Chambers

GLOBAL PRACTICE GUIDES

Definitive glo
comparative a

Cybersecurity

Definitive global law guides offe
comparative analysis from top-r

China

Law & Practice
and
Trends & Developments

Susan Ning and Han Wu
King & Wood Mallesons

practiceguides.chambers.com

2021

CHINA

Law and Practice

Contributed by:
Susan Ning ***and*** *Han Wu*
King & Wood Mallesons see p.24

CONTENTS

1. BASIC NATIONAL REGIME

1.1 Laws

The Civil Code of the PRC (Civil Code) is a periodic legislative response to the problem of personal information (PI) protection. The Personality Rights Chapter of the Civil Code adopts a special section to provide protection on both PI and privacy right, recognising the personality attributes of PI. In addition, the Civil Code preliminarily stipulates the definition and types of PI, the legal basis for processing PI, and the rights of PI subjects, etc. The provisions on PI are periodical and general, therefore remaining to be further refined and implemented by subsequent legislation.

As compared to the scattered provisions set forth by the Civil Code, the Cybersecurity Law of the PRC acts as the overarching construct of the cybersecurity regime in China and sets forth specific requirements in various cybersecurity segments. The Cybersecurity Law applies to network operators (NOs) in China, a term defined as any entities that own or administer a network or provide network services, setting forth liabilities of violation in the form of fines and injunctions against the network operators and/or their responsible personnel.

The subject matter regulated by the Cybersecurity Law, supplemented by relevant regulatory documents (including drafts), can be summarised in two main categories: (i) network operation security, which addresses the security of operation, structure and management of a network system; and (ii) network information security, which mainly focuses on measures and structural arrangements to protect PI and important data. The specific requirements of the two categories can be divided into the following major segments.

In addition, the Data Security Law, released on 10 June 2021 and to be effective on 1 September 2021, articulates specific security requirements for data processing. The Law for the first time explicitly articulates extra-territorial jurisdiction in the Chinese data regulation regime, applying to overseas data processing activities that jeopardise China's national security or the interests of the state or citizens. The Law contemplates a variety of state data protection mechanisms from an overarching architecture perspective, such as classified data protection system, state data security certification and standardisation, data transaction system, state open data system, and others, with implementation measures to be later promulgated by state and municipal regulatory authorities.

Network Operation Security

Multi-level protection scheme (MLPS)

A classified cybersecurity protection scheme (also known as the multi-level protection scheme or MLPS) is recognised as the basic legal system to ensure structural network security in China. Under MLPS, network operators must be classified by one of the five levels according to their security impact if the system is damaged, with classification levels ranging from one to five. Progressively stringent requirements for network security and filing obligations with authorities are imposed on network operators at higher MLPS classification levels. Please refer to **4.3 Critical Infrastructure, Networks, Systems** for further details of MLPS.

Security requirements

Certain security requirements are imposed on the suppliers of network products and services, such as taking remedial actions to correct security vulnerabilities and continuing provision of security maintenance services. Any identified key network equipment and specialised cybersecurity product must pass security certification before its supply.

Critical information infrastructures (CIIs)

Critical information infrastructures (CIIs) – defined as network facilities and information systems that may severely endanger national security, social welfare and public interests upon sabotage, malfunction or data breach – are afforded additional and strict security protection requirements and there are obligations regarding security management mechanism, training, technical measures of cybersecurity protection, procurement of network products and services, emergency response plans, and others.

In addition, in the event that procuring network products and services by CII operators (CIIOs) may affect national security, competent authorities must conduct cybersecurity review of such procurement.

Monitoring, etc

Network operators shall set up cybersecurity monitoring, early warning and emergency response plans to mitigate cybersecurity risks and timely notify relevant parties upon the occurrence of cybersecurity incidents.

Network Information Security

Legitimate processing

NOs shall process (including collection, storage, use, sharing, transfer, disclosure and deletion) personal information lawfully, legitimately, and only to the extent necessary, and obtain informed consent from the PI subjects regarding the purpose, methods and scope of processing. NOs shall also take necessary measures to ensure the security of PI it collects and promptly inform PI subjects and relevant authorities upon divulgence of PI.

NOs shall take measures to respond to legitimate request from PI subjects related to their PIs. In particular, with reference to national standards supporting the Cybersecurity Law, depending on their different roles in PI processing, NOs are categorised as personal information controllers (PICs) – defined as any entity or individual capable of determining the purpose and method of PI processing – and personal information processors (PIPs) – defined as entities or individuals processing PI on behalf of PICs.

When PI contains sensitive personal information (SPI), additional security requirements are imposed on PICs, such as protection by encryption. Please see **4.1 Personal Data** for details of PI protection requirements for NOs, PICs, and PIPs.

Important data

Important data refers to data whose divulging may directly affect national security, economic security, social stability, public health and security, such as undisclosed government information and information regarding mass population, genetic health, geographical and mineral resources. Entities responsible for processing important data are subject to various security obligations under Data Security Law, such as conducting and reporting periodic security assessments and adopting technical measures of encryption, back-up and monitoring. The scope of important data will be defined by regulatory authorities of different industries and regions in upcoming legislations. Please see **4.2 Material Business Data and Material Non-public Information** for details on important data protection requirements.

Cross-border data transfer

CIIOs conducting cross-border data transfer abroad of PI and important data must store such data within China and perform security assessment of cross-border transfer. General NOs conducting cross-border data transfer are also advised to perform such security assessment. According to the current draft regulations on cross-border data transfer, such assessment may cover the nature of data to be transferred,

the data exporter and the data recipient's respective capabilities of data security protection, the receiving country or region's political and legal environment of data protection, and evaluation of the impact to PI subjects, national security and social interests by such transfer. Cross-border data transfer is prohibited if it threatens national security or public interests. For general NOs to transfer data abroad, please see 'Cross-border Data Transfer' under **3.1 De Jure or De Facto Standards**.

The Cybersecurity Law and relevant regulatory documents are mainly enforced by the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology of China (MIIT), the Ministry of Public Security of China (MPS), and the State Administration for Market Regulation (SAMR). It is worth mentioning that regulatory documents in drafts are commonly applied as important reference for cybersecurity enforcement.

State secrets

The Guarding State Secrets Law of PRC (State Secrets Law) classifies state secrets into three tiers and articulates respective protection requirements, which generally prevail over other data protection requirements when data is identified as state secrets.

Restrictions on state activities

Under Data Security Law, governmental authorities bear confidentiality obligations with respect to the personal information and business confidential information held by them.

Other Laws and Regulations

Various other laws and regulations also contribute to other segments of the cybersecurity regime as illustrated below.

The Cryptography Law

The Cryptography Law, mainly enforced by the Cryptography Administration of China (SCA), sets forth requirements for supplying and adopting various encryption, in particular the commercial encryption which plays a key role in network security required by the Cybersecurity Law. The law also sets forth civil liabilities of violation.

The Provisions on the Ecological Governance of Network Information Contents

The Provisions on the Ecological Governance of Network Information Contents takes network information contents as the main governance objects, and, by aiming at establishing and perfecting a comprehensive network governance system, creates a clean cyberspace and builds a sound network ecosystem.

The Criminal Law

The Criminal Law of the People's Republic of China (Criminal Law) recognises the various cybercrimes infringing PI or computing systems and crimes utilising networks, and the crime of failure to perform cybersecurity obligations, punishable by imprisonment and/or fines. The above-mentioned Criminal Law provisions are enforced by MPS and its local agencies.

1.2 Regulators

All key regulators of cybersecurity in China – namely the CAC, MIIT, MPS and SAMR – have regulatory authorities at the national level and their branch agencies at the county level or above that exercise their authorities within their respective geographic jurisdiction, including audits and investigations of NOs regarding violation of cybersecurity-related laws and regulations.

CAC has the overarching responsibility of planning and co-ordination of cybersecurity regulation. It is the most active regulator in terms of enacting cybersecurity regulatory documents,

and its enforcement focuses on the governance of the "internet ecology" and network information content.

The MPS is the key regulator and enforcement authority of the MLPS and network operation security, and responsible for investigating and preventing crimes related to computing system and PI infringement.

