



中倫律師事務所  
ZHONG LUN LAW FIRM

北京市朝阳区金和东路20号院正大中心3号楼南塔22-31层，邮编：100020  
22-31/F, South Tower of CP Center, 20 Jin He East Avenue, Chaoyang District, Beijing 100020, P. R. China  
电话/Tel: +86 10 5957 2288 传真/Fax: +86 10 6568 1022/1838  
网址: www.zhonglun.com

## **Pitfalls for Multinationals in Doing Research Activities in China**

China has recently heightened its regulatory enforcement against research and information collection activities within the country. As part of this initiative,

- Chinese security authorities investigated into a number of entities and individuals in the past couple of months, including detaining a Japanese executive from Astellas Pharma Inc. for suspected “espionage” behaviors and raiding at least two consulting firms (Bain and Capvision) in Shanghai and Suzhou respectively for suspected obtaining sensitive information concerning state secret and defense intelligence.
- On April 26, 2023, China announced its latest amendment to the *Counterespionage Law of the People's Republic of China* (“**Counterespionage Law**”), which will become operative as from July 1, 2023. This follows China’s promulgation/revision of a set of laws and regulations governing data export control.

The above signal Chinese policymaker’s increasingly prioritized agenda on national security issues. Accordingly, multinational companies are recommended to assess its regulatory compliance exposure when conducting research or information collection activities in China to mitigate potential risks. We set forth below some frequently asked questions and quick answers for your reference.

### **1. What is the key legal framework?**

The China-related research and information collection activities primarily concern the regulation of three pillars of Chinese laws: the Counterespionage Law, the *Statistical Law of the People's Republic of China* (“**Statistical Law**”) and the *Data Security Law of the People's Republic of China* (“**Data Security Law**”). In addition, there could be several other laws and regulations concerned depending on the specific behaviors in question.

### **2. What entity can become a subject?**

Regardless of the nationality/domicile of an entity and whether it links to an espionage organization, to the extent it conducts research and information collection activities in Chinese mainland and/or transfers collected/produced information outside Chinese mainland, it could be subject to the abovementioned laws. While they generally do not apply to Hong Kong, in exceptional circumstances where the relevant research activities constitute crime of “stealing, spying, buying, or illegally providing state secrets or intelligence involving national security for foreign or overseas organizations, institutions, or individuals”, they could also be subject to the jurisdiction of both China’s Criminal Law and Hong Kong’s *Law of Safeguarding National Security*.

### **3. What are the key points of the applicable laws**

- *The Counterespionage Law* is primarily designed to regulate (i) espionage activities,

(ii) illegal acquisition of state secrets and their carriers, and (iii) the illegal use of specialized espionage equipment. Also, the 2023 newly amended Counterespionage Law: (i) expands the scope of application, broadens the definition of “espionage behavior”, and adds provisions for cyber-espionage, (ii) provides greater support for counterespionage work and proposes to establish a national coordination mechanism, and (iii) increases the authority and protection for national security agencies, and specifies the investigation and powers of national security agencies.

We wish to note that the law does not only capture the activities relating to or carried out by espionage organizations but also considers anyone involved in the illegal acquisition or possession of state secrets, intelligence, and other national security concerned information in violation of the law, even if they have no links to espionage organizations. Based on our observations, engaging in activities involving illegally collection and cross-border transfer of information on China's cutting-edge technologies, defense information, and critical industry information, will likely be deemed as a violation under the applicable law.

- *The Statistics Law*, along with its implementing rules, set forth compliance obligations for “foreign-related surveys” in China. Foreign entity(ies) who wish(es) to conduct statistical surveys in China must commission qualified agencies in China to do so. Additionally, private statistical survey agencies may not disclose private statistical survey data that duplicates state-important macroeconomic and social indicators of China. Furthermore, relevant regulations also stipulate a number of prohibited activities that may adversely impact China's national interests.
- *The Data Security Law* and certain other regulations provide the relevant regulatory requirement on the cross-border data transfer activities. The transfer of different types of data entails different compliance obligations. For instance, “important data” and personal information can be exported, but relevant parties should take proper measures and/or conduct specific compliance procedures to ensure data security; furthermore, for personal information, the legitimate rights and interests of the data subject must be protected. In addition, certain industries (e.g. life science sector) have localization storage requirements or specific regulatory requirements for data export.

#### **4. What are the typical problematic behaviors?**

- Engaging in activities related to espionage organizations and their agents that endanger national security, illegally acquiring Chinese state secrets, intelligence, or other information.
- Illegally obtaining state secrets, intelligence, as well as other national security concerned information and providing them to overseas parties, absent any connection to espionage organizations and their agents.
- Illegally producing, selling, possessing, and using special espionage equipment required for espionage activities.
- Conducting statistical and survey activities in China without commissioning qualified enterprises and obtaining approval from the competent authorities.
- Disclosing privately conducted survey and statistical data that duplicates or contradicts important macroeconomic and social indicators specified by the state or disclosing

information that does not meet regulatory requirements.

- Collecting, processing, and transmitting personal information to overseas parties without consent.
- Failing to follow legal procedures when transferring important data, personal information more than a certain amount, and specific industry data outside of China.

**5. What are the possible legal consequences?**

- Civil and administrative penalties. Civil and administrative penalties such as warnings, fines (incl. sanctions up to one to ten times the illegal gains), and administrative detention, will be imposed on those who violate the applicable laws.
- Criminal charges. In addition, if any of the misconducts are found to have violated China's Criminal Law, the individuals and organizations involved may face criminal charges (with sentences up to life imprisonment).

**6. Any practical recommendations?**

For compliance purpose, we recommend multinationals take various measures to mitigate potential risk exposures. For example,

- From the perspective of information collection, they should be cautious about the information in question and settings, especially if it concerns China's cutting-edge technologies, defense, or critical industry information. They should avoid using illegal tools or methods, and refrain from accessing state secrets. Also, when collaborating with third-party institutions to collect information, compliance reviews should be conducted to identify any organizations suspected of espionage or their agents.
- From the perspective of information processing and transfer to any third party, they should obtain consent from relevant personal information subjects in advance when processing or transferring his/her personal information. In case of transmitting information outside of China, not only personal information but also specified categories of non-personal information data such as important data or specific industry data, must follow proper protocol in advance for compliance with the applicable laws and regulations.

\*\*\*

If you have any questions, please feel free to contact us.

<b>Frank JIANG</b> Email: <a href="mailto:jianghuikuang@zhonglun.com">jianghuikuang@zhonglun.com</a> Direct Line: (8610) 5957-2131	<b>Jason JIA</b> Email: <a href="mailto:jiashen@zhonglun.com">jiashen@zhonglun.com</a> Direct Line: (8610) 5957-2263
<b>Rachel LI</b> Email: <a href="mailto:lirui@zhonglun.com">lirui@zhonglun.com</a> Direct Line: (8610) 5957-2143	<b>Scott YU</b> Email: <a href="mailto:scottyu@zhonglun.com">scottyu@zhonglun.com</a> Direct Line: (8610) 5957-2078