Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

TMT
2022

China: Law & Practice
and
China: Trends & Developments

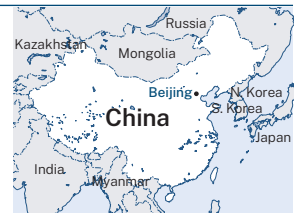
Cloud Li, Joanna Jiang and Dimitri Phillips
DaHui Lawyers

practiceguides.chambers.com

CHINA

Law and Practice

Contributed by:
Cloud Li, Joanna Jiang and Dimitri Phillips
DaHui Lawyers see p.18



CONTENTS

1. CLOUD COMPUTING

1.1 Laws and Regulations

There are no laws and only a few legal regulations in the PRC relating specifically to cloud computing, but cloud computing service providers are subject to various general bodies of legislation and regulation, including the following:

- the Telecommunications Regulations of the People's Republic of China and related regulation, such as the Administrative Measures for the Licensing of Telecommunications Business and the Administrative Measures for Internet Information Services (see **8.1 Scope of Telecommunications Rules and Approval Requirements**);
- the Cybersecurity Law of the People's Republic of China (see **6.1 Core Rules for Individual/Company Data**) and related laws and regulations forming the framework for governing data security and privacy protection in China (Cybersecurity Regime), including the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China (PI Protection Law), the Critical Information Infrastructure Security Protection Regulations (CII Regulations) and Measures for Cybersecurity Reviews;
- the Cryptography Law of the People's Republic of China; and
- the Measures for Security Evaluation for Cloud Computing Services (Cloud Computing Security Evaluation Measures).

The Standardisation Administration of China (SAC) also publishes numerous non-binding recommended standards relating to cloud computing, covering topics ranging from security guidance to data centre requirements and file service application interfaces.

Heightened Scrutiny on Critical Information Infrastructure Operators

The Cybersecurity Law, the Data Security Law and the CII Regulations and Measures for Cybersecurity Reviews all set out obligations on Critical Information Infrastructure Operators (CIIOs – see **6.1 Core Rules for Individual/Company Data** for more details), which are defined broadly to include companies whose business involves significant issues for PRC national security, the national economy, social well-being or other public interests. There is no express law or regulation in effect currently specifying that offering, let alone using, cloud services is a category of Critical Information Infrastructure (CII), but the scale and importance of some cloud computing operators could conceivably lead to them falling within this categorisation.

Subject to the specific data stored or processed on a cloud computing service or the party to which the cloud computing services are provided, a cloud computing service provider could be required to comply with various obligations under the Cybersecurity Law, the Data Security Law and the CII Regulations, such as local data hosting and offshore data transfer restrictions, or the Cloud Computing Security Evaluation Measures (see further below). Ultimately, in such a scenario, a cloud computing network with offshore components (eg, servers hosted outside China, or networks between a PRC subsidiary and foreign parent company) might have to restructure its entities or operations to comply with these laws and regulations.

Even if a business does not fall within the categorisation of CIIO solely for offering (or using) cloud computing services, it may do so because of an industry in which it operates or other characteristics, if significant issues of PRC national security, the national economy, social well-being or other public interests are implicated. Areas in

which a substantial number of businesses are likely to be deemed CIIOs include the following:

- public telecommunication and information services;
- energy resources;
- transportation;
- finance;
- public services;
- science; and
- technology for national defence.

Such businesses, and therefore any cloud computing services in which they are involved, would be subject to greater restrictions, such as the Measures for Cybersecurity Reviews.

Cybersecurity Reviews for Procurement of Cloud Computing

The Measures for Cybersecurity Reviews provide that any CIIO seeking to procure any network product or service that affects or may affect national security needs to undergo a so-called "cybersecurity review". Cloud computing products and services (as well as high-performance computers or servers, mass storage equipment, large databases or applications and network security equipment) are specifically included in the scope of network products that are subject to the Measures for Cybersecurity Reviews. Therefore, any CIIO procuring cloud computing products or services that may affect national security will need to go through a process that may include an application for cybersecurity review being submitted to the Cybersecurity Review Office (CRO), an initial review by the CRO and potentially a "special review" by the CRO if no agreement can be reached by CRO members after the initial review.

Moreover, under the revised Measures for Cybersecurity Review, which were issued on 28 December 2021 and will take effect on 15 February 2022, cybersecurity review now applies not only to CIIOs procuring any network product or service that affects or may affect state security, but also to:

- any data processor that carries out any data processing activities that affect or may affect issues of national security, even if such parties are not CIIOs; and
- any company that has the personal information (PI) of more than one million users and intends to conduct a stock listing outside the country.

Cloud Computing Security Evaluations

The Cloud Computing Security Evaluation Measures provide that cloud computing service providers supplying to the Communist Party of China (CPC), the government or any CIIO may complete a security evaluation of each of their cloud computing platforms providing such services. The evaluation result can be used as a reference to support a supplier's bid for procurement contracts for cloud computing services for the CPC, government bodies and CIIOs. The evaluation may cover the following:

- the credit and operation status of the cloud service supplier;
- the stability of the cloud service supplier's personnel;
- the security of the technologies, products and service supply chains of the cloud platforms;
- the security management capability of the cloud service supplier and the security protection of the cloud platforms;
- the feasibility and convenience of customer data migration; and
- the business continuity of the cloud service supplier.

Personal Information Protection Obligations

Cloud computing service providers generally must comply with the requirements of the

Cybersecurity Regime in respect of the collection and use of PI.