The MIIT oversees the telecommunication and information technology industry and thus administers the licences of the market participants in this industry. Its enforcement focuses on PI protection in these industries, especially the telecommunication value-added services.

The SAMR is responsible for the protection of consumer rights, including consumers' rights in PI and fair market competition.

In addition to the four key regulators, some national regulators focus on specific areas of cybersecurity-related matters. The National Security Commission of the Communist Party is responsible for overseeing and formulating state data security strategies under Data Security Law. The Ministry of State Security (MSS) is responsible for safeguarding national security of data processing activities. The National Information Security Standardisation Technical Committee (TC260) is responsible for the promulgation of cybersecurity-related national standards; the National Administration of State Secrets Protection (NASSP) is responsible for MLPS classification and protection related to state secrets. The SCA is responsible for regulation and enforcement in relation to encryption activities. The China Securities Regulatory Commission (CSRC), the China Banking and Insurance Regulatory Commission (CBIRC), the China Insurance Regulatory Commission (CIRC), and the China Banking Regulatory Commission (CBRC) also regulate cybersecurity matters in their respective financial areas.

1.3 Administration and Enforcement Process

In general, the penalties that cybersecurity regulators or data protection authorities impose on the investigated entities or individuals must comply with the liabilities articulated by the Cybersecurity Law and, in case where criminal culpability arises, the Criminal Law.

As for regulator-specific administrative process, the Provisions on Internet Security Supervision and Inspection by Public Security Organs (Public Security Provisions) set forth the standard administrative process of cybersecurity enforcement by the MPS and its branch agencies. The Public Security Provisions limit the scope of the targeted network service providers and the contents of supervision and investigation by public security agencies. It also articulates two methods of supervision and investigation, namely onsite inspection and remote inspection, and sets forth procedural requirements for each method.

Other due process and appeal rights issues not contemplated by the above-mentioned laws and regulations shall, in theory, apply the administration laws of China, namely the Administrative Penalty Law, the Administrative Reconsideration Law and the Administrative Litigation Law. In practice, we have no knowledge of any remedies under the three above-mentioned administration laws initiated by respondents. Thus, further observation is advised regarding the applicability of the administration laws to cybersecurity-related administrative process and enforcement.

1.4 Multilateral and Subnational Issues

Currently, most cybersecurity enforcement actions are based on laws and regulations at the national level. Regulations at provincial or municipal level are comparatively limited in num-

ber and lack uniformity and consistency in subject matter and legal effectiveness. Furthermore, such regional regulations may only specify but not exceed the requirements already contemplated by the Cybersecurity Law. For example, the Tianjin City Cyberspace Administration issued the Measures for the Administration of Data Security of Tianjin (for Trial Implementation) in June 2019 to further specify Cybersecurity Law requirements for data collection and processing conducted within Tianjin.

Agencies at the subnational level play a piloting and critical role in cybersecurity enforcement activities. For example, during the "*Jingwang*" ("cleansing the internet") national campaign in 2020 against cybercrimes and PI infringement, the Nanning Cyber Police Department investigated 812 cybercrime cases and arrested 1,282 criminal suspects. In November and December 2020, Guangdong Communications Bureau ordered 201 apps to rectify illegal collection and usage of personal information, and took down eight apps for illegal network service.

1.5 Information Sharing Organisations

The National Computer Network Emergency Response Technical Team/Coordination Centre of China (CNERT) is a national non-government cybersecurity information-sharing organisation that has played the key co-ordinating role in China's cybersecurity emergency response community since 2001.

CNERT runs the two databases that monitor, alert and provide solutions of information vulnerabilities and malware, namely the China National Vulnerability Database (CNVD) and the Critical Information Infrastructure Security Response Centre (CII-SRC), both of which are joint efforts of information system operators, telecommunication operators, cybersecurity service providers and internet service providers.

In addition, the China National Vulnerability Database of Information Security (CNNVD) is a central government-funded database that has analysed, alerted and responded to information vulnerabilities since 2009.

1.6 System Characteristics

While the scope of cybersecurity regime in China is comparatively comprehensive and diverse in subject matter, it is still under development with more supplemental measures expected to be released. Cybersecurity enforcement in China has been active and aggressive, especially since 2019, usually focusing in specific areas, such as the mobile application data protection campaign in 2019. Enforcement is expected to expand in scope and enhance in extent in 2020 and 2021.

The cybersecurity legal system in China absorbs some security protection mechanisms from both the US and the EU systems, while maintaining its distinctive designs. For the network security perspective, China affords special protection to CII, a concept derived from the critical infrastructure in both the EU and the US systems; China also sets forth requirements for emergency response, similar to the EU and the US systems. However, the methodology to identify CII and its boundaries in China differs from that used in the EU and the US; in addition, security requirements for CII is more expansive in China as they are organically connected to other cybersecurity segments, such as security review, MLPS, and cross-border data transfer.

As for data protection, China is similar to most other jurisdictions in the respect that consent of PI subjects is the foundation of PI protection, yet it is different in at least three major respects:

- currently, PI in China cannot be transacted;
- consent by the PI subject is absolutely central to the legal system in China, and thus the dominant source of the lawfulness of PI pro-

cessing in China, save for a few exceptions such as PI processing mandated by laws and regulations, directly related to national security, directly related to criminal legal actions, or others;
- the China regime affords additional protection to important data, a concept that the EU or the US system does not explicitly contemplate.

1.7 Key Developments

In the prior 12 months, a series of key laws and regulations (including drafts) were released or came into force, including the following.

- The Civil Code came into force, with its Personality Rights Section recognising the protection of legal interests in PI at the most foundational level of Chinese civil law.
- The Data Security Law was released on 10 June 2021. Please see **1.1 Laws** for further information.
- The Personal Information Protection Law of the PRC (Second Draft) (Draft PIPL) was announced in April 2021, marking China's first attempt to systematically define, establish, and integrate the provisions regarding PI protection at the statute level. It covers comprehensive aspects of PI protection, including the legal basis for processing PI, requirements for obtaining consent, entrusting third parties to process PI, sharing PI, cross-board PI transfer, PI subjects' rights, and processors' PI protection obligations, as well as severe liabilities for violation.
- The Information Security Technology – Personal Information Security Specification (PI Specifications) came into force. Compared with the earlier version of PI Specifications (GB/T 35273-2017), it introduces enhanced security requirements and extended rights of PI subjects, such as heightened SPI, especially personal biometric information protection requirements and additional restrictions in PI collection.
- The Provisions on Governance of Network Information Content Ecology came into force, which set forth certain requirements to network information content providers, platforms and users in order to promote a positive internet environment.

As for significant law enforcement activities, the special enforcement campaign against mobile applications illegally collecting and processing PI has discovered thousands of mobile applications infringing PI and ordered violators to rectify accordingly, marking the trend of increasing and extensive enforcement activities by joint forces of regulators. The "*Jingwang 2020*" campaign against internet-based crimes and PI infringement also marks the continuous strengthening of elevated cybersecurity enforcement by the MPS.

1.8 Significant Pending Changes, Hot Topics and Issues

It is anticipated that the Draft PIPL will be finalised in 2021, following the recently released Data Security Law. The release of Draft PIPL is expected to be game-changing to the market, in particular due to the Draft PIPL's expanded legal basis for processing PI, concrete rules for cross-border PI transfer, and heavy liabilities. With the release of the Data Security Law and the Draft PIPL, in 2021, a number of draft regulations and national standards are expected to finalise in the area of:

- measurements for cross-border data transfer of PI and important data;
- identification and security requirements for important data, in particular the catalogue of important data to be formulated by municipal governments as required by the Data Security Law; and
- the identification of CIIO.

A number of draft regulations and national standards regarding these sectors are likely to be finalised this year. Both the Data Security Law and Draft PIPL provide extra-territorial jurisdiction clauses, which are expected to be a focus for judicial attention and regulatory documents in the rest of 2021 – a number of offshore entities providing services to Chinese customers may fall within the jurisdiction of the two laws.

Hot topics of enforcement emerging since the second half of 2020 include (i) the lawfulness of collecting data from third parties by technical measures, in particular software development kit (SDK), and (ii) processing PI within the scope of necessity, in particular since the release of Provisions on the Scope of Necessary Personal Information of Common Mobile Internet Applications in March 2021.

