1 | 2018
19th Year
15 February 2018
P. 1–32

CRi

Computer Law Review International

A Journal of Information Law and Technology

cr-international.com

ottoschmidt

CRi
Computer Law Review International
A Journal of Information Law and Technology

Articles

Daniel Albrecht

Chinese Cybersecurity Law Compared to EU-NIS-Directive and German IT-Security Act

When cybersecurity not only protects interests of the masses but ultimately also safeguards national sovereignty

In order to effectively address the challenges of attacks on IT systems, cybersecurity measures have been intensified internationally in the latest years. Germany, the EU and China have launched significant legislative initiatives in the last two years. However, the approach and the coverage of the regulations differ considerably in some areas. After briefly looking at the IT Security Act in Germany (I.) and the Directive of Security and Network and Information Systems in the European Union (II.), the article explains key provisions of the Chinese Cybersecurity Act as well as its systematic approach and its effects on businesses (III.).

I. Germany: IT Security Act

The German IT security law intends primarily to effectively deal with attacks on the critical infrastructures. According to this law, which entered in force mid 2015, critical infrastructures can be companies and institutions, both private and public, in different industries, such as in banking, in water and energy supply and also in media section.[1] They fall under the compulsory registration. These companies and institutions must periodically verify their specially secured relevant systems and processes by certificates. They must also categorize and report any external attacks. To be specific for example, the operators of the telemedia industry are required by law to implement the suitable state-of-the-art IT security basics. Furthermore, the technology institutions must be safeguarded against violations of personal data protection, e.g. by implementing encryption methods recognized as secure. Anyone who breaches of these duties, risks a fine.

The Federal Office for Information Security[2] is the authoritative institution of the entire procedure and the central registration office for IT attacks.

II. Directive on Security of Network and Information Systems

The EU NIS-Directive introduces measures to ensure a high common level of security of network and information systems in the Union and follows a similar approach like the German IT Security Act. The EU NIS-Directive entered into force on 8 August 2016 and is to be transposed by all Member States into national law by May 2018. It traces back to a European Commission policy paper that had been adopted on 7 February 2013 in the framework of the EU cyber security strategy, and

1 Gesetz zur Umsetzung der NIS Richtlinie, Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html.

2 Federal Office for Information Security ("Bundesamt für Sicherheit in der Informationstechnik, BSI"): https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html.

should help to improve the resilience of IT systems, to fight cybercrimes and to strengthen the EU cyber defense.[3]

All EU Member States are required to set up registration offices for national "Network and Information Security" (NIS). For this purpose, a close cooperation between the Computer Security Incident Response Teams (CSIRTs), the national security authorities and the European coordination center must be ensured. Security requirements and reporting obligations for the operators of essential services are regulated. "Essential services" correspond in this respect to the critical infrastructures within the meaning of the NIS-Directive and Council Directives on the Identdification for European Critical Infrastructures.[4] Besides essential services, the NIS-Directive also regulates digital services. The providers of "digital services" are first and foremost search engines, cloud computing services and online marketplaces. These providers are responsible for preventing risks with technical and organizational preventive measures, enforcement of network and information systems security measures, and plans for security and reaction, to be able to react on acute attacks in emergencies.

Cybersecurity in the EU is also influenced by the new EU General Data Protection Regulation which demands data safety with regard to dealing with sensitive personal data.[5][Public authorities and companies must take appropriate technical and organizational measures to ensure and provide evidence that they are processing personal data in accordance with the new EU regulations.

III. Cybersecurity Law in China

The 24th session of China's Standing Committee of the 12th National People's Congress enacted the Cybersecurity Law **(CSLaw)** on 7 November 2016, effective on 1 June 2017.[6] The aim of the CSL is to protect China's national interests in a broad sense by giving the government visibility and control over data collected in China and improving the safety and security of data generally.

1. Background

Measures on how to handle personally identifiable information (PII) and critical infrastructure data, along with China's National Security Law of 2015, are part of a growing body of regulations expressing China's continued resolve to "maintain sovereignty" in this area.