Since 2017, PI protection has been subject to regulation primarily by the Cybersecurity Law (supplemented by a number of national standards, including the Information Security Technology – Personal Information Security Specification (Specification) and the Information Security Technology – Guideline for Personal Information Protection within Information Systems for Public and Commercial Services). Key requirements on parties, including cloud computing service providers, include obtaining consent from data subjects for the collection and further uses of their PI, undergoing so-called "security assessment" procedures prior to overseas data transfers in certain circumstances (see **10.1 Legal Requirements and Exemptions**) and such further general principles as "legitimacy, rightfulness and necessity" in the collection and use of PI. The Consumer Protection Law of the People's Republic of China sets similar requirements on the collection of consumer information by business operators. Other high-level laws provide general privacy protections – eg, the Tort Law of the People's Republic of China, the Civil Code of the People's Republic of China and the Criminal Law of the People's Republic of China.

In 2021, the Cybersecurity Regime was subject to many clarifications and additions, primarily from the passing and coming into effect of the Data Security Law and the PI Protection Law. Taken together, they significantly heighten the restrictions, requirements and potential liability to which "data processors" (inside and ostensibly to a certain extent outside China) would be subject. They define "data" and "personal information" broadly as "any record of information in electronic or other form" and "all kinds of information recorded by electronic or other means related to identified or identifiable natural persons", respectively. They impose preconditions on transfers of PI and even more general data in various circumstances, especially cross-border transfers. Moreover, PI can be processed – in any way – only if:

- consent has been obtained from the individual whose PI is processed (PI Subject);
- the processing is necessary for the conclusion or performance of a contract to which the PI Subject is a party;
- it is necessary for the performance of legally prescribed duties or obligations;
- it is necessary for responding to public health incidents or protecting natural persons' lives, health or property in an emergency;
- it is necessary for carrying out acts such as news reporting and public opinion oversight in the public interest; or
- it is done, for carrying out activities permitted under the PI Protection Law, on PI that has been voluntarily disclosed by PI Subjects or otherwise disclosed legally.

Cloud computing service providers must now comply with all of the above in all their processing of PI.

2. BLOCKCHAIN

2.1 Legal Considerations

Blockchain technologies are generally permitted and even encouraged in China, except in the cryptocurrencies sector. Developing blockchain was identified as one of the core aims more than five years ago, in the PRC government's 13th Five-Year Plan. The 14th Five-Year Plan, released by the China Communist Party Central Committee on 29 October 2020, did not specifically mention blockchain technology, but actually emphasised the research and development of digital currency and fintech. While China's Central Bank Digital Currency (CBDC) is currently not based on blockchain technology,

fintech is among the most important functions of blockchain technology.

Blockchain Activities Generally

In the last few years, 12 authorities (including the Ministry of Commerce) have published guiding opinions on the promotion and development of blockchain for use in commodity trading markets. In addition, with the growth of mobile payments and online banking, the People's Bank of China (PBOC) has developed a new consumer credit rating system that employs blockchain technology and is used to monitor the wealth and debt of individuals (including household borrowing and utility bills) to give banks or third parties a more comprehensive picture of an individual's financial position and their credit risk so that systemic risks can be better controlled.

The Provisions on Administration of Blockchain-based Information Services (Blockchain Services Provisions), issued by the Cyberspace Administration of China (CAC) on 10 January 2019, represent the first administrative guidelines for providers of non-cryptocurrency, blockchain-based services in China. The Blockchain Services Provisions define blockchain-based service providers as entities or nodes that provide blockchain-based information services, or any institution or organisation that provides technological support to such entities (Blockchain Service Providers). Under the Blockchain Services Provisions, Blockchain Service Providers are responsible for information security and should build internal management systems for user registration, information censorship, emergency responses and security protection. The Blockchain Services Provisions require Blockchain Service Providers to conduct a record-filing with the CAC or its provincial-level branch to report certain key information, such as the type and scope of services, application sectors and server addresses, within ten business days of launching their services. Blockchain Service Providers are also required to undertake a security evaluation administered by the CAC or its provincial branches, and to authenticate the identities of their users based on ID card numbers, organisational codes (for PRC entities) or mobile phone numbers before providing services to such users, in accordance with the Cybersecurity Law.

The CAC has publicly released lists showing there were a total of 1,440 registered blockchain information services projects as of 9 November 2021.

Cryptocurrencies

On the other hand, the Chinese government continues to take a hard line against private cryptocurrencies and initial coin offerings (ICOs). The regulators have had an outright ban on cryptocurrency exchanges and ICOs in China since 2017, and have also imposed severe restrictions on the use of cryptocurrencies and relevant trading services. Since then, at times, both the PBOC and a government group on internet financial risk rectification have announced crackdowns on cryptocurrency and illegal blockchain activities. Although some market players have continued to conduct limited cryptocurrency operations in China, these actions continue to attract increased government scrutiny, with regulators vowing to impose additional restrictions and strengthened monitoring of cryptocurrency-related activities. In the judiciary, claims on or related to cryptocurrency are usually dismissed on the grounds that it is not recognised as having any legal or economic value or even existence.

However, the PBOC has started a trial utilisation of the CBDC in a number of cities and regions in China, as its own contribution to the growing world of digital currencies. Pilot schemes for Digital Currency Electronic Payments (DCEP) have been running in various parts of China, including the Greater Bay Area, the Beijing-

Tianjin-Hebei region and the Yangtze River Delta region, and are set to continue through the 2022 Beijing Winter Olympics. Up to 30 June 2021, there were more than 1.32 million pilot scenarios for digital renminbi, with more than 20.87 million personal account wallets and 3.51 million public account wallets opened, yielding a total number of 70.75 million transactions, amounting to a total of RMB34.5 billion.