2. KEY LAWS AND REGULATORS AT NATIONAL AND SUBNATIONAL LEVELS

2.1 Key Laws

As mentioned in **1.1 Laws**, the Cybersecurity Law lays the foundation of the cybersecurity legal system in China that applies to all kinds of data, systems, NOs, and information infrastructures, supplemented by a series of implementation measures and other laws and regulations as listed below and sorted by the segments of the Cybersecurity Law.

Network Operation Security

A1: MLPS – Regulation on Graded Protection of Cybersecurity (Draft for Comments) (Draft MLPS Regulations).

A2: CII Protection – Regulations on the Security Protection of Critical Information Infrastructure (Draft for Comments) (Draft CII Regulations); Cybersecurity Review Measures.

A3: Cybersecurity Review and Emergency Response – Cybersecurity Review Measures (Draft for Comments), to replace the Measures for the Security Review of Network Products and Services (for Trial Implementation) upon finalisation.

A4: Encryption – the Cryptography Law and the Law on Guarding State Secrets.

Network Information Security

B1: Personal Information Protection – Civil Code, Draft PIPL, Provisions on the Scope of Necessary Personal Information of Common Mobile Applications and Provisions on the Cyber Protection of Children's Personal Information.

B2: Important Data and State Secrets – Data Security Law.

B3: Cross-border Data Transfer – Data Security Law and Draft PIPL.

B4: Internet Information Content Administration – Provisions on Governance of Network Information Content Ecology, Provisions on the Administration of Blockchain Information Services, Provisions for the Administration of Internet News Information Services, and others.

In addition, Articles 253(1), 285, 286, and 287(2) of the Criminal Law apply to the crimes related to cybersecurity.

2.2 Regulators

Please refer to **1.2 Regulators** for their respective responsible area of cybersecurity.

2.3 Over-Arching Cybersecurity Agency

Under Article 8 of the Cybersecurity Law, the CAC is the overarching cybersecurity regulator

and agency in China. Please refer to **1.2 Regulators** for its specific regulatory role.

2.4 Data Protection Authorities or Privacy Regulators

The CAC, MIIT, MPS, SAMR at the national level and their branches at the county level or above are the major data protection authorities and privacy regulators. Please refer to **1.2 Regulators** for their respective role in data protection. The TC260 is also an important privacy regulator that focuses on the promulgation of data protection-related national standards, and most of the national standards are not legally binding but serve as important reference in legal enforcement activities.

2.5 Financial or Other Sectoral Regulators

The CSRC administers a series of securities-related financial activities in China, including initial public offering (IPO), corporate restructuring, and related transactions. Data compliance of listing companies has become one of the key factors in CSRC approving such activities and contributes to CSRC's rejection of IPO listing application in some cases.

The CBIRC, CIRC, and CBRC also regulate cybersecurity matters in their respective responsible financial areas. In particular, the CBIRC takes an active regulatory role, as it issued the Guidelines for Data Management of Banking Financial Institutions in May 2018 and is currently promoting the legislation regarding personal financial information protection. The People's Bank of China (PBOC) is also a key regulator over financial institutions, and released Implementing Measures of the PBOC for Protection of Financial Consumers' Rights and Interests, which came into force on 1 November 2020.

2.6 Other Relevant Regulators and Agencies

Other key regulators include the NASSP and the SCA, as discussed in **1.2 Regulators**.

3. KEY FRAMEWORKS

3.1 e Jure or De Facto Standards

Key Frameworks

A series of national standards and government announcements have been released. Most of these documents are still in draft form for public comments and currently all such national standards are not mandatory. However, in practice a number of these documents are commonly deployed as guidance for law enforcement and corporate compliance, such as the following.

MLPS and network security in general

The Information Security Technology – Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019) (MLPS Baseline Standards) and the Information Security Technology – Classification Guide for Classified Protection of Cybersecurity set forth specifications encompassing the MLPS classification and evaluation process and the respective requirements for systems at each MLPS classification level. Guidelines on the Protection of Information Security of Industrial Control Systems (ICS Guidelines), promulgated by the MIIT, set forth security protection for industrial control systems (ICS) in various aspects, such as physical environment, authentication, remote access, and emergence response.

CIIs

The Information Security Technology – Cybersecurity Protection Requirements of Critical Information Infrastructure (Draft for Comments), the Information Security Technology – Guide to Security Inspection and Evaluation of Critical Information Infrastructure (Draft for Comments), and the Information Security Technology – Indi-

cator System of Critical Information Infrastructure Security Assurance (Draft for Comments) contemplate the requirements of the identification, inspection, evaluation and security of CIIs.

Emergency response

The National Cybersecurity Incident Emergency Response Plan, promulgated by the CAC, sets forth emergency response measures to various cybersecurity incidents by authorities. The Emergency Response Plan for Cybersecurity Incidents in Public Internet Network, promulgated by the MIIT, sets forth emergency response measures applicable to internet industry participants.

Personal information

The national standard, PI Specifications, is the key and fundamental guidance to PI protection-applicable PICs and is prevalently referred to and adopted in data protection compliance practice and enforcement. Guidelines for Internet Personal Information Security Protection, promulgated mainly by the MPS, provides guidance of PI protection tailored to internet companies. Measures for the Identification of Collecting and Utilising Personal Information by Apps in Violation of Laws and Regulations, jointly issued by the CAC, MPS, MIIT and SAMR, sets forth methods of identifying unlawful PI processing by mobile applications. Provisions on the Scope of Necessary Personal Information of Common Mobile Applications, released in 2021, identifies the scope of necessary PI for the basic services of 36 categories and prohibits apps from refusing to provide basic service when users refuse to provide non-necessary PI.

Cross-border data transfer

As mentioned above, under the CSL, unless otherwise required by laws and regulations, CIIOs are required to localise PI and important data obtained from operations in China, conduct cross-border transfer of such data only when necessary, perform security requirement before such transfer, and obtain PI subjects' consent for the transfer of PI. The Draft PIPL, if finalised "as is", extends the security obligations above to entities processing a large volume of PI. Other entities to transfer PI abroad shall satisfy at least one of the following conditions, in addition to the subjects' consent:

- conducting security assessment;
- personal information protection certification by qualified entities;
- entering into standard contracts recognised by the state with the PI receiver; or
- other conditions provided by applicable regulations.

3.2 Consensus or Commonly Applied Framework

The major commonly applied framework for required "reasonable security" are the regulations and national standards related to the MLPS. Please see **2.1 Key Laws** and **3.1 De Jure or De Facto Standards** for further details.

3.3 Legal Requirements

The following illustrate the legal requirements and applicable standards for specific cybersecurity sectors.

Written Information Security Plans or Programmes

China has not established any legal requirements regarding the written information security plans or programmes. However, NOs are generally required to provide PI subjects with written documents, usually in the form of privacy policies or consent letters, to inform them of the purpose, methods, and scope of PI collection and processing, the NOs' PI security protection mechanisms, PI subjects' approaches of asserting PI-related claims, risks of PI processing, and others.

Incident Response Plans

The Cybersecurity Law requires that relevant government authorities formulate emergency response plans for their respective industries and fields. Such emergency response plans shall comply with the National Cybersecurity Incident Emergency Response Plan, which classifies cybersecurity incidents into four categories according to their severity and articulates the respective responses to each level.

As for private practices, systems classified at MLPS level 2 or above must formulate their own emergency response plans, provide training to its relevant personnel, and conduct drills. The Emergency Response Plan for Cybersecurity Incidents in the Public Internet Network also sets forth response requirements for foundational telecommunication companies.

Appointment of Chief Information Security Officer or Equivalent

Under the Cybersecurity Law and MLPS-related regulations, each NO shall appoint an officer with the general responsibility of overseeing the NO's cybersecurity and MLPS-related arrangements. The CIIOs shall, in addition to appointing such officer, also conduct a security background check of the officer. Further, the PI Specifications and some other national standards also require PICs to appoint the officer responsible for personal information protection.

Involvement of Board of Directors or Equivalent

In China, there is no general legal requirement for direct involvement of the board of directors or equivalent in the cybersecurity matters of a company. However, the fiduciary duty of board of directors under the Company Law of the PRC may give rise to the board's obligations to establish and maintain an effective cybersecurity systems and to take corresponding security measures, depending on the circumstances such as the company's affiliated industry, the significance of cybersecurity risks, and others.