In the past, China's data industry was loosely controlled compared to the comprehensive legal codes in place for cybersecurity and data management in Europe and North America. In recent years, China has focused its efforts on controlling access to the internet within its borders with its Great Firewall, and beginning in July 2015 has introduced a series of laws and draft laws on internet controls and state access to private data. Legislation regulating data management in the insurance sector was already passed in mid-2016.[7]

2. Key Provisions

The key provisions in the CSLaw apply to owners of network facilities, network operators and service providers. These terms are not defined but these and similar terms are common in Chinese internet regulations and are intended to be given a wide interpretation. At its broadest, any company using the internet to provide a service could be captured, and several cases indicate that this is the intended meaning.[8]

Unfortunately, the CSLaw is full of subjective terms such as important data, while the two most important terms in the law, "network operator" and "critical information infrastructure" lack a clear definition.

The term "critical information infrastructure" (CII) is crucial because the most stringent security obligations fall on CII operators. The CSLaw states that CII includes traditionally sensitive sectors such as public telecommunications and information services, energy, transportation, irrigation, finance, public services, e-government, but also includes the catch-all phrase "as well as other areas that may harm national security, the economy, and the public interest"[9], Article 31 CSLaw. Furthermore, the CSLaw also encourages voluntarily participation by network operators which are not a CII, Article 31 CSLaw The measures required from a CII are not insignificant[10]:

– establishing security management procedures,

– national security-approved equipment, mandatory audit logs and

– disaster recovery backups;

– making the calculations of determining preparatory costs

Furthermore, what constitutes "critical information infrastructure operators/areas" and "other important data" are also key definitions yet to be articulated.[11]

3. Network Operators

Network operators are defined in Article 76 CSLaw as network owners, managers and providers. In addition to traditional telecommunication operators and internet firms, network operators may also include financial institutions that collect citizens' personal information and provide online services, such as banking institutions, insurance companies, security companies

3 Heise Online, Verordnete Sicherheit, Neue gesetzliche Anforderungen an den Schutz kritischer Infrastrukturen, Joerg Heidrich, 19.08.2016.

4 Art. 2, COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, L 345/75, 23.12.2008.

5 European Union (EU)] 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [general data protection regulation (GDPR) Article 4(1) of the GDPR.

6 See the translation into English provided by the US Chamber of Commerce, Beijing at: https://cdsglobalcloud.com/wp-content/uploads/2017/02/AmCham-Cybersecurity-Translation.pdf?x71640.

7 The diplomat: China's Cybersecurity Law: What You Need to Know, Jack Wagner, June 1 2017.

8 China's New Cybersecurity Law, What International Companies should now, Richard Bird, Freshfields, Hong Kong.

9 China's Cybersecurity Law: An Expression of China's Cyber-Sovereignty Ambitions, APCO Worldwide's Investments, Bruce Fu, EuroBiz Feb. 14, 2017.

10 Art. 34 CSLaw.

11 Internet Governance Project, Georgia Tech, *Milton Mueller*, China's Cyber Security law: The Impact of digital trade; August 7th, 2017.

and foundations; providers of cybersecurity products and services; enterprises that have websites and provide network services.

According to Article 10 CSLaw, technical and other necessary measures should be taken to:

– safeguard network operations,

– effectively respond to cybersecurity incidents and

– prevent cybercrime.

These measures should also maintain the integrity, confidentiality and accessibility of network data, in accordance with the CSLaw's provisions and national standards.

The CSLaw requires network operators to cooperate with Chinese crime and security investigators which enjoy full access to data and offer unspecified technical support to the authorities upon request. No further details are provided. The CSLaw also imposes mandatory testing and certification of computer equipment for critical sector network operators (Article 21 CSLaw). The Cyberspace Administration of China is known to have been working for several months on the development of technical standards, and is consulting with both domestic and international IT vendors.

Article 37 CSLaw requires network operators in critical sectors to store data gathered or produced in mainland China. The term "critical sectors" comprises businesses involved in communications, information services, energy, transport, water, financial services, public services and electronic government services.[12]

In addition, the CSLaw requires business information and data on Chinese citizens gathered within China to be kept on domestic servers and not to be transferred abroad without permission.