Intellectual Property Protection for Blockchain

A blockchain-based application will typically be in the form of computer software, which may make it subject to copyright protection under PRC law. If the application is sufficiently sophisticated (eg, if it includes sufficient technical elements in addition to being mere computer algorithms or business methods) and constitutes a solution to a technological problem, then it could be considered patentable under China's patent law. That said, many blockchain technologies are based, at least partially, on open-source software, which will generally be governed by the terms of an open-source licence that may impose restrictions on patent applications, or may contain provisions undermining patent enforcement.

Data Privacy

There are no PRC rules on data privacy that relate to blockchain technologies specifically. However, an operator of blockchain services would be subject to various other PRC laws and regulations relating to data privacy, such as under the Cybersecurity Regime (see, generally, **1.1 Laws and Regulations** and **6.1 Core Rules for Individual/Company Data**).

As such, Blockchain Service Providers (and other operators of blockchain technologies) must comply with privacy protection requirements under the PI Protection Law, including but not limited to obtaining consent before collecting PI from users (except for certain legally allowed situations) and disclosing rules for PI collection, the intended use of such information, its purpose and the means and scope of collection.

Blockchain Service Providers who are engaged in certain industries could be deemed to be operating CII and therefore subject to more strict obligations under the Cybersecurity Regime. For example, for some operators of blockchain services, the PI or other information constituting important data collected within mainland China through their blockchains would be required to be stored in China – it could not be transferred outside China without undergoing additional security assessment procedures. Ultimately, all the nodes of such blockchains may have to be located within China as well.

Service Levels

Currently, there are no specific PRC laws or regulations on any service levels or service-level agreements (SLAs) for an operator of blockchain services. That said, the SAC and the China National Information Technology Standardisation Committee (CNITSC) have issued a number of recommended national standards and industry standards on SLAs for cloud computing. While none of these standards are compulsory, an increasing number of Chinese internet and software service providers appear to be adopting SLAs. As such, SLAs are expected to evolve primarily in light of technical and commercial considerations between Blockchain Service Providers and users.

Jurisdictional Issues

Because the nodes of a blockchain could potentially be dispersed across servers located in multiple countries and jurisdictions, the question of which laws the blockchain will be subject to is complicated and has not been specifically addressed by PRC law. Under current PRC law and in the absence of an agreement among rel-

evant blockchain parties on governing law and forum selection, whether or not a blockchain is subject to PRC law will be governed by standard PRC choice-of-law and forum selection rules under the Civil Procedure Law of the People's Republic of China and the Law of the People's Republic of China on the Application of Laws to Foreign-Related Civil Relationships. Even under these laws uncertainties remain, such as whether having a single blockchain node located on a server in the PRC will be sufficient to subject the entire blockchain to PRC jurisdiction, or whether something more is required.

3. LEGAL CONSIDERATIONS FOR BIG DATA, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

3.1 Challenges and Solutions

Big Data

Currently, there are restrictions on foreign investment into big data companies. The Telecommunications Business Catalogue published in 2015 by the Ministry of Industry and Information Technology (MIIT) lists the operation of an internet data centre (IDC) as a business that requires a value-added telecommunications operating permit. Subject to certain limited exceptions, this permit cannot be obtained by a foreign-invested entity. Therefore, foreign entities are generally required to outsource their data storage and data analysis services to local PRC IDCs. As a notable example, since 28 February 2018, the Apple iCloud service in mainland China (which formerly operated via an offshore service provider) has been transferred to and operated by Guizhou-Cloud Big Data Industry Development Company, a PRC IDC.

Beyond these restrictions on foreign investment, there are no laws or regulations in the PRC specifically applicable to "big data" companies or providers of big data and related services, such as big data analytics and consulting services. As such, there are no statutory limitations or allocations of liability or insurance requirements applicable to duly established big data companies.

Generally, big data companies are subject to the requirements of the Cybersecurity Regime and data privacy laws, except in certain circumstances (eg, to the extent PI is required for contract performance), such as informed consent must be procured from users or data subjects before a company can collect and process their PI. The PI Protection Law provides that a "security assessment" is required for a cross-border transfer of PI exceeding certain thresholds. CAC draft measures set out the following thresholds:

- any cross-border transfer of PI by any data processor that processes PI from more than one million data subjects; and
- any cross-border transfer of PI that concerns more than 100,000 data subjects (on a cumulative basis), or of "sensitive personal information" that concerns more than 10,000 data subjects (on a cumulative basis).

A company engaging in business related to big data in certain industry sectors might be subject to additional regulatory requirements. For example, health-related data must be stored on a secure and trusted server in China; hospital authorisation is required to collect and process such data (even anonymised), and a security assessment is required before transferring such data offshore. Finally, a big data service provider may be deemed a CIIO and therefore subject to stricter compliance requirements, including the requirement to store all PI and other important data within the PRC and the restrictions on transmitting such data outside the PRC without performing certain security assessment procedures.

Machine Learning

There are no PRC laws or regulations specifically pertaining to the creation, development or use of machine learning algorithms or technologies. As such, there are no rules specifically addressing the allocation of liability or setting insurance requirements on companies that provide products or services employing machine learning algorithms or technology.

