Academic internationalisation
outlook
| Issue 1 | May 2024 |

China's data protection laws and their implications for research collaborations

In recent years, China has introduced several laws on data management that all have had a considerable impact on research collaborations, and which can also impact research on China conducted outside the country without the direct involvement of Chinese partners. This regulatory framework has created concerns among the academic community on what can and cannot be done in research collaborations with institutions and individual researchers in China. Regulations and praxis based on the legislation are constantly developing and everyone involved in academic partnerships with China are strongly encouraged to investigate this topic more closely.

In March 2024, China in effect eased the regulation of outbound data flow when the Cyberspace Administration of China released new provisions on cross-border data flow. In the light of this, this Outlook provides an overview of China's data protection laws including the newly released provisions as well as a new set of standards that aims to classify different data types. This Outlook is a republication of a newsletter jointly published in November 2023 by STINT and the Office of Science and Innovation at the Embassy of Sweden in Beijing.[1] The original text has been translated to English and updated to include information about the new provisions.

[1] Nyhetsbrev Nr. 3 Kinas datasäkerhetslagar och deras implikationer för forskningssamarbeten, Office of Science and Innovation, Embassy of Sweden in Beijing and STINT, https://us14.campaign-archive.com/?u=44610bbe35909cacfaa664602&id=d45b9df658

STINT
Stiftelsen för Internationalisering av högre utbildning och forskning

The Swedish Foundation for International Cooperation in Research and Higher Education

ISSN: 1404-7209

With increased digitalisation, mass collection of personal data as well as the rapid development of business models based on such data, countries across the globe have developed legislation and regulations aimed to protect personal data. China is no exception, though these efforts started relatively late, and the management of personal data was a long time more or less unregulated. As a result, one feature of Chinese life is receiving advertising calls on one's mobile phone on an almost daily basis.

From c. 2012 China embarked on the establishment of a legal framework for data management in earnest. In 2017 China introduced its Cybersecurity Law (CSL, 网络安全法). CSL applies to the construction, operation, maintenance, and use of networks as well as the monitoring and administration of cyber security. CSL also introduced the concept of *important data* (重要数据) which, despite lacking a clear definition, clearly indicated that national security is the overriding focus for data security in China. On the whole, CSL was vaguely formulated and it was not entirely clear which authority was responsible for its implementation, which led both the Cyberspace Administration of China (CAC, 国家互联网信息办公室) and the Ministry of Public Security (MPS, 中华人民共和国公安部) to publish draft regulations based on CSL. However, neither of these draft regulations came into force, which meant that CSL has been relatively ineffectual in practice. CSL may nevertheless affect joint research projects involving Chinese partners, particularly in the areas of data management and transfer. It is therefore essential to determine what types of data will be processed within a partnership and where the data will be stored.

In 2018 steps were taken to draw up two new laws aimed at increasing data control. Both these laws, the Personal Information Protection Law (PIPL, 人信息保护法) and the Data Security Law (DSL, 数据安全法), entered into force in 2021. PIPL is similar to personal data legislation in other countries, *albeit* not in any way limiting data collection and surveillance by the state/party. It encompasses the processing of physical persons' personal data and is therefore particularly important when it comes to research and research collaborations involving the collection and processing of personal data. DSL, on the contrary, is a unique law

that not only covers personal data but all types of data.[2] While the focus of PIPL is on the processing of individuals' personal data, DSL focuses on national security. DSL may therefore have great impact on projects involving Chinese partners, particularly if such projects concern national core data, important data, and data in new technological areas.[3] In summary, DSL is applicable to a very broad area. The extraterritorial application of the law is also an important aspect to consider when processing data. If research activities are deemed liable to damage China's national security they may be sanctioned on the basis of this law. PIPL also has extraterritorial clauses.

In addition to CSL, PIPL and DSL, further laws have been enacted in recent years: Measures for the Management of Scientific Data (SDM, 科学数据管理办法) and the Export Control Law (ECL, 出口管制法). SDM applies to all organisations or individuals who, supported by public funding, participate in activities in China that deal with scientific data. The main aim of SDM is to exert control over publicly-funded research. To comply with SDM, scientific data must be classified to ascertain whether they fall under relevant regulations aimed at clarifying confidentiality levels and confidentiality periods as well as establishing a data management system. ECL applies to both cross-border and domestic data transfers, which of course may affect virtually all research collaborations.

Together, CSL, PIPL, DSL, SDM and ECL form an extensive body of legislation that clearly has considerable consequences for data management in China, as well as for how, if at all, data may be transferred to other countries. This of course is of great significance for scientific partnerships with Chinese researchers or institutions. PIPL for instance stipulates that if data export is allowed, permission must be obtained before such export may take place.

One consequence of the new legislation is that the China National Knowledge Infrastructure (CNKI, 中国知网), the country's largest academic database, no longer can be accessed outside China, with potentially devastating effects on social sci-

[2] With the exception of state secrets.
[3] The exact definitions of these concepts are not necessarily clear and/or are changeable.

ence research on China. The German Research Foundation (DFG, Deutsche Forschungsgemeinschaft) holds that the potential impact of China's data security legislation on research collaboration is so severe that all co-funding of German – Chinese research projects was temporarily frozen in 2023 pending the outcome of a joint project with the National Natural Science Foundation of China (NSFC, 国家自然科学基金委员会) in which legal experts from Germany and China examines what is and is not possible under the combination of China's data security legislation and the EU's General Data Protection Regulation (GDPR).