4. Information Infrastructures

Based on the current definitions by the Office of the Central Leading Group for Cyberspace Affairs, CIIs can be distinguished into websites, platforms and production businesses. Other than influential organizations that affect the national economy and people's livelihood, the following criteria may bring most information infrastructures in the financial industry, in the Internet industry and in the consumer industry within the scope of CII:

– websites with more than one million daily average visits;

– infrastructures that can cause leakage of data of more than one million people in the event of a cybersecurity incident;

– infrastructures with more than 10 million registered users, or one million active users; and

– infrastructures with daily average transaction or trade amounts of more than 10 million RMB.[13]

If a network operator is responsible for a CII, then additional rules apply. No clear definition of CII is found in the CSLaw and the catch-all language leaves plenty of room for interpretation. However, there is a Network Security Check Practice Guide, created by the Cyberspace Administration of China (CAC) before the CSLaw came into force, that may give some guidance in determining CIIs. CIIs also include networks that may endanger state security, the economy, public welfare and the public interest if they were destroyed, disabled or subject to data breaches. CII operators must carry out an assessment of their cybersecurity facilities at least once a year and report potential risks and proposed remediation measures to the authorities.

CII operators purchasing network products and services that might impact national security are required to undergo a national security review organised by National Network Information Department and relevant department of the State Counsil (the Ministry of Industry and Information Technology (MIIT) and the Cyberspace Administration of China), Art. 35 CSLaw. It is not clear what such national security review will entail or how it is different from the requirement for safety inspection of other CIIs. Such policy will have significant impact especially on multi-national enterprises operating in China. Once the information systems are classified as CII, its data may not be transmitted cross-border arbitrarily.

5. Network Operations Security

The CSLaw introduces the following security regime for network operators: They are required to clarify responsibilities within their organisations, and ensure network security by implementing sound rules and regulations and operational processes. Network operators shall adopt various technologies to prevent, combat and investigate cyber-attacks in order to mitigate network risks. Network operators shall ensure data availability and confidentiality by backing up and encrypting data. Building an effective security administration system, finding rational technical solutions and improving data protection capabilities are expected to be key priorities for network operators.

China currently has two existing network security protection systems:

– One is the Computer Information Systems Security Tiered Protection,

– the other is Telecommunication Networks Security Tiered Protection.

The requirements established by these two tiered protection systems overlap regarding network security. Both protection systems distinguish between five levels of protection required of a computer information system or a telecommunication network, depending on the system's importance for national security, economic development, social life and potential damages to these aspects in the event of network interference.[14] Whether the tiered system established in the CSLaw will be similar to these two existing systems or a separate third system is not yet clear. But all these systems and related national standards will likely be helpful guidance to understand the concept of China's tiered protection system.

12 Overview of China's Cyber Security Law, IT Advisory KPMG China, February 2017.

13 National Cyberspace Security Strategy, China Copyright and Media, The law and policy of media in China, Rogier Creemers, Dec. 27, 2016.

14 China Law Blog, China's New Cybersecurity Law: The 101, Sara Xia, June 24, 2017.

6. Personal Information

Personal information is defined broadly under both the CSLaw and its implementing regulations. It can be anything that identifies a person: the person's full name, the person's date of birth, their telephone number, their address.

a) Storage

Article 37 CSLaw states that personal information and other important business data gathered or produced by CII operators during operations within the mainland territory of the People's Republic of China, shall be stored within mainland China. Where due to business requirements it is truly necessary to provide such data outside the mainland, they shall follow the measures jointly formulated by the State network information departments and the relevant departments of the State Council to conduct a security assessment.[15]

b) Processing

Article 41 CSLaw prohibits a network operator from disclosing personal information of living individuals to others, including overseas, without the consent of the person whose data may have been collected. The CAC has recently clarified that a person's implied consent may be assumed to their data being processed in a number of everyday operations, such as making an international phone call, sending an email, instant messaging or performing transactions online. The CSLaw does not clarify particular procedures for a security assessment, what the scope of the assessment will be and what conditions will need to be satisfied. It is also not clear whether approval will be required on a case-by-case basis or only when there is a change to a previously approved arrangement.

c) Impact

The impact on normal data storage and processing of foreign companies in China is therefore hard to assess at this stage. The inclusion of financial systems is again notable, albeit banks and insurance companies are already heavily constrained by sectoral regulations in their ability to outsource data heavy back-office operations outside of China.