As the operation of machine learning algorithms tends to require large data sets, service providers obtaining such data will be subject to the requirements of the Cybersecurity Regime and privacy protection laws, including but not limited to obtaining consent before collecting PI from users (except for certain legally allowed situations), and disclosing rules for PI collection, the intended use of such information, its purpose and the means and scope of collection.

A software program employing machine learning technology is likely to be subject to copyright protections under PRC law. However, machine learning algorithms themselves will be very difficult to patent in the PRC. Moreover, any machine learning software that is based on open-source software will generally be governed by the terms of an open-source licence, which may impose restrictions on patent applications or contain provisions undermining patent enforcement.

Artificial Intelligence

There are no PRC laws or regulations specifically pertaining to the creation, development or use of artificial intelligence (AI). As such, there are no rules specifically addressing the allocation of liability or setting insurance requirements for companies that provide products or services employing AI.

As the operation of AI tends to require large data sets, service providers obtaining such data will be subject to the requirements of the Cybersecurity Law and privacy protection, including but not limited to obtaining consent before collecting PI from users (except for certain legally allowed situations), and disclosing rules for PI collection, the intended use of such information, its purpose and the means and scope of collection. Under draft rules, if "sensitive personal information" (eg, facial information) is processed, more strict requirements would apply – for example, biological characteristics (eg, fingerprints, faces, voices, gaits) could not be used as the sole method for personal ID verification, and, when they are used, the data processor would be required to conduct a risk assessment on the necessity and safety of the use, and would be prohibited from requesting the natural person to agree on facial information processing as a precondition to using products or services where the facial information is not necessary for their provision.

With respect to the ownership of intellectual property rights, under the Copyright Law of the People's Republic of China, only natural persons, legal persons or organisations can be entitled to copyright. As a result, PRC law currently appears to suggest that any works and content created by AI cannot be protected by copyright, though in theory discoveries and inventions by AI might be patentable if a natural person, legal person or organisation could be shown to have the right to the patent rights.

4. LEGAL CONSIDERATIONS FOR INTERNET OF THINGS PROJECTS

4.1 Restrictions on a Project's Scope

Chinese legislators have taken a relatively broad view of the concept of the internet of things (IoT). The Guiding Opinions of the State Council on Promoting the Orderly and Healthy Development

of Internet of Things (IoT Opinion) describes IoT as technologies "based on the intensive integration and comprehensive application of a new generation of information technology", and designates IoT as an important strategic emerging industry of the country. The IoT Opinion further emphasises the co-ordinated overall development of IoT applications, technologies, industries and standards.

Although China has yet to promulgate any comprehensive legislation on the security and regulation of IoT, recent legislation on IoT-related issues – such as data security and privacy, cloud computing, protection of critical infrastructure, and network products more generally – is all applicable to IoT, and a number of different government departments and regulatory bodies have been involved in the regulation and standardisation of the IoT sector. These government bodies include the MIIT (the key regulator for the telecoms sector and approximately 20 other industries), the CAC (which acts as the main watchdog for information security and content administration), the NDRC, the Ministry of Science and Technology (MOST), the SAC and others.

While there is no specific law on the information security of IoT, many if not most of the rules of the Cybersecurity Regime are generally applicable to the IoT sector – particularly the rules regarding the confidentiality and safekeeping of consumers' PI and the protection of privacy (see **1.1 Laws and Regulations** and **6.1 Core Rules for Individual/Company Data**). Accordingly, if an IoT service provider is deemed to be operating CII, then it will be subject to more stringent compliance requirements.

5. CHALLENGES WITH IT SERVICE AGREEMENTS

5.1 Legal Framework Features

By and large, the PRC legal framework concerning IT service agreements presents many of the common aspects found in other jurisdictions. In particular, provisions dealing with indemnification and liability caps for data breaches, service outages and other service malfunctions tend to be among the most heavily negotiated clauses of IT service agreements in China. Another routinely contested contractual point concerns a service provider's reporting obligations to its customers in the event that it discovers breaches, attempted intrusions, actual intrusions and data leaks. Maintenance timetables and service-level credits are also potential matters of discussion, as is IP ownership of customised software applications.

Taken together, these general issues of IT service agreements tend to be deal-specific, and their resolution is often subject to the risk profiles of the parties involved. It is worth noting that the Civil Code entered into effect on 1 January 2021, rendering a number of laws obsolete, such as the Contract Law of the People's Republic of China. The Civil Code will also govern IT service agreements, although no significant changes to existing and prevailing contractual arrangements for such agreements are expected.

Furthermore, for cross-border IT agreements, parties would do well to look into the Catalogue of Technologies Prohibited or Restricted from Export and the Catalogue of Technologies Prohibited or Restricted from Import to determine if the technologies involved are prohibited or require pre-approval.

There are no sector-specific rules on IT service agreements, aside from those generally governing the cloud computing/data privacy sectors

(see **1.1 Laws and Regulations** and **6.1 Core Rules for Individual/Company Data**).

6. KEY DATA PROTECTION PRINCIPLES

6.1 Core Rules for Individual/Company Data

Core Rules Regarding Data Protection

The Cybersecurity Law is the first PRC law that systematically lays out the regulatory requirements on cybersecurity and data protection, subjecting many previously under-regulated or unregulated activities in cyberspace to government scrutiny. After the Cybersecurity Law, China issued and released other laws and regulations aiming to improve the data protection regime in China. The following significant legislative developments in data protection occurred in 2021.