The Provisions on the Administration of Informatisation of Insurance Institutions (Draft for Comments) issued by CBIRC require institutions to establish an informatisation committee, responsible for informatisation matters including cybersecurity, under the direct leadership of the board of directors.

Conducting Internal Risk Assessments, Vulnerability Scanning, Penetration Tests, etc

- MLPS national standards and draft regulations set forth a large variety of risk-assessment requirements, such as periodical security assessments taken by systems at level 3 or above.
- The Draft CII Regulations require that the CIIOs establish and maintain a CII risk assessment mechanism and conduct assessment at least annually and before the initiation of CII operation or any material change of the CII.
- According to Draft PIPL and other draft regulations, NOs transferring PI or important data abroad may be required to conduct security assessments.
- Under PI Specifications, PICs shall conduct PI security impact assessments on its PI processing in certain circumstances such as before entrusting, sharing, or transferring PI to a third party or publicly disclosing PI. PICs shall assess the sufficiency of consent, necessity of processing, risks of adverse effect to PI subjects, effectiveness of security measures, and others. The Information Security Technology – Guidance for Personal Information Security Impact Assessment defines the framework, methods and processes of PI security impact assessment under different scenarios.

Multi-factor Authentication, Anti-phishing Measures, Ransomware, Threat Intelligence

The MLPS national standards set forth a variety of security requirements to network and computing systems, such as:

- systems at level 2 or above shall adopt multi-factor authentication of user identity using passcodes, encryption, biometric technologies and/or other technical measures, in which at least one factor must be encryption; and
- all systems shall install counter-malware software, update malware code database regularly, and establish internal policies of malware countermeasures.

Insider Threat Programmes

The MLPS national standards set forth a variety of security requirements to network and computing systems, such as:

- systems at level 2 or above shall adopt multi-factor authentication of user, in which at least one factor must be encryption; and
- all systems shall install and maintain updated counter-malware software and establish internal policies correspondingly.

Vendor and Service Provider Due Diligence, Oversight and Monitoring

Obtaining PI from vendors and service providers is recognised as indirect collection of PI. The PI Specifications articulate that PICs indirectly collecting PI shall request the PI providers to clarify the source of PI, the lawfulness of the source, and the scope of PI subjects' consent, and obtain supplemental consent from PI subjects if the intended processing exceeds the scope of consent.

When PICs provide their vendors or service providers with PI, their activities constitute the entrusting, sharing, or transferring of PI. The PI Specifications set forth a series of requirements for such PI provision, such as obtaining informed consent, conducting PI security assessments, contracting with and monitoring PI receivers, and assisting PI subjects to assert lawful requests.

In the event of providing PI to vendors and service providers abroad, PICs shall conduct cross-border data transfer security assessments.

When procuring network products or services from vendors or providers, under MLPS, the NOs shall ensure that the products or services comply with applicable regulations and standards, and systems at level 3 or above shall conduct inspections before procurement and regularly update and review the list of candidate products. In addition, CIIOs shall ensure that the products or services procured have passed the cybersecurity review by the state if such procurement may affect national security.

Use of Cloud, Outsourcing, Offshoring

The use of cloud is mainly regulated from the MLPS aspect. The MLPS national standards articulate a complexity of extended security requirements for cloud computing at each MLPS level, covering various aspects of cloud computing security, such as physical environment, network structure, access control, audits, authentication, data integrity and back-up, internal management, and service providers. Cloud computing systems at level 2 or above shall maintain their servers physically within China. When the use of cloud involves PI, PICs shall keep such PI physically stored within China.

Outsourcing PI processing is recognised as entrusting, sharing or transferring of PI to third parties. Please see Vendor and service provider due diligence, oversight and monitoring' (above) for details.

Offshoring mainly concerns cross-border data transfer. Please see the discussion of this topic in **1.1 Laws** for details.

Training

Under the Cybersecurity Law, CIIOs are required conduct cybersecurity education, technical training and skill assessment for employees on a periodical basis. Under PI Specifications, NOs are required to conduct periodical training and assessments for their relevant personnel regarding PI protection.

3.4 Key Multinational Relationships

China has entered into Regional Comprehensive Economic Partnership (RCEP) in 2020 covering 15 countries. RCEP establishes regional consensus on cross-border data transfer and limits its member's restrictions on the international digital trades, which facilitate the regional free circulation of data.

China has entered into various bilateral agreements on mutual legal assistance in civil, commercial or criminal matters with a number of countries. These treaties set forth due process requirements of bilateral international legal assistance, which lays the foundation of China's participation in multinational co-operation, such as international co-operation in combating internet-related crimes and frauds.

In addition, China has been actively participating in activities of the establishment of international standards initiated and organised by the International Organisation for Standardisation (ISO).

4. KEY AFFIRMATIVE SECURITY REQUIREMENTS

4.1 Personal Data

According to Article 42 of Cybersecurity Law and Article 1038 of Civil Code, NOs shall take technical and other necessary measures to ensure the security of PI it collects, and to protect PI from disclosure, damage or loss. In case of disclosure, damage or loss of, or possible disclosure, damage or loss of such information, the network operator shall take immediate remedies, notify the users in accordance with the relevant provisions, and report to the competent authority.

Specifically, with reference to the Cybersecurity Law and its supporting measures, information security requirements focus on four main areas – de-identification, safe transmission, deletion and contingency plan. NOs shall establish and improve in internal system for user information protection. Internal department or personnel in charge of the cybersecurity must keep any and all PI, privacy, and business secrets obtained during their performance of duties in strict confidence.

De-identification

PI should be immediately de-identified after being collected by PICs, and technical and managerial measures should be taken to separately store the de-identified data and information that can be used to restore the identification, and it should be ensured that no particular individual will be identified during subsequent processing of such data.

Safe Transmission

According to PI Specifications, in principle, PI is not allowed to be shared or transferred. If sharing or transfer by the PICs is necessary, PICs shall perform a PI security impact assessment beforehand, obtain PI subjects' consent after proper notification, and accurately record the sharing or transferring of PI. Particularly, SPI shall be transferred and stored using encryption and other security measures.

As to the issue of cross-border data transfer, please refer to **1.1 Laws** ("Cross-border Transfers") for details.

Deletion

If a PI subject finds that collection and use of his or her PI by NO violates the laws, administrative regulations or the agreement by and between such NO and the PI subject, the PI subject is entitled to require NO to delete his or her PI. In case of the PI subject's discovery of an error, PI subject is entitled to require NO to make corrections and shall take measures to delete or correct.

What's more, in order to meet the necessity requirement under Cybersecurity Law and Civil Code, the retention period of PI shall be the minimum necessary to realise the purpose. When the agreed-upon retention period expires, PI shall be deleted or anonymised as soon as possible.

Emergency Response Plan

Please refer to **3.3 Legal Requirements** ('Incident Response Plans') for details.

4.2 Material Business Data and Material Non-public Information

In general, NO's internal department or personnel in charge of the cybersecurity must keep all business secrets obtained during their performance of duties in strict confidence. Data protected by China's cybersecurity regime can generally be divided into categories of PI, important data, trade secrets, commercial encryption, and others.

Enterprises are advised to first identify whether its material business data and material non-public information would fall under the definition of PI or important data. If both categories do not apply, such data may, if applicable, fall under the scope of trade secrets, the identification and protection of which are set forth by the Anti-Unfair Competition Law of the PRC.

For security requirements of business data or non-public information identified as PI, please refer to **4.1 Personal Data**.

If material business data is recognised as important data, according to the Cybersecurity Law, NOs are required to take measures such as back-up and encryption of important data. Besides, the Data Security Law also provides the protection system for important data. Article 21 states that each region and department shall formulate the specific catalogue of important data for the region, department, related industry and sector, and focus on the protection of data listed. Article 27 (2) further mandates important data processors to appoint the person and set up management institution in charge of data security. Article 30 requires that such processor to carry out risk assessment on data processing activities on a regular basis, and submit the risk assessment report to the relevant competent department.