7. Sanctions

The Cyberspace Administration of China (CAC) is the primary governmental authority supervising and enforcing the CSLaw.

Penalties for violating the CSLaw can vary according to the specific violation, but typically includes a warning, an order to correct the violation, confiscation of illegal proceeds and/or a fine (typically ranging up to RMB 1 million); personal fines for directly responsible individuals (typically ranging up to RMB 100,000); and in particularly serious circumstances, suspensions or shutdowns of offending websites and businesses, including revocations of operating permits and business licenses. The penalty for an unauthorised data export is a fine of up to RMB 500,000.

8. Concerns and Uncertainty

The CSLaw has raised concerns among some foreign companies over greater data controls as well as increased risks of intellectual property theft. Vague terminology and absent official guidance on complying with the CSLaw have created uncertainty, prompting many to call for the CSLaw to be delayed. At this point, the announcment of an 18-months phase-in period appears likely. The vagueness of the CSLaw provisions will lead most companies into a wait-and-see approach in compliance preparations.

Foreign companies could be asked to provide source code, encryption, or other crucial information for review by the authorities, which increases the risk of such information being lost, passed on to local competitors, or used by the authorities themselves.

To comply with data localization, foreign firms will have to either invest in new data servers in China which would be subject to government spot-checks, or incur new costs to hire a local server provider, such as Huawei, Tencent or Alibaba, which have spent billions in recent years establishing domestic data centers as part of Beijing's 12th Five-Year Plan (2011-2015). The substantial investment by these Chinese technology firms in recent years is one of the reasons why critics of the new law believe, it is partly designed to bolster the domestic Chinese data management and telecommunications industry against global competitors.

9. Effect on Non-Chinese Companies doing Business in China

Non-Chinese companies operating in China are more likely to transfer information and data outside of China. Many foreign players have existing internal policies for information technology and data management and privacy in China, linked to long-standing concerns around intellectual property security, which apply to both in-country operations and travel for international staff.

Multi-nationals are equipped to take on the cost of compliance, but a lot of the small and medium sized companies may not be able to afford to establish the control that the Chinese government is asking for. In December 2016, Airbnb announced that it had begun storing data for its Chinese users on servers in China. Other multinational giants, including Uber, Evernote, LinkedIn and Apple, have done the same.[16] International technology firms are especially concerned, however, as the law uses ambiguous verbiage that could create new barriers for trade.[17]

15 A new era for Cybersecurity in China, Deloitte, https://www2.deloitte.com/cn/en/pages/risk/articles/new-era-cybersecurity-law.html.

16 *Horwitz, Josh*, "A key question at the heart of China's new cybersecurity law: where should data live?" *Quartz*, June 7, 2017.

17 Internet Governance Project, Georgia Tech, *Milton Mueller*, China's Cyber Security law: The Impact of digital trade; August 7th, 2017.

10. Effect on Companies Outside of China with Chinese Business Partners

The CSLaw will affect how CIIs conduct business with partners overseas. Export of data outside of China will require regulatory approval and higher standards. This means that a Chinese business partner may be less willing to exchange information than before. In its risk assessment, the foreign party should also factor in the possibility that the CAC (or another regulator) will examine the CII and that any regulatory action may also involve the foreign party's data held by the CII.[18]

11. Effect on Chinese Companies

Chinese enterprises desperately need international data portability for daily operations. In the end, domestic economic drivers like this may pressure the government to seek flexible interpretations of the CSLaw. This would create some room for corporate concessions. While every country has legitimate security interests in industries related to IT, the approach taken by the Chinese authorities seems to be distorting the market and will carry real economic cost. For example, it has been calculated that the potential de-globalisation of China's ICT industry more broadly could lead to a 1.8 to 3.4 per cent reduction in China's GDP. Based on 2015 figures, this amounts to EUR 190 billion per year, and by 2025 could amount to a cumulative reduction of EUR 2.85 trillion.[19]