- The PRC Data Security Law was promulgated on 10 June 2021 and took effect on 1 September 2021. It sets forth the data security protection obligations for entities and individuals. For example, it prohibits entities and individuals not only from acquiring data by theft or other illegal means but also from collecting and using data in excess of the necessary limits.
- The CII Security Regulations were promulgated on 17 August 2021 and took effect on 1 September 2021. They consist of implementation rules concerning security requirements for CIIOs and heightened requirements regarding how CII must be protected in China. The CII Security Regulations do not specify or list CIIOs, but provide that industrial regulators will be responsible for formulating rules for, and undertaking, determinations of what constitutes CII in their industries.
- The PI Protection Law was promulgated on 20 August 2021 and became effective on 1 November 2021. It provides a comprehensive set of data privacy and protection requirements that apply to the processing of PI, including compliance obligations for organisations and individuals in China as well as those that process PI outside China if such processing is for the purposes of providing products and services to, or analysing and evaluating the behaviour of, persons in China. The PI Protection Law also provides that CIIOs, as well as PI processing entities who process PI amounting to a certain threshold to be set by the CAC, are required to store PI generated or collected in China locally, and to pass a security assessment administered by the CAC for any export of such PI.
- The revised Measures for Cybersecurity Review were issued on 28 December 2021, taking effect on 15 February 2022. Under this legislation, the so-called "cybersecurity review" procedure no longer applies only to CIIOs but also to any party whose data processing activities affect or may affect issues of national security, even if such party is not a CIIO, and to any company that has the PI of more than one million mainland China users and intends to conduct a stock listing outside the country.

Distinction between Companies/Individuals

The Cybersecurity Law and other data security and privacy protection laws and regulations do not make a technical distinction between companies and individuals. However, they do contain other important distinctions – eg, at the level of data processors (typically companies) and at the level of data itself (typically belonging to consumers/individuals).

At the data processor level, the Cybersecurity Law distinguishes between "Network Operators" and the narrower concept of CIIOs. Network Operators are broadly defined as "network owners and administrators, and network ser-

vice providers". As no further definition of these sub-categories is provided, this definition could potentially include any company or individual operating a website or using a company intranet/cloud computing network. CIIOs, on the other hand, are defined to include certain companies that are heavily connected to industries implicating PRC sovereignty or national economy, or the well-being of PRC citizens, the collapse of which would likely have an adverse impact on the PRC government or its citizens (eg, major utilities and banks). Different rules and requirements within the Cybersecurity Regime are applicable to Network Operators and CIIOs, with the restrictions placed on the latter tending to be more onerous.

At the level of data itself, the Cybersecurity Regime is focused especially on two particular types of network data: PI and "Important Data". PI is defined under the PI Protection Law as "any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymised." Important Data is technically undefined under the Cybersecurity Law, but subsequent though only draft measures define it as "data that, once leaked, may directly affect national security, economic security, social stability or public health or safety." Taken together, companies processing information that could be considered PI or Important Data over a network should take particular care that they are in full compliance with the components of the Cybersecurity Regime.

General Processing of Data

The Data Security Law provides for data security and privacy obligations on entities and individuals carrying out data activities. It also introduces a data classification and hierarchical protection system based on the importance of data in economic and social development, as well as the degree of harm it will cause to national security, public interests or the legitimate rights and interests of individuals or organisations when such data is tampered with, destroyed, leaked or illegally acquired or used. Appropriate levels of protective measures are required to be taken for each category of data. For example, a processor of Important Data must designate personnel and a management body responsible for data security, carry out risk assessments for its data processing activities and file risk assessment reports with competent authorities. In addition, the Data Security Law provides for a national security review procedure for data activities that may affect national security, and imposes export restrictions on certain data and information.

If a data processor in China is deemed to be a CIIO, then a series of more stringent data processing rules will be applicable. Most significant to multinational companies, these heightened data processing rules include a local data-hosting requirement, which requires that all Important Data (and PI) collected or maintained during business operations in China is hosted on servers physically located in the PRC. CIIOs are also restricted from transferring Important Data (and PI) offshore without performing certain security assessment procedures. Notably, any data transfers between a PRC subsidiary and its offshore parent company in which the former is deemed to be a CIIO would fall under these local hosting and offshore data transfer restrictions.

Processing of Personal Data

The PI Protection Law provides enhanced requirements for the processing of PI compared to other data, including but not limited to the following:

- the standard for "consent" is notable in that it will likely be a heightened standard of "voluntary and explicit", as opposed to the generic consent so far understood in practice to apply under the Cybersecurity Law;

- more details relating to the data processing are required to be disclosed; and
- PI processors must conduct periodic audits of their PI processing activities and conduct and record PI protection assessments when processing "Sensitive Personal Information", providing PI abroad or providing PI to other PI processors.

A data processor that is a CIIO or whose volume of PI processing reaches a threshold to be specified by the CAC is required to pass a "security assessment" organised by the CAC before transferring PI overseas. Any other data processor transferring PI overseas will likely have to either obtain a PI protection certification from a specialised body designated by the CAC, or execute a standard agreement (to be issued by the CAC) with the overseas party.

Moreover, in any overseas PI transfer, the PI subjects must be notified of the foreign recipient's name and contact method, the purpose, manner and type of PI to be processed, and the ways and procedures through which the PI subject may exercise its rights under the PI Protection Law in relation to the foreign recipient – and specific consent for the overseas transfer is needed.