It is in other words of great importance for Swedish research funders, higher education institutions, and individual researchers who collaborate (or plan on collaborating) with actors in China to obtain a basic understanding of the Chinese data protection legislation and to monitor its implementation. Like CSL, both PIPL and DSL are primarily foundational legal frameworks with little detail, and Chinese authorities are gradually creating more detailed complementary regulations. The combination of the lack of clarity in some of the legal formulations (e.g. what constitutes *important data*, introduced in CSL, has long remained unclarified) and what at times appears to be arbitrary implementation has led to considerable concerns in the international business sector based in China.

In a related development, China expanded its Counter-Espionage Law (CEL, 反间谍法) during the spring of 2023. It now includes a prohibition against all transfer of data related to national security and expands the definition of espionage. The law means that documents, data, and other material related to national security and interests must be protected in parity with state secrets. However, it is problematic that *national interests* are not defined, thereby creating risk and uncertainty for foreign companies, journalists, and researchers based in China. At the end of October 2023, a draft revision of the Law on Guarding State Secrets (保守国家秘密) was published, which compounded foreign companies' and researchers' concerns about risks connected to operating in China.[4]

[4] China to tighten its state secrets law in biggest revision in a decade/South China Morning Post. https://www.scmp.com/news/china/politics/article/3239340/china-tighten-its-state-secrets-law-biggest-revision-decade?module=lead_hero_story&pgtype=homepage

Regulatory Updates Published in March 2024

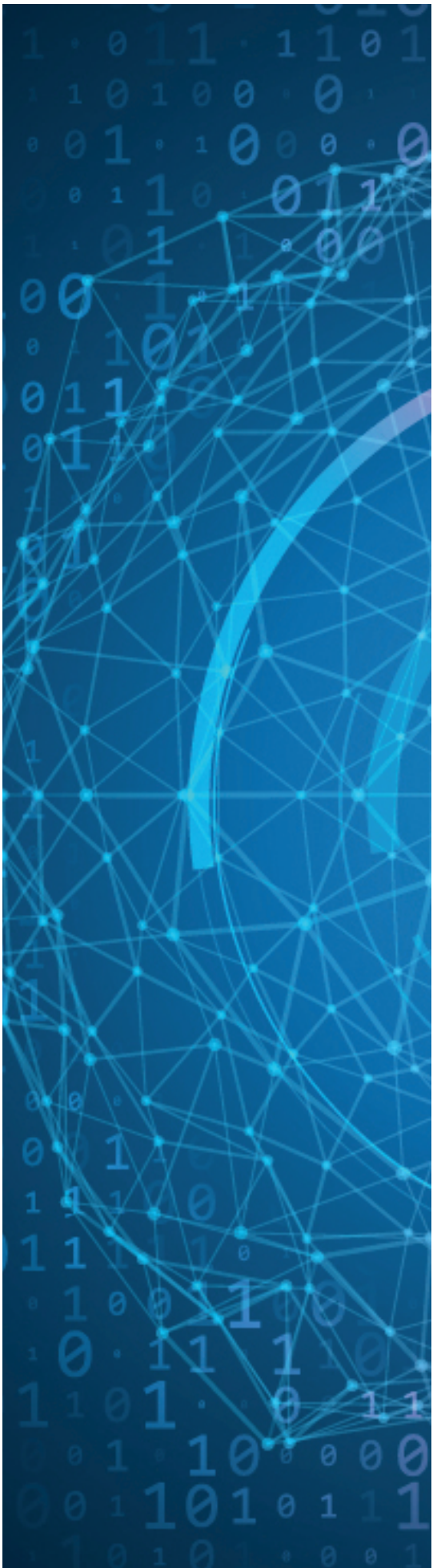
In March 2024, the CAC published Provisions on Promoting and Regulating Cross-Border Data Flows (促进和规范数据跨境流动规定), which amounts to a significant easing of the regulations of outbound data. While the provisions do not change the regulatory mechanism per se, they do in effect raise the thresholds of when security assessments for outbound data are required. The provisions include clarifications and exemptions as well as a reduced scope of the regulatory mechanism. A key provision is that data that have not specifically been labelled as important data by relevant authorities need not to be treated as such, which provides needed clarification on the issue of what constitutes important data. Most importantly for the science community is Article 3 of the provisions that states that outbound transfer of data collected and generated as part of academic collaboration is exempt from security assessments, provided no personal information or important data are transferred.

Furthermore, the State Administration of Market Regulation (SAMR) and the Standardization Administration of China (SAC) also released a new set of technical standards for data classification in March 2024, namely Data Security Technology – Rules for Data Classification and Grading (数据安全技术 数据分类分))? set5o be implemented on October 1, 2024. The purpose of the standards is to provide clarification for both authorities and data processors on how to identify different types of data. Definitions are included on what constitutes *important data, core data, general data, personal information, sensitive personal information*, and more.