Various requirements are imposed by the Cryptography Law when enterprises adopt commercial encryption to protect its data. The commercial encryption products closely related to national and social public interests shall be certified by qualified inspection agencies before marketisation. CIIOs adopting commercial encryption shall conduct security assessments by themselves or qualified inspection agencies. When CIIOs' procurement of network products or services adopting commercial encryption may affect national security, security review of the procurement shall be conducted by relevant state authorities.

4.3 Critical Infrastructure, Networks, Systems

Under the MLPS, in principle NOs are required to:

- formulate internal security management systems and operation instructions to determine the person in charge of cybersecurity and define accountabilities for cybersecurity;
- take technical measures to prevent computer virus, network attacks, network intrusions and other activities that endanger cybersecurity;
- monitor and record network operation and cybersecurity events, and maintain cyber-related logs for no less than six months as required; and
- take measures such as data classification, back-up and encryption of important data, etc.

MLPS protects generic information networks, ICS, cloud computing platforms, internet of things (IoT), big data platforms, mobile communication systems, and others network systems (MLPS subjects). NOs have different filing and self-assessment obligations for their MLPS subjects at each of the five protection levels – the higher level the classification is, the higher compliance obligations the NOs have.

In addition to the above requirements applicable to all NOs, CIIOs are in principle identified as level 3 or above, and have additional general obligations to:

- establish a dedicated security management department, appoint a cybersecurity officer, and carry out security inspection of such cybersecurity officer and people in key positions;
- provide periodic cybersecurity education, technical training and assessments for its employees;
- maintain back-up for important systems and databases in anticipation of catastrophes; and
- formulate emergency response plans for cybersecurity breach incidents and conduct periodic drills.

In the scenario of cross-border data transfer by CIIOs, please refer to **1.1 Laws** ('Cross-border Transfers') for details.

In addition, the Draft CII Regulations further specify the requirements on the security protection of CII, encompassing the establishment of CIIs, response to security incidents, daily operation and security maintenance, security monitoring and inspections, local data storage, security assessment of cross-border data transfers, security of network products and services procurement, and others.

Following the issuance of the Practical Guide to the Multi-level Protection Scheme and Critical Information Infrastructure Security Protection System (Practical Guide) by MPS, the basic framework of CII protection will be gradually set by series of supporting standards, including the identification, security, monitoring and warning, testing and evaluation and incident handling of CII, and important industries and sectors will simultaneously make preliminary progress in establishing the CII identification mechanism based on characteristics of each sector. Overall, the regulatory efforts focus on the CIIOs' obligation of multi-level assessment and CII protection.

4.4 Denial of Service Attacks

Apart from the general security requirements for NOs under the Cybersecurity Law described in **4.3 Critical Infrastructure, Networks, Systems**, the Draft MLPS Regulations contemplate general MLPS monitoring requirements related to preventing denial of service attacks. Particularly, while NOs shall monitor and record their

network security status, operators of MLPS subjects at level 3 or above shall in addition adopt further precautionary and monitoring measures and timely file the results with local public security bureaus.

With regard to the technical specifications of preventing denial of service attacks, the MLPS Baseline Standards prescribe respective requirements for MLPS subjects at each level regarding the security protection capacity in the four key technical aspects: secure management centre, secure network, safe regional boundary and safe calculation environment.

4.5 IoT, Supply Chain, Other Data or Systems

Apart from overarching guidelines in the Cybersecurity Law and supporting regulatory documents, there are laws and regulations in particular industries or sectors that also touch on the topic of cybersecurity, as exampled below.

- The Law of the People's Republic of China on Guarding State Secrets mandates that hierarchical protection measures shall be adopted for the computer information systems which are used for storing or processing state secrets and organs and agencies shall enhance their control over the secret-involved information system.
- The Administrative Regulations on Maps prescribes that entities engaging in internet map services shall establish the management system as well as protection measures for the data security of internet maps.
- According to Measures for the Administration of Population Health Information (for Trial Implementation), population health information shall be subject to hierarchical storage. Entities in charge shall establish a reliable working mechanism for disaster back-up of population health information, and conduct back-up and recovery inspections on a regular basis.
- The Cybersecurity Review Measures requires CIIOs to conduct cybersecurity review prior to the purchase of network product and services that affects or may affect national security to ensure the supply chain security of critical information infrastructure and safeguard national security.

5. DATA BREACH REPORTING AND NOTIFICATION

5.1 Definition of Data Security Incident or Breach

According to the National Cybersecurity Incident Emergency Response Plan, "cybersecurity incidents" refer to incidents that cause harm to the network and information systems or data therein and adversely affect society due to human factors, hardware or software defects or failures, natural disasters, etc. They can be categorised as hazardous program incidents, network attack incidents, information destruction incidents, information content security incidents, equipment and facility failures, catastrophic incidents, and other incidents. Furthermore, cybersecurity incidents are graded into four levels, namely: severely material, material, relatively material, and general cybersecurity incidents.

5.2 Data Elements Covered

For the purpose of data security incident or breach regulations, generally all types of data may be covered. In addition to general types of protected data – namely, PI, important data, trade secrets and data contemplated under the National Cybersecurity Incident Emergency Response Plan – other data that may be covered include state secret information, important sensitive information, critical data or other data whose loss would pose certain threats to or have

certain impacts on national security, social order, economic construction, and public interests.

5.3 Systems Covered

The legal construct of data security incident or breach covers:

- systems involving important network and information systems that undertake business closely related to national security, social order, economic development and public interest; and
- network and information systems that would pose threats to or incur impacts on national security, social order, economic construction, and public interests upon being damaged.

5.4 Security Requirements for Medical Devices

The Guidelines for Technical Review of Medical Device Network Security Registration articulate general security requirements for the applicants for medical device network registration, such as:

- paying continuous attention to cybersecurity issues during the whole life cycle of medical device production;
- perfecting the user access control mechanism; and
- notifying users of relevant cybersecurity information in a timely manner.

5.5 Security Requirements for Industrial Control Systems (and SCADA)

The fundamental security requirements for ICS (including SCADA) can be found in the ICS Guidelines which list 11 protection requirements, covering:

- security software selection and management;
- configuration and patch management;
- boundary security;
- physical and environmental security;
- identity authentication;
- remote access security;
- security monitoring and emergency drills;
- asset security;
- data security;
- supply chain management; and
- responsibility implementation.

In addition, the MLPS Baseline Standards provide security requirements specifically for ICS, such as outdoor control equipment protection, network structure security, dial-up usage control, wireless use control and control equipment security.

5.6 Security Requirements for IoT

MLPS Baseline Standards provide security extension requirements for IoT such as the physical protection of sensor nodes, device security of sensor nodes, device security of gateway nodes, management of sensor nodes and data fusion processing. Other national standards also serve as reference to IoT security, such as the security technical requirements for data transmission.

The Guidelines for the Construction of Basic Security Standard System of Internet of Things (Draft for Comment) (Guidelines for Construction) puts forward the framework of the basic security standards, key standardisation fields and directions of the basic security of IoT, including overall security requirements, terminal security, gateway security, platform security and security management.

5.7 Reporting Triggers

Government Authorities

Under the Cybersecurity Law, concerned NOs shall report incidents that threatens cybersecurity to the competent authority. Thereunder, for instance:

- according to Regulations of the PRC on the Security Protection of Computer Information

System, users of a computer information system shall report any case arising from such system to the local public security bureau at county level or above within 24 hours;
- the Telecommunications Regulations of the PRC prescribe that telecom operators shall report to the relevant national authorities upon discovery of illegal transmission of information contents as described in Article 56 in the course of their public information services.

As for CII, authorities in charge shall establish the cybersecurity monitoring mechanism and information reporting mechanism for specific industries/sectors within their respective jurisdictions.

In case of increasing risk of cybersecurity events, governments at provincial level and above shall take measures to require authorities, agencies and personnel concerned to promptly collect and report necessary information and enhance monitoring of cybersecurity risks.

In accordance with the Cybersecurity Law, China has established a national cybersecurity information reporting mechanism led by the CAC and MPS, while multi-ministries/bureaus – including MIIT, NDRC, secrecy bureau, – are also participating.

