瑞士文斐律师事务所
WENFEI ATTORNEYS-AT-LAW LTD.

# CHINA LEGAL REPORT*

## JUNE 2017

* CHINA LEGAL Report is a monthly collection of Chinese law related news gathered from various media and news services, edited by WENFEI ATTORNEYS-AT-LAW LTD. distributed to its clients and CHINA LEGAL Report subscribers.

WENFEI ATTORNEYS-AT-LAW LTD. does not accept responsibility for accuracy of quotes or truthfulness of content. CHINA LEGAL Report is not intended to provide advice.

# Cyber Security Law

## I. Introduction

China's network security suffers great challenges, especially in critical information infrastructure areas, such as public communication and information service, energy, communications, water conservation, finance, public services and e-government affairs.

Since these critical information infrastructures have become key object of cyber-attack, China's national security and public interests suffer serious threats in respect of state and public security by using networks. In addition, China always had the ambition to control information and the internet.

On 1 June 2017, the Cyber Security Law of the PRC ("the Law") has come into force. The new law shall address such issues. The law focuses on 4 topics and provides specific features to regulate these topics: (1.) The concept of sovereign cyberspace, (2.) the protection of personal information, (3.) key information infrastructure, (4.) the cross-border transmission of the data for key information infrastructure.

As the Law provides different features, it shall also apply to different types of addresses, as set out here.

## II. The Scope of Application of the Law

The Addressees of the Law

The Cyber Security Law applies to three sorts of addressees.

(a) Critical Information Infrastructure Operators (CIIO)

CIIO refers to organizations that are operating networks used for critical public services such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs that would cause serious danger to state security and public interest if damaged.

(b) Network Operators

Network refers to systems that are composed of computers or other information terminals and relevant equipment to collect, store, transmit, exchange, and process information. Network operator shall include any person conducting business in China who owns, manages or offers service through network, website or other electronic platforms in which information collected from third party users in China is stored, transmitted, exchanged or processed applies to the law.

(c) Providers of Network Products and Services (PNPS)

The Law does not provide a proper definition. According to the Regulations on the Protection of Right of Dissemination via Information Network of the P.R.C, PNPS include organizations that provide search, link or access service, or offer storage space service for information.

The Features of the Law

(a) The concept of sovereign cyberspace

The concept of sovereign cyberspace is provided by an extension and expression of the State's sovereignty to the cyberspace. The Law provides that the State shall be entitled to exercise Chinese jurisdiction power on any information facility in the territories of the People's Republic of China, as well as on any activities related with such facilities. The State shall also be entitled to protect these information facilities and the data/information from being attacked or destroyed. Last but not least, the State shall be entitled to stop *illegal information* to be spread through domestic information facilities/cyberspace.

(b) The protection of personal information

The protection of personal information is regulated in different laws. The Law provides a chapter "Network Information Security" with the purpose of providing protection to personal information and preventing network crime. E.g. individuals and organizations shall not set up the websites or "social media groups" for the purpose of conducting fraud (inclusive of trademark piracy), smuggling or production and distribution of regulated/controlled goods, as well as they shall not use such networks to conduct such activities.

Network Operators shall collect and use the personal information in a legal, due and necessary way. If a person notices that Network Operators are violating the laws to collect or use the personal information, that person shall be entitled to demand the deletion or correction of the personal information.

No network operator may provide relevant services to any users that fail to provide authentic identity information.

(c) Key information infrastructure and CIIO

CIIO shall Implement standards and procedures to ensure data security such as formulating internal security management system and operating procedures, adopting the technical measures for preventing computer virus and activities endangering network security, as well as for monitoring and recording network operation status and the network security incidents. The relevant network logs shall be kept for at least 6 months.

CIIO shall establish internal security management systems and operating rules such as setting up special security management departments and security management responsible persons, conducting background check of persons at key positions, conducting network security education, and technical training on a regular basis, carrying out disaster recovery backup of important systems and database, formulating emergency response plans for network security incidents and conducting drilling on a regular basis. CIIO shall further establish a mechanism for reporting violations to the relevant authorities.

CIIO shall conduct the testing and evaluation of the security and potential risks of its networks by themselves or by commissioning a network security service institution at least once per year and submit the testing and evaluation report and the measures for improvement to the departments responsible for security protection of critical information infrastructures.

(d) The cross-border transmission of the data for key information infrastructure

According to the Law, personal information and important business data collected and generated in the operation within the territory of China shall be stored within the territory of China. Where it is necessary to provide such information and data abroad due to business needs, a CIIO or Network Operator must obtain the consent of the National Cyberspace Administration and State Council, upon a security assessment.

Sanctions

The Law sets up a regime of fines for breach of its provisions. These fines range from RMB 10'000 to RMB 500'000 for Network Operators, from RMB 10'000 to RMB 1'000'000 for CIIO and PNPO, from RMB 10'000 to RMB 100'000 for individuals "directly responsible" for an infringement of the Law.

If Network Operator, CIIO or PNPO refuse to make correction or in serious circumstances, relevant competent authority may order to suspend relevant business activities, suspend business activities for rectification or close the website or revoke their relevant business permit or business license.

## III. Conclusion

In order to enhance the protection of personal data, confirm the concept of cyberspace sovereignty, secure national security and public interests, the Cyber Security Law requires Network Operators to establish user information protection systems and impose Network Security Protection Obligations on CIIO and establishes rules of cross-border transmission of critical infrastructure information to protect the national sovereignty and security.

However, some wording still needs to be specified, for example, the definition of the Providers of Network Products and Service.

The Law will cause additional difficulties and restrictions in doing business in China, since the Law will increase compliance costs and operational difficulties. For example, Network Operators are obliged to require users to provide true identity information when signing service agreements.

For any organization who has an online presence in China, owns or operates any computer systems in China, or intends to launch network products and services in China, it is important to keep up with the development of the new law and prudent to start reviewing strategies and policies preparing written policies for implementation of the relevant procedures in accordance with the law.

However, a prosperous increase in the cyber security industry is also expected in China.

*****

We may be reached under the following addresses:


**Zurich**
Wenfei Attorneys-at-Law Ltd.
Mainaustrasse 19
CH-8008 Zurich, Switzerland
T +41 43 210 8686
F +41 43 210 8688

**苏黎世**
瑞士文斐律师事务所
Mainaustrasse 19 号
CH-8008 瑞士文斐律师事务所
电话：+41 43 210 86 86
传真：+41 43 210 86 88

**Beijing**
Wenfei Attorneys-at-Law Ltd.
Room A1506, Nanxincang Business Plaza,
A No.22 Dongsishitiao,
Dongcheng District,
Beijing 100007 P.R.C.
T +86 10 5169 0263
F +86 10 5169 0965

**北京**
瑞士文斐律师事务所北京代表处
北京市东城区东四十条甲 22 号
南新仓商务大厦 A 座 1506 室
邮编 100007
电话：+86 10 6468 7331
传真：+86 10 6460 3132

**Shanghai Cooperation**
Wenfei Business Consulting
Office 18D, Shanghai Industrial
Investment Building,
No.18, Cao Xi Bei Road,
Shanghai 200030 P.R.C.
T +86 21 6427 6258
F +86 21 6427 6259

**上海合作单位**
文斐商务咨询
中国上海市徐汇区漕溪北路 18 号
上海实业大厦 18D
邮编 200030
电话：+86 21 6427 6258
传真：+86 21 6427 6259




Check the China Legal Report archives on: http://www.wenfei.com/index.php?id=21
Obtain your personal subscription from: china@wenfei.com