In Conclusion

As should be evident from the above, it is of utmost importance for everyone involved in academic collaborations with China to investigate this topic in more depth and follow developments closely. Stay informed and ensure that your Chinese partners comply with existing regulations.

The content of this Outlook does not constitute legal advice but should be interpreted as highlighting an area of great importance in terms of academic cooperation with China.



STINT
Stiftelsen för Internationalisering av högre utbildning och forskning

The Swedish Foundation for International Cooperation in Research and Higher Education

Further reading

European Union. (2021). China's specific regulatory framework on data and how it impacts EU-China R&I collaboration, https://www.businessfinland.fi/4a9a71/globalassets/finnish-customers/news/calls/2021/china_s_specific_regulatory_framework_on_data_1634509396.pdf

R. Creemers, China's emerging data protection framework, Journal of Cybersecurity, vol 8(1), 2057-285 (2022), https://doi.org/10.1093/cybsec/tyac011

D. Lewis, China's souped-up data privacy laws deter researchers, Nature (2023), https://doi.org/10.1038/d41586-023-01638-1

Global Law Office. (2024). China Eases Regulation of Outbound Data Flow Fact Sheet on the Provisions to Promote and Regulate Cross-Border Data Flow, https://www.lexology.com/library/detail.aspx?g=8b3672c8-6d7f-477d-9806-c96d5e30234f

A. Huld, China Releases Technical Standards Guiding the Classification of "Important" Data, China Briefing (2024), https://www.china-briefing.com/news/china-data-classification-standards-important-data/

STINT Academic internationalisation outlook presents short thematic articles on current issues relevant to academic internationalisation.

To subscribe to the newsletter on science and innovation in China, published by STINT and the Office of Science and Innovation at the Embassy of Sweden in Beijing, please sign up, https://us14.list-manage.com/subscribe?u=44610bbe35909cacfaa664602&id=f80b23eb97

Laws, Provisions, and Standards

Cybersecurity Law
– 中华人民共和国网络安全法
– Came into force: 2017-06-01
– Translation: Cybersecurity Law of the People's Republic of China (CSL)/Stanford Cyber Policy Center, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

Measures for the Management of Scientific Data
– 科学数据管理办法的通知
– Came into force: 2018-03-17
– Translation: Measures for the Management of Scientific Data (SDM)/Center for Security and Emerging Technology, https://cset.georgetown.edu/publication/china-scientific-data-management-measures/

Export Control Law
– 中华人民共和国出口管制法
– Came into force: 2020-12-01
– Translation: Export Control Law of the People's Republic of China (ECL)/China Law Translate, https://www.chinalawtranslate.com/export-control/

STINT
Stiftelsen för Internationalisering av högre utbildning och forskning

The Swedish Foundation for International Cooperation in Research and Higher Education

About the author:
Dr Erik Forsberg has been STINT's Representative in APAC since 2018. He has worked over 15 years in China, predominantly in the university sector, and remains an Adjunct Associate Professor at Zhejiang University. He is also the co-founder of several companies in China. Dr Forsberg has been a visiting scientist at Hokkaido University in Japan and was also the Founding Graduate Dean at the Higher Colleges of Technology (HCT) in the United Arab Emirates.

STINT, The Swedish Foundation for International Cooperation in Research and Higher Education, was set up by the Swedish Government in 1994 with the mission to internationalise Swedish higher education and research.

STINT promotes knowledge and competence development within internationalisation and invests in internationalisation projects proposed by researchers, educators and leaderships at Swedish universities.

Address: STINT, Wallingatan 2, SE-111 60 Stockholm, Sweden

Telephone: +46 8 671 19 90

info@stint.se www.stint.se

Data Security Law
– 中华人民共和国数据安全法
– Came into force: 2021-09-01
– Translation: Data Security Law of the People's Republic of China (DSL)/Stanford Cyber Policy Center, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

Personal Information Protection Law
– 中华人民共和国个人信息保护法
– Came into force: 2021-11-01
– Translation: Personal Information Protection Law of the People's Republic of China (PIPL)/Stanford Cyber Policy Center, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

Counter-Espionage Law (updated)
– 中华人民共和国反间谍法
– Came into force: 2023-07-01
– Translation: *Counter-espionage Law of the Peoples Republic of China (CEL) 2023 ed.*/China Law Translate, https://www.chinalawtranslate.com/en/counter-espionage-law-2023/

Provisions to Promote and Regulate Cross-Border Data Flow
– 促进和规范数据跨境流动规定
– Came into force: 2024-03-22
– Translation: Provisions on Regulating and Promoting Cross-border Data Flows /China Law Translate, https://www.chinalawtranslate.com/en/draft-data-export-rule-revisions/

Data security technology–Rules for data classification and grading
– 数据安全技术 数据分类分级规则
– To come in force: 2024-10-01
– Untranslated text: 数据安全技术 数据分类分级规则, www.tc260.org.cn/upload/2024-03-21/1711023239820042113.pdf