7. MONITORING AND LIMITING OF EMPLOYEE USE OF COMPUTER RESOURCES

7.1 Key Restrictions

PRC law provides no rules specifically covering the monitoring of employees' use of computer and internet resources owned by their employers. As such, employers are generally permitted to use various means (eg, monitoring software) to monitor and restrict employees' use of company computer resources.

However, the right of privacy has been developing in PRC law, and with its first major explicit instantiation in the recently promulgated Civil Code, challenges may be levied (successfully) in the near future against certain (unreasonable) monitoring. Moreover, if a company collects or otherwise processes employees' PI, the employers are subject to the requirements under the PI Protection Law. For example, employers are not allowed to process PI from employees unless express consent from the employees has been obtained, or unless it is necessary to collect such PI in order to carry out human resources management activities under a legally adopted employment policy. Furthermore, the PI Protection Law provides that any personal image or PI of an individual collected through image capturing or personal identification equipment in a public place can only be used for the purpose of maintaining public security, unless specific consent is obtained from the individual.

8. SCOPE OF TELECOMMUNICATIONS REGIME

8.1 Scope of Telecommunications Rules and Approval Requirements

The Telecommunications Regulations of the People's Republic of China (Telecommunications Regulations) apply to all types of "telecommunications" services. "Telecommunications" is defined broadly as any "act of using wired or wireless electromagnetic or optoelectronic systems to transmit or receive voice, text, data, images or any other form of information."

The Telecommunications Regulations categorise telecommunications services as either "basic telecommunications services" or "value-added telecommunications services", and different operating permits are required to engage in each. Basic telecommunications services

include communications services, public data transmission and public network infrastructure, while value-added telecommunications services consist of call centre services, IDC services, CDN services, VPN services and others. A complete list of services or businesses qualifying as basic telecommunications services and value-added telecommunications services can be found in the Telecommunications Business Catalogue, as first formulated by the MIIT in 2000 and last updated in 2019.

Therefore, depending on the type of telecommunications services being provided, the telecommunications operator will need to obtain either a "Basic Telecommunications Service Operating Permit" or a "Value-Added Telecommunications Services Operating Permit" prior to bringing a service to market. Each permit requires a telecommunications services operator to meet different requirements, as follows.

- Basic Telecommunications Service Operating Permit:
  - (a) the operator must be a legally established company that specialises in basic telecommunications services and in which the state has no less than 51% ownership;
  - (b) a feasibility study and technical plan for the formation of the network must be completed;
  - (c) the operator must have access to funds and specialised personnel commensurate with the business activities to be engaged in;
  - (d) there must be a site and corresponding resources to carry out envisioned business activities;
  - (e) the operator must have the reputation or the capability to provide long-term service to its subscribers; and
  - (f) the operator must comply with other conditions specified by the state.
- Value Added Telecommunications Services Operating Permit:
  - (a) the operator must be a legally established company with a minimum domestic shareholding of no less than 50% for most value-added telecommunication services (except for those fully opened up to foreign investment, such as domestic multi-party communications services and call centres);
  - (b) the operator must have access to funds and specialised personnel commensurate with the proposed business activities;
  - (c) the operator must have the reputation or the capability to provide long-term service to its subscribers; and
  - (d) the operator must comply with other conditions specified by the state.

On 15 October 2020, the MIIT released the Notice on Strengthening Interim and Ex-Post Supervision of Foreign-Invested Telecommunications Enterprises (FITE Notice), which confirms that a separate process for MIIT approval (MIIT FITE Approval) is no longer required for the establishment of foreign-invested telecommunication enterprises (FITEs), and that all the procedures and documents required under the former MIIT FITE Approval application will be integrated into the existing application process for licences of telecoms services. This is yet another easing of foreign-invested enterprises' entry into China's telecoms market, which has been opening up more and more since the country joined the World Trade Organization.

9. AUDIO-VISUAL SERVICES AND VIDEO CHANNELS

9.1 Audio-Visual Service Requirements and Applicability

China does not maintain a unified regulatory regime for all components of the audio-visual media industry as a whole. Instead, industry sub-sectors are regulated separately through a range of different laws and regulations. With respect to audio-visual media, the key areas of regulation include cable broadcasting, online audio-visual services and over-the-top (OTT) services. In general, the broadcasting or online transmission of audio-visual content is highly regulated and in many cases restricted to both foreign and domestic investment.

Cable Broadcasting

Cable broadcasting is highly regulated in the PRC and is not open to foreign participation or even new domestic market entrants. Currently, a broadcasting television station may only be set up and established by central or local government branches, such as the National Radio and Television Administration (NRTA) or the Ministry of Education. The station's establishment will also be subject to the central PRC government's national market plans. No individual or other enterprise or organisation is allowed to set up any broadcasting television station in China.

The most central piece of legislation relating to cable broadcasting – ie, offering traditional cable television channels – is the Administrative Regulations for Radio and Television. All cable broadcasters are required to obtain the following two key permits, among others:

- the "Radio and Television Broadcasting Institution Permit"; and
- the "Radio or Television Programme Production Permit".

PRC law requires applicants for these permits to meet certain requirements, including regarding their location, equipment, technology and personnel, and to complete an application process with the applicable authorities. No application fees are required. As mentioned, however, it is difficult if not impossible for new entities – whether purely domestic or foreign-invested – to obtain either of these permits in China.