12. Recent Developments

There are many unknowns about how the CS Law will be implemented and enforced, or how it will affect the overall market for businesses operating in China. In early August 2017, Chongqing's Public Security Bureau issued a warning to a local internet data center company for its failure to preserve a user login information blog, ordering the company to rectify it within 15 days.[20] In 2017 local branches of the CAC launched investigations into Baidu Inc., Weibo Corp. and Tencent Holdings Ltd. for user-generated content "laden with 'violence, porn, rumors'" that it claimed to be disruptive to social order.[21] However, one may question if such crackdowns are actually a novelty since internet content has long been closely monitored and subjected to government censorship in the Peoples Republic of China.[22] The true intent of the Chinese government will be revealed once the enforcement of the CS Law begins. It will be most interesting to see how the enforcement actions will relate to the storage and usage of users' personal data and information and whether and how those enforcement actions are brought against foreign internet service providers.[23]

IV. Conclusion

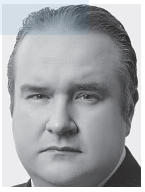
Both the EU NIS-Directive and China CSLaw pursue a closer cooperation between industry and supervision. Particularly in the field of IT security, the success of this endeavor will increasingly depend on how cooperatively and effectively public bodies and private companies work together, especially in the field of standardization and certification.

There are also several parallels between the CSLaw and the European approach. Both security regimes are rooted in a shared desire for accountability (Art. 40 CSLaw), transparency and lawfulness (Art. 41 CSLaw), full disclosure of leaks or breaches (Art. 42 CSLaw), collection and usage statements (Art. 40 CSLaw), and even the right to correct or delete information (Art. 43 CSLaw).

The biggest difference between the European and the Chinese security approach is, that the Chinese CSLaw is "not only for the legal protection for the interests of the masses in cyberspace, but also effectively safeguards national cyberspace sovereignty and security."[24] Stimulating domestic production may be seen as a positive byproduct of the CSLaw internally, but if foreign businesses are unable to retain their proprietary assets in an environment already rife with counterfeits, they will take their business to other markets, ultimately hurting the Chinese economy.[25] International business leaders have lobbied to delay full implementation of the CSLaw, but no official changes have been made to date. The Internet regulatory body Cyberspace Administration of China (CAC), has authorized the delay of restrictions on cross-border data flows until the end of 2018.

Nevertheless, this legal trend has far-reaching effects that make the companies calculating liabilities now in order to avoid painful regulatory burdens later. To run a business in China will become more costly for several companies.

Attorney at law Daniel Albrecht



Guest Professor for Civil Law (CUPL Beijing, China) and Managing Counsel at Starke, Beijing

Corporate Law, Trademark Law, E-Commerce

law@beijing-starke.com

www.beijing-starke.com

18 *Ashurst, Michel Sheng*, China's new cybersecurity law, - implications for foreign busnisses, Corporate Briefing July 2017.

19 Preventing Deglobalisation: An Economic and Security Argument for Free Trade and Investment in ICT, US Chamber of Commerce, Rhodium Group and Covington & Burling LLP.

20 See report in Chinese on the official website of the Chongqing Municipal Public Security Bureau at http://www.cqga.gov.cn/jfzx/53137.htm.

21 Chinese Regulator Launches Probe Into Tencent, Weibo and Baidu, *Bloomberg News*, August 11, 2017, available. at: https://www.bloomberg.com/news/articles/2017-08-11/chinese-regulator-starts-probe-into-tencent-weibo-and-baidu.

22 *Bennett, Isabella*, "U.S. Internet Providers and the 'Great Firewall of China,'" *Council on Foreign Relations*, February 23, 2011.

23 An Overview about China's new cybersecurity Law, *Jeffrey A. Rinde* u.A., CKR Law, 15.Aug.2017.

24 China Daily 31.05.2017, http://cn.chinadaily.com.cn/2017-05/31/content_29558817.htm.

25 Internet Governance Project, Georgia Tech, *Milton Mueller*, China's Cyber Security law: The Impact of digital trade; August 7th, 2017.