Individuals

Under the Cybersecurity Law, in case of disclosure, damage or loss (or possible disclosure, damage or loss), NOs are obligated to notify the affected users promptly. In addition, for any risk, such as security defect or bug in network products or service, the product/service providers concerned shall inform the users of such risk. In addition, according to PI Specifications, in case of PI security incident, affected PI subjects shall be notified of information related to the incident.

Other Companies or Organisations

Duty to report to other companies may be triggered by contractual obligations.

Industry organisations may determine reporting obligations to its members, under Article 29 of the Cybersecurity Law. Other industry self-regulated obligations to report to information-sharing organisations as described in **1.5 Information Sharing Organisations** may also exist.

5.8 "Risk of Harm" Thresholds or Standards

There are various thresholds and standards of notification in the China's cybersecurity regime.

For instance, according to the Emergency Response Plan for Cybersecurity Incidents in Public Internet Network, the lowest level of network security incident is the general network security incident which shall suit one of the following conditions:

- a large number of internet users within one municipality are unable to access the internet normally;
- the leakage of the information of more than 100,000 internet users; and
- other incidents that cause or may cause general harm or effect. It could be implied at least the same level of threshold of cybersecurity harm is applicable to data breach incident notification.

In addition to the harm to cybersecurity, notification obligations are also triggered when personal information is "likely to be divulged, damaged or lost" under the Cybersecurity Law.

6. ABILITY TO MONITOR NETWORKS FOR CYBERSECURITY

6.1 C bersecurity Defensive Measures

According to the Measures for Monitoring and Handling Threats to the Cyber Security of Public Internet, telecommunications authorities (including MIIT and provincial communication administrations) are in charge of monitoring cybersecurity threats. Thereafter, Information Security Technology – Basic Requirements and Implementation Guide of Network Security Monitoring sets out the framework and baselines for network security monitoring, which contemplate that network security monitoring are conducted through real-time collection of network and security equipment logs, system operation data and other information.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

The intersection of cybersecurity and privacy illustrates the conflict arising from the intertwined interests of the community and of individuals/entities. For instance, from the commercial practice perspective, as companies impose confidentiality obligations on their employees, an employee reporting the vulnerability of his or her company's network system to a third party is in conflict with his or her confidentiality obligations.

Though it is difficult to clearly define the boundaries between the two, the state tries to balance the scales. For example, public authorities may only collect and use personal information upon data subjects' authorised consent or statutory authorisations by laws or administrative regulations, even when cybersecurity threat is involved; generally speaking, we understand that only circumstances of certain criminal investigations or threats to national security may trigger such statutory authorisation. Additionally, under Article 45 of the Cybersecurity Law, authorities and their staff bearing cybersecurity regulatory authority must carefully keep strict confidentiality of any PI, privacy information, and business secrets obtained in their performance of duties. Furthermore, Article 30 of the Cybersecurity Law prescribes that cyberspace administrations and authorities concerned shall only use the information accessed in performance of their duties for cybersecurity protection purposes.

7. CYBERTHREAT INFORMATION SHARING ARRANGEMENTS

7.1 Required or Authorised Sharing of Cybersecurity Information

Please refer to **5.7 Reporting Triggers** ("Government Authorities") for details of this matter.

7.2 Voluntary Information Sharing Opportunities

With regard to Article 29 of the Cybersecurity Law, the state supports the co-operation among network operators in collection, analysis and notification of cybersecurity information and emergency response, in order to improve their cybersecurity protection capacities. The relevant industry organisations shall establish and improve respective cybersecurity rules and coordination mechanisms, enhance analysis and assessment on cybersecurity risks, regularly release risk alerts to their members, and assist their members with coping with cybersecurity risks.

In China, users, suppliers and research institutions are encouraged to report any potential system vulnerabilities identified to the CNVD, as described in **1.5 Information Sharing Organisations**, so as to gather, verify and warn against any security vulnerabilities and to establish an

effective and co-ordinated emergency response mechanism among all operators.

8. SIGNIFICANT CYBERSECURITY AND DATA BREACH REGULATORY ENFORCEMENT AND LITIGATION

8.1 Regulatory Enforcement or Litigation

In the field of administrative supervision, app governance is still the most important work for regulatory authorities in the field of data protection in 2020. MPS launched the "*Jingwang 2020" campaign to crack down all kinds of illegal and criminal activities related to network. As of June 2021, MIIT has issued a total of 14 batches of*"app notification on infringement of user rights", whereby five batches were in 2021. The notified apps concern many fields, and the listed problems focus on the illegal collection of PI compulsory access to authority, etc.

8.2 Significant Audits, Investigations or Penalties

The Agricultural Bank of China was fined CNY4.2 million for six issues involving failure to report emergencies in important information systems, illegal explicit retention of card production data, improper protection of production network and branch wireless interconnection network, network information system vulnerabilities, risk of data leakage due to sloppy data security management, and leakage of sensitive information from internet portals on 19 January 2021.

8.3 Applicable Legal Standards

Please refer to **1.3 Administration and Enforcement Process** and **1.4 Multilateral and Subnational Issues**.

8.4 Significant Private Litigation

One customer of Hangzhou Safari Park filed a lawsuit against the Park for its violation of service contract, one cause of action being the Park's unnecessary collection of facial feature information. On 20 November 2020, the court ruled that the Park shall compensate the customer for the loss of contract interests and transportation expenses and delete the facial feature information, including photos submitted by the consumer when handling the fingerprint annual card.

8.5 Class Actions

As of today, we are not aware of any class actions related to cybersecurity incidents or data breach in China.

9. DUE DILIGENCE

9.1 Processes and Issues

The process of diligence in corporate transactions mainly concerns the security aspect and the asset aspect of data.

For the security aspect, MLPS classification and evaluation of company's information system are the first steps of due diligence. Comprehensive assessments of cybersecurity based on MLPS classification will then be conducted to perform gap analysis of various security-related matters, including emergency response, PI protection, cross-border data transfer security and CII protection.

As for the asset aspect, due diligence will focus on confirming the legitimacy of the corporate data and identifying the legal boundary of corporate data assets. As security and compliance of data are the premises of data assets, taking data mapping as reference, assessment reports will be issued to review the corporate compliance of data regarding various matters, such as PI

processing, internal corporate systems related to cybersecurity and data compliance, information content administration, and others. Identifying the boundary of the company's data and the claims the company has over them will be the next step to confirm the company's proprietary rights on the corporate data.

9.2 Public Disclosure

The National General Response Plans for the Public Emergency Incidents set forth local government authorities' obligations to report public emergency incidents to higher level authorities. Cybersecurity risks that constitute public emergency incident may be disclosed and reported to various level of authorities for emergency alerts and responses. The Emergency Response Law of the PRC also requires that all entities shall timely report their potential emergency incidents to local authorities in accordance with applicable laws and regulations. In financial area, the Measures for the Administration of Initial Public Offering and Listing of Stocks and other similar IPO administration measures require that any information that may have any major impact on the investors' decisions on investment shall be disclosed in IPO prospectuses.

However, entities should note that the disclosure of cybersecurity information may be subject to certain limitations under recent draft measures by the CAC, as described in **1.5Information Sharing Organisations**.

10. OTHER CYBERSECURITY ISSUES

10.1 Further Considerations Regarding Cybersecurity Regulation

Considering the extraterritorial jurisdiction of PRC cybersecurity regulations, "domestic operation" also entails an enterprise's acts that are intended to provide goods or services to individuals within PRC.

King & Wood Mallesons is an international law firm headquartered in Asia with a global network of 27 international offices. KWM's cybersecurity team is one of the first legal service teams to provide professional services concerning cybersecurity and data compliance in China; it consists of more than ten lawyers with solid interdisciplinary backgrounds, mainly located in Beijing, while further specialisms are found within KWM's global network. The team has expertise in assisting clients in responding to cybersecurity inspections and network emergencies, the establishment of network information compliance systems, self-assessment, internal training on cybersecurity and data compliance, and other related matters. Recently, KWM advised a renowned short-term lodging platform on compliance with the multi-level protection of cybersecurity, during which KWM provided elaborative analysis on the current graded protection obligations and further comparatively analysed the newly proposed mechanism and the existing one, thereby enabling it to offer practical advice to the client.