Online Audio-Visual Services

Online audio-visual services are primarily regulated through the following legislation:

- the Interim Administrative Provisions on Internet Culture, which is central to the so-called "Internet Culture" sector, regulating online cultural activities;
- the Administrative Measures for the Transmission of Audio-Visual Programs Through the Internet or Other Information Networks;
- the Administrative Regulations on Internet Audio-Visual Program Services; and
- the Administrative Regulations on Audio-Visual Program Services via Private Networks and Targeted Transmission.

To operate an online streaming platform – ie, to provide video on demand (VOD) services, such as Youku (the Chinese YouTube) – the most important operating permits are the "Internet Culture Business Permit" and the "Internet Audio Video Broadcasting Permit" (IAVB Permit). The IAVB Permit requires an application process to be completed with local and central government authorities, while the application for the Internet Culture Business Permit involves only provincial level government authorities. No application fees are required. An applicant for an IAVB Permit must be controlled or wholly owned by one of China's state-owned enterprises (SOEs). Neither the Internet Culture Business Permit nor the IAVB Permit may be obtained by an applicant that has any direct or indirect (on a see-through basis)

foreign investor, although indirect control structures featuring variable-interest-entity structures established before the requirement that the IAVB Permit must be controlled or wholly owned by SOEs are widely used in this sector.

OTT Services

The most important operating permit for providers of OTT Services is the OTT licence. To apply for an OTT licence, a qualified applicant must meet certain requirements, including being controlled by an SOE, along with equipment and personnel requirements. Here too, both local and central government approval are needed. There are no application fees. To date, only 16 OTT licences have been issued.

Contractual Partnerships/Licensing

Directly operating an online video channel in the PRC is highly regulated and requires the procurement of operating licences/permits (ie, an Internet Culture Business Permit and an IAVB Permit/OTT licence) that are generally only available to companies with SOEs as (controlling) shareholders. As such, it is more common for content owners outside China to simply license content to a domestic entity that holds all required permits – eg, the licensing arrangement between iQiyi and Netflix. Such domestic entities will also ensure that licensed content complies with PRC content/censorship requirements, and will potentially self-censor any content that could result in an infringement.

10. ENCRYPTION REQUIREMENTS

10.1 Legal Requirements and Exemptions

The use of certain encryption products is highly regulated in the PRC. While there are some general, affirmative obligations for companies to safeguard/encrypt protected types of data (such as PI and Important Data under the Cybersecurity Law), such companies must always ensure that they remain in compliance with the PRC's more tailored legal provisions on encryption, such as the recent Cryptography Law.

Prior to 2017, the manufacture, distribution and use of commercial encryption products was restricted in China. In 2017, China's State Council and the State Cryptography Administration (SCA) suspended a series of restrictive regulations that made the production and distribution of cryptography products in China subject to a burdensome pre-approval process. The Cryptography Law, promulgated on 26 October 2019 and effective since 1 January 2020, continues this trend by making clear that the state encourages and supports research on cryptography and its applications, as well as the innovation of cryptography science and technology.

The Cryptography Law divides cryptography into different types:

- core cryptography;
- ordinary cryptography; and
- commercial cryptography.

Core and ordinary cryptography are used to protect state secret information; all other cryptography is classified as commercial cryptography. The Cryptography Law sets out different rules and regulations for each type.

The Cryptography Law generally affords national treatment to foreign-invested entities in the research, production, sale, service, import and export of cryptography, and prohibits the forced transfer of proprietary information from commercial cryptography entities. Moreover, the Cryptography Law provides for a testing and certification requirement for commercial cryptography products involving national security, the national economy and the public interest, clarifies that

CIIOs must use commercial cryptography, and stipulates that a national security review must be completed if national security is involved. The SCA is tasked with formulating a list of commercial cryptography involving national security or public interests, which will be subject to an import licensing requirement.

The use of encryption does not exempt an organisation from any specific rules under PRC law. However, in practice, the use of certain encryption products as certified/authorised by Chinese authorities will often satisfy certain obligations to safeguard and protect data under PRC law, such as the provisions applicable to Network Operators under the Cybersecurity Law. In addition, the Cryptography Law requires that any state secret information transmitted by wired or wireless communications is sent using encryption.

The revised Catalogue of Technologies Prohibited or Restricted from Import was issued and became effective on 2 November 2021. Under the Catalogue, the transfer, licensing or even provision of services concerning "data encryption technology employing a key length greater than 256 bits" by a foreign entity to a Chinese party might constitute the import of controlled encryption technology and thereby require an import permit from local authorities.

11. COVID-19

11.1 Pandemic Responses Relevant to the TMT Sector

Although China was the first to be hit by COVID-19, despite initial disruptions the Chinese economy has stabilised over the course of the past two years, particularly in the TMT industry. Perhaps the only TMT sector that has received sector-specific government relief funds is the cinema sector: cinemas in China remained closed until late July 2020, when the National Film Bureau conditionally allowed cinemas to resume business, but they can only operate at up to 75% of their capacity, and seats must remain over 1 metre apart.

That said, the government has provided relief to many small-to-medium sized Chinese companies, including TMT companies, in forms ranging from relief grants and tax rebates/reductions to low-interest loans. Companies are also encouraged to arrange for employees to work from home rather than in-office, and companies in hardship may arrange for employees to take leave with minimum wages to reduce cost. The COVID-19 crisis has not directly led to any changes in TMT-specific rules.

