all the countries of the EU regions. Given this, Germany and France established the Gaia-X, a Pan-European cloud network, to provide cloud services for EU enterprises. With the projects such as the Gaia-X, businesses within the EU region can use a Pan-European shared cloud to conduct their affairs within the EU environment. The Gaia-X project has grown from 2019 with 22 EU companies in Germany and France to more than 500 members in 2021 (Gaia-X, 2021). Given the significance of Gaia-X to the EU, this research moves to make recommendations for China and the establishment of a Pan-Asian data regulation body.

6. Recommendation for Pan-Asian Data Policy: Applying EU Gaia-X

China currently has one of the biggest digital economies and robust data laws. However, the DSL will be more robust if China, given its powers and leadership role within the Asian continent, calls for a Pan-Asian data protection law to ensure that the continent is protected in terms of data laws. For instance, China is currently developing one of the strongest facial recognition technologies in the world, and the country can benefit from data from other Asian countries. Furthermore, policies that bring Asian countries together can benefit the continent's economy and enable the continent to be a strong data production force. Given the enormous wealth and force China has, China should step in to create the Pan-Asian data regulations. In addition, creating such a relationship may stimulate other partnerships within the continent.

7. Conclusion

While China has a strong data protection policy to govern and manage the data processed in China, the Asian region does not have a robust data policy. However, such a lack may have some adverse effects. This is because the continent cannot unanimously mitigate any issues on data protection that stem from the continental level. As a result, this paper called for a bilateral relationship between China and other Asian countries to establish a Pan-Asian data policy. However, the paper contended that China should make a move given the size of its digital infrastructures.

Reference List

Barlow, J.P. 1996. A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation*. Available at https://www.eff.org/cyberspace-independence.

China National People's Congress. 2021. Personal Information Protection Law of the People's Republic of China. Available at http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

Couture, S. and Toupin, S. 2019. What does the notion of "sovereignty" mean when referring to the digital? *New Media and Society*, pp. 1-18.

DigiChina. 2021. Translation: Data Security Law of the People's Republic of China (Effective September 1, 2021). Stanford University. Available at https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.

Gaia-X Position Paper. 2021. Gaia-X: Driver of digital innovation in Europe. Available at: https://www.datainfrastructure.eu/GAIAX/Navigation/EN/Home/home.html#:~:text=More%20than%20500%20organisations%20from%20various%20countries%20are,our%20goals%20of%20data%20sovereignty%20and%20data%20availability.

Haldane, M. 2021. What China's new data laws are and their impacts on big tech. *South China Morning Post*. Available at: https://www.scmp.com/tech/policy/article/3147040/what-chinas-new-data-laws-are-and-their-impact-big-tech

Himbert, M.E. 2009. A brief history of measurement. *The European Physical Journal Special Topics* 172(1), pp. 25-35.

Hummel, P., Braun, M., Tretter, M. and Dabrock, P. 2021. Data sovereignty: A review. *Big Data and Society*, pp. 1-17.

Mueller, M.L. 2020. Against Sovereignty in Cyberspace. *International Studies Review*, 22(4), pp. 779–801, https://doi.org/10.1093/isr/viz044.

Perritt, H.H. 1998. The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance. *Indiana Journal of Global Legal Studies*, 5(2).

Sheng, J., Xu, C. & Tao, E. 2021. China adopts new data law. *Pillsbury*. Available at: https://www.pillsburylaw.com/en/news-and-insights/china-adopts-new-data-security-law.html

Snipp, C. 2016. What does data sovereignty imply: What does it look like? In Kukutai, T. and Taylor, J. (Eds). *Indigenous Data Sovereignty: Towards An Agenda*. Sydney: Australia National University Press.

Wu, T. 1997. Cyber Sovereignty? – The Internet and the International System. *Harvard Journal of Law and Technology*, 10(3), pp. 647-666.

United Nations Conference on Trade and Development (UNCTAD). 2021. *Cross-border data flows and development: For whom the data flow*. Digital Economy Report 2021. United Nations, Geneva. Available at https://unctad.org/webflyer/digital-economy-report-2021.