AUTHORS

Susan Ning is a senior partner and the head of the regulatory group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals, such as the Journal of Cyber Affairs. Her publications include Big Data: Success Comes Down to Solid Compliance, and No "Data", No "Internet of Vehicles", etc. Susan's practice areas cover self-assessment of network security, responding to network security checks, data compliance training, etc. She has assisted companies in sectors such as IT, transportation, finance, etc, in dealing with network security and data compliance issues.

Han Wu is a partner of the commercial and regulatory group. He excels in providing cybersecurity and data compliance advice to multinationals' Chinese branches and in establishing network security and data compliance systems for Chinese enterprises operating abroad. In the areas of cybersecurity and data compliance, Han provides legal services, including assisting clients in establishing a cybersecurity compliance system, self-investigation on cybersecurity, network security investigations, cybersecurity incidents, data fusion and identification of data assets, etc. Han has provided legal services on cybersecurity and data compliance to companies in multiple industries. The projects in which he has participated encompass the financial payment, consumer electronics, internet advertising and healthcare industries.

King & Wood Mallesons

18th Floor, East Tower, World Financial Center
1 Dongsanhuan Zhonglu
Chaoyang District
Beijing
100020, PRC

Tel: +86 10 5878 5588
Fax: +86 10 5878 5566
Email: kwm@cn.kwm.com
Web: www.kwm.com

Trends and Developments

Contributed by:
Susan Ning ***and*** *Han Wu*
King & Wood Mallesons see p.31

Reforming the Cybersecurity Regime in China

The rapid development of cybersecurity regulation in the People's Republic of China (PRC) continues to roar down the legislative pipeline in 2020, anchoring an exciting foundation for reform of the cybersecurity regime. In particular, the release of the Civil Code of the PRC, the Draft Personal Information Protection Law (Draft PIPL), and the Draft Data Security Law (Draft DSL) have brought significant changes to the current regulatory structure centred around the Cybersecurity Law of the PRC.

The Civil Code

The Civil Code, released in May 2020 and effective since 1 January 2021, has specifically set forth a chapter for privacy rights and personal information (PI) protection. As the Civil Code is the foundational legislation for all civil rights under PRC laws, this chapter provides the overarching principles for protecting the personality aspect of PI rights in the PRC Cybersecurity regime.

The Civil Code adopts a dichotomy of rights in privacy and PI, which, respectively, are defined as "the undisturbed private life of a natural person and his [or her] private space, private activities, and private information that he [or she] does not want to be known to others" and "the information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person" which is the same as the definition under Article 76 of the Cybersecurity Law. It articulates that all privacy information in PI shall apply to provisions on privacy rights. As for PI that does not relate to privacy, the Civil Code generally reaffirms the overarching protection scheme under the Cybersecurity Law, but has also made a few significant changes.

The Civil Code expands the legal basis of processing PI compared to the only legal basis under the Cybersecurity Law, namely consent by PI subjects and prescription by laws or regulations; The Cybersecurity Law does not contextually contemplate this legal basis, but such interpretation is inferred from the Cybersecurity Law entirely and is widely accepted in practice. Specifically, Article 1035 of the Civil Code provides the legal basis of processing PI, such as consent by the natural person or his or her guardian and prescription by laws or regulations, and Article 1036 prescribes the exemptions of civil liability for processing PI, such as reasonably processing PI publicly disclosed by the natural person or by other legal means, or reasonable acts to protect the public interest or the lawful rights and interests of the natural person.

It is worth mentioning that the Civil Code provides heightened and special protection for PI related to privacy. Article 1033 of the Civil Code specifically provides that no entity or person shall process privacy information or conduct actions that infringe privacy rights without express consent by the right-holder or unless otherwise prescribed by laws (without mentioning "by regulations"), which is more restrictive than the legal basis of processing generic PI under Article 1035 of the Civil Code and the exemptions of liability under Article 1036.

The Civil Code generally refers to any entity or individual processing PI as the "PI processor", as opposed to the dichotomy of PI controller and entrusted processor (PI processer) adopted

by the national standards Information Security Technology – Personal Information Specification ("Personal Specification"). Therefore, it is possible that PI subjects may have a greater scope of claims to entrusted processors under the Civil Code than under the previous GDPR-like controller/processor dichotomy adopted by the Personal Specification.

The Civil Code emphasises the confidentiality obligation of government agencies and their employees when performing legal duties under laws and regulations.

In sum, the Civil Code affirms the principles of protecting PI from the perspective of the PRC's foundational law of civil rights, and has sufficiently paved the way for future PI regulation by setting forth a legal basis of PI processing that is even broader than the Cybersecurity Law. The affirmation of PI rights in the Civil Code implies great potential for future civil litigation related to PI rights. There has been some exploration in public interest civil actions regarding PI protection in the past two years, and in January 2021 the Hangzhou Internet Court released the first decision in the country that applies the PI protection provisions of the Civil Code in public interests civil actions. As such, enterprises are advised to pay close attention to the developing trend of civil litigation related to PI rights.

The Draft Personal Information Protection Law

The Draft Personal Information Protection Law (Draft PIPL), released in October 2020, further demonstrates the legislators' determination to promote PI protection. In essence, the Draft PIPL aims to work as an independent legislature specifically focused on PI protection and suggests a number of significant changes to the current PI protection regime articulated by the Cybersecurity Law and the PI Specification, as follows.

The Draft PIPL contemplates extra-territorial jurisdiction over offshore processing of the PI of natural persons within the PRC if the action is intended to provide goods or services to such person or to access the behaviour of such person. This illustrates the legislation's response to the trend of extraterritorial jurisdiction worldwide, such as the GDPR and the CCPA, to afford PI subjects within the PRC equal protection. If the Draft PIPL is enacted as is, foreign enterprises that are without PRC presence but relevant to PI subjects in the PRC – such as the services provided to PRC users via offshore servers – are likely to be subject to the PIPL.

The Draft PIPL changes the terminology of the participants of PI processing compared to the current one established by the PI Specification. In particular, it lines up with the terminology of the Civil Code, and defines the entity or individual capable of determining the purpose and methods of PI processing as the "PI processor", to replace the term of "PI controller" under the PI Specification (which is comparable to "data controller" under the GDPR). In addition, the "entrusted PI processor" under the Draft PIPL is comparable to "data processor" in the GDPR. While the changes do not extend to the definitions of the terms, the Draft PIPL prescribes obligations arising from "data processing" and thus it opens the possibility of some obligations traditionally assigned to data controllers being interpreted to apply to "entrusted PI processors".

The Draft PIPL introduces additional legal bases of processing PI, in addition to consent by subjects and prescription by laws or regulations, such as the necessity for executing or performing a PI subject's contracts, protection of public health in emergency, and certain reasonable acts for public interests. It is a drastic expansion from the Cybersecurity Law's framework and grants enterprises much more flexibility.

The Draft PIPL also introduces the first attempt to regulate PI cross-border transfer by general entities at the statute level, compared to the cross-border transfer provisions applicable to critical information infrastructure operators (CIIOs) in the Cybersecurity Law. Specifically, it extends the scope of data localisation and mandatory security assessment for outbound PI transfer, previously only applied to transfer conducted by CIIOs, to mass-volume PI processors (identification standards to be further specified); for transfer conducted by other entities, it also provides several new approaches of compliant outbound PI transfer as compared to the sole approach of security assessment under the current cross-border security transfer rules. In general, for foreign enterprises processing large volume of user data, it may incur legal risks to provide service to PRC users without deploying the server within the PRC if the Draft PIPL is enacted as is. It also requires PI processors to obtain independent consent from PI subjects.

The Draft PIPL introduces several significant changes to the current PI protection regime, such as more complicated requirements for obtaining consents, joint and several liabilities for joint PI processors, much higher liability for violation, further restrictions on government authorities processing PI, and others.

In sum, the Draft PIPL reflects the legislation's attitudes and objectives in PI protection that elevates requirements for PI protection while endeavouring to strike a nuanced balance between PI rights and market participants' interests in processing PI data in the evolving era of digital economy. As such, while the Draft PIPL is still subject to revision before finalisation, it is still highly valuable in guiding enterprises' compliance strategies.

The Draft Data Security Law

The Draft Data Security Law (Draft DSL) released in July 2020 represent the legislation's first effort at the state level to regulate data activities, such as data collection, storage, processing, usage, provision, transaction and disclosure in order to protect state security, public interests and private interests. The highlights of the Draft DSL include the following.

Similar to the Draft PIPL, the Draft DSL contemplates extraterritorial jurisdiction over offshore data activities affecting state security, public interests and private interests within the PRC.

It contemplates a general principle of data categorisation and classification based on the importance of data and the damage incurred upon data breach. However, currently there are no categorisation and classification standards applicable to data in general, but there are some finalised or draft national and industry standards for certain specific sectors, such as finance and healthcare.

The Draft DSL requires governments at different levels to issue catalogues of important data to identify and provide heightened protection to such important data, including periodical risk assessment.

It contemplates a data security review system for data activities that may affect state security. The Draft DSL only discusses the security review system generally and is pending further implementation measures. While there are already some regulations applicable to security review for specific cybersecurity areas – for example, the Measures for Cybersecurity Review, issued by the Cybersecurity Administration of China (CAC) in April 2020, applies to CIIOs procuring network products and services – the Draft DSL is the first attempt at statute level to contemplate

a general security review mechanism for data activities.

Other important highlights include reciprocal measures against countries adopting data-related discriminative measures against the PRC, encouragement of data transaction, governmental data opening and protection, obligations to co-operate with enforcement action, punitive damage for violation.

While the Draft DSL is still subject to future changes, this draft represents a clear indication of the state's increasing efforts to protect data as a competition resource at a national strategic level, and state security and public interests becoming even more important factors in data regulation.

Promoting Protection of the Critical Information Infrastructure

On 22 July 2020, the Ministry of Public Security (MPS) issued the Practical Guide to the Multi-level Protection Scheme and Critical Information Infrastructure Security Protection System ("Practical Guide") to all ministries and commissions of the central and state organs, all agencies, offices and institutions directly under the State Council, and all central enterprises, with the aim of constructing a comprehensive defence system for the national network's security by emphasising the significance of the protection of the critical information infrastructure (CII), important networks and data security.

The Practical Guide is expected to be the essential working paper that directs supervisory departments in CII protection in 2021. Furthermore, the importance of CII protection is also highlighted by the State Council's Legislation Work Plan of Year 2020 (released on 26 June 2020), which lists the Regulations on CII protection within the legislation plan.

For the identification of the CII, the Practical Guide stipulates that competent authorities and supervisory departments of each important industry and sector – including public telecommunications and information, energy, transportation, water conservation, finance, public services, e-government, national defence, etc – shall: (i) formulate the CII identification rule within the respective industry and file with the MPS; and (ii) organise the CII identification work at industry level and report the results to the MPS. Meanwhile, the Practical Guide further states that the CII list shall be adjusted dynamically and relevant operators may apply for the re-identification of CII if there are major changes in network infrastructure and information system.

In line with the Practical Guide, the National Information Security Standardisation Technical Committee (TC260) is in the process of formulating a series of initiatives supporting the national standard on CII. The proposed system covers different topics, ranging from the basic terms and framework of CII protection to the identification, security, monitoring and warning, testing and evaluation, and incident handling of CII. It is noted that the national standards for each topic are already drafted and are under review or released for public comments. Since the national standard always serves as implementing guidelines to PRC laws and regulations in practice, we understand that the finalisation of CII national standards will support the supplementation of the laws and regulations on CII protection and promote relevant supervisory works.

In addition to the development of CII-related national standards, important industries and sectors also witnessed regulatory efforts in the management of CII. Taking the transportation sector for example, the Ministry of Transport has made preliminary progress in identifying critical services in the transportation sector and aims to establish the CII identification mechanism.

Furthermore, the Practical Guide also provides the regulatory focus on CII protection and emphasises that CII operators shall undertake multi-level assessment for their networks and reinforce the CII protection in accordance with relevant standards. Specifically, the Practical Guide draws attention to the use of new technology in CII protection, including cryptographic technology, trustworthy computing, artificial intelligence, and big data.

As illustrated above, regulatory departments led by the MPS will continue to strengthen the regulation on CII protection. Network operators are advised to closely monitor the legislative and regulatory trends at both industrial and national levels, and to take immediate actions in complying with corresponding cybersecurity responsibilities.

Dynamic Cybersecurity Law Enforcement Activities

In the course of 2020, there were a number of dynamic cybersecurity law enforcement activities led by multiple regulatory departments, including the CAC, MPS, the Ministry of Industry and Information Technology (MIIT), as well as local cyberspace departments, and industrial supervisory departments such as the People's Bank of China (PBOC) and the Department of Education.

One recent significant administrative penalty was the hefty fine of CNY4.2 million imposed on the Agricultural Bank of China (ABC) by the China Banking and Insurance Regulatory Commission (CBIRC) on 19 January 2021. According to the public information on the CBIRC's official website, CBIRC determined that ABC breached the relevant rule of prudent operation under the PRC Banking Supervision Law in illegalities concerning the following:

- an unreported important information system incident;
- failure to retain card production data in clear text;
- inadequate protection of the bank's production network and wireless networks at branches;
- poor data security management with data leakage risks;
- network vulnerabilities in network information system; and
- leakage of sensitive information through the bank's internet portal.

It is foreseeable that various supervisory departments from all sectors and at all levels will participate in the law enforcement activities in cybersecurity protection. Enterprises are advised to value and prioritise the task in building and upgrading the internal management of their cybersecurity systems according to relevant PRC laws, including the Cybersecurity Law and the upcoming Personal Information Protection Law and Data Security Law, as well as corresponding implementing measures.

Overall, with the trend in societal digitalisation and societal transformation, China is introducing fundamental laws, regulations and relevant national standards on multiple topics concerning personal information protection, data security, CII protection, etc, as well as engaging in dynamic law enforcement activities on cybersecurity. As such, enterprises should prepare in advance for the new compliance tasks in building and reforming their internal cybersecurity mechanisms.

Contributed by: *Susan Ning and Han Wu,* ***King & Wood Mallesons***

King & Wood Mallesons is an international law firm headquartered in Asia with a global network of 27 international offices. KWM's cybersecurity team is one of the first legal service teams to provide professional services concerning cybersecurity and data compliance in China; it consists of more than ten lawyers with solid interdisciplinary backgrounds, mainly located in Beijing, while further specialisms are found within KWM's global network. The team has expertise in assisting clients in responding to cybersecurity inspections and network emergencies, establishment of network information compliance system, self-assessment, internal training on cybersecurity and data compliance, and other related matters. Recently, KWM advised a renowned short-term lodging platform on compliance with the multi-level protection of cybersecurity, during which KWM provided elaborative analysis on the current graded protection obligations and further comparatively analysed the newly proposed mechanism and the existing one, thereby enabling it to offer practical advice to the client.

AUTHORS

Susan Ning is a senior partner and the head of the regulatory group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals, such as the "Journal of Cyber Affairs". Her publications include "Big Data: Success Comes Down to Solid Compliance", and "No 'Data', No 'Internet of Vehicles'". Susan's practice areas cover self-assessment of network security, responding to network security checks, data compliance training, etc. She has assisted companies in sectors such as IT, transportation and finance in dealing with network security and data compliance issues.

Han Wu is a partner of the commercial and regulatory group. He excels in providing cybersecurity and data compliance advice to multinationals' Chinese branches and in establishing network security and data compliance systems for Chinese enterprises operating abroad. In the areas of cybersecurity and data compliance, Han provides legal services, including assisting clients in establishing a cybersecurity compliance system, self-investigation on cybersecurity, network security investigations, cybersecurity incidents, data fusion and identification of data assets. Han has provided legal services on cybersecurity and data compliance to companies in multiple industries. The projects he has participated in encompass the financial payment, consumer electronics, internet advertising and healthcare industries.

Contributed by: *Susan Ning and Han Wu,* ***King & Wood Mallesons***

King & Wood Mallesons

18th Floor, East Tower, World Financial Center
1 Dongsanhuan Zhonglu
Chaoyang District
Beijing
100020, PRC

Tel: +86 10 5878 5588
Fax: +86 10 5878 5566
Email: kwm@cn.kwm.com
Web: www.kwm.com