DaHui Lawyers combines in-depth knowledge of China's legal and business landscape with extensive international experience. It has particular strength in new economy industries and complex cross-border transactions. DaHui has become a go-to firm for multinational companies in the highly regulated Chinese technology, media and internet/telecoms sectors, where its expertise has led to it becoming a key adviser and strategist to clients of all types and sizes in China's emerging but challenging market, providing the most effective and solution-oriented services tailored to clients' diversified business needs. The firm's TMT team consists of 13 partners and 63 fee earners.

AUTHORS

Cloud Li is a partner of DaHui Lawyers' TMT practice. He has represented European and North American multinationals, large Chinese state-owned and privately held companies, and numerous private equity funds in various TMT-related M&A, investments, disputes, compliance and general corporate matters. Cloud has acted for some of the largest and most established participants in China's TMT sector.

Joanna Jiang is a partner of DaHui Lawyers' corporate and TMT teams. She focuses on advising businesses in the information technology and telecoms, media, entertainment and healthcare industries on market entry as well as regulatory and transactional matters. Joanna has deep and extensive expertise in data and privacy protection, especially assisting clients to understand current and potential future requirements and risks, developing and helping to implement localised data compliance guidelines and systems, conducting data compliance due diligence and audits, handling government routine procedures and exceptional inquiries relating to data compliance, etc.

Dimitri Phillips is a member of DaHui Lawyers' dispute resolution, compliance and corporate/M&A practice groups. He handles a range of issues for foreign companies doing or seeking to do business in China, as well as Chinese companies operating abroad. Dimitri has advised clients on litigation, international arbitration, compliance, inbound and outbound investment and general corporate matters.

DaHui Lawyers

China World Tower A
1 Jianguomenwai Avenue
Beijing
100004
China

Tel: +86 10 6535 5888
Fax: +86 10 6535 5899
Email: richard.ma@dahuilawyers.com
Web: www.dahuilawyers.com

Trends and Developments

Contributed by:
Cloud Li, Joanna Jiang and Dimitri Phillips
DaHui Lawyers see p.25

The TMT Sector in China

While 2021 was characterised as the "new normal", after the emergence of COVID-19 and major geopolitical recalibrations, and although uncertainties remain due to variant strains of COVID-19 and other issues, the continuing stability of the economy and society of the People's Republic of China (PRC), as well as a growing domestic market, resulted in strong performance in the TMT sector and a positive outlook. At the same time, China's legislative and regulatory bodies were especially busy in the TMT sector, on the one hand facilitating its further opening up and on the other controlling its growth, particularly with respect to monopolies, data security and protection and online content more generally. The following is a rundown of some of the most notable legislative and regulatory developments of the past year and where they may point for the coming year.

Foreign Investment

The Measures on Foreign Investment Security Review (Security Review Measures), released by China's National Development and Reform Commission (NDRC) and the Ministry of Commerce (MOFCOM), took effect on 18 January 2021. They give the PRC government a powerful and legitimate legal weapon against any foreign investments that have genuine and apparent national security concerns – ie, the security review process on certain foreign investments that may be deemed to have a significant impact on China's national security.

That said, foreign investors making investments in China without significant national security issues or who are otherwise not "important/key" market players in the PRC (eg, non-dominant market players who would not likely trigger PRC anti-monopoly concerns) should not be particularly concerned, at least until further policy or legislative developments indicate otherwise. The potential concern that even insignificant foreign investments into the PRC might have to be reported, or if not reported will be queried and subject to a security review, may be premature, and ultimately turn out to be unrealistic. The Security Review Measures might rather be taken as a sign that, for the foreseeable future, security review will be a precision tool for narrowly targeted specific countermeasures or just a safety net at the central government level to capture particular sensitive foreign investments.

More generally, under the PRC legal and regulatory regime, parts of the PRC economy remain subject to foreign investment restrictions, generally limiting or prohibiting foreign participation in various industry sectors that the PRC government deems sensitive or a matter of national/public security. The Special Administrative Measures for Access of Foreign Investment (Negative List) specifies the maximum foreign shareholding limits applicable to restricted industry sectors. The Negative List is generally updated once a year. On 27 December 2021, the NDRC and MOFCOM jointly issued a 2021 Negative List, which took effect on 1 January 2022. The 2021 Negative List removed two restricted items from the previous edition (bringing the total number of such items down from 33 to 31), including that foreign investors are no longer subject to any restrictions in the production of ground receivers and key components for satellite television broadcasts, having previously been completely prohibited from such production.

Another legislative development, with general application but covering (foreign-invested) TMT businesses, was the 24 December 2021 release of draft revisions to the Company Law of the People's Republic of China (Draft Company Law Revisions), which, if adopted, would affect the corporate governance, potential legal liability faced by directors, supervisors, senior officers and shareholders, processes for liquidation and deregistration, and some other aspects of potentially every kind of PRC company (including foreign-invested ones). For example, the Draft Company Law Revisions impose a requirement that companies with 300 or more employees have an employee-representative director. If the PRC Company Law is amended as the Draft Company Law Revisions indicate, companies with 300 or more employees may be required to have at least three directors. Moreover, the Draft Company Law Revisions clarify and expand liability for directors (as well as others) – eg, a new rule would make them potentially jointly and severally liable with the company for damages and losses caused to others from intentional or grossly negligent actions.

Blocking Rules and Anti-sanction Law

On 9 January 2021, MOFCOM issued the Rules on Blocking Unjustified Extraterritorial Applications of Foreign Legislation and Other Measures (Blocking Rules), effective as of the same day. Under the context of ongoing US sanctions on Chinese companies, pursuant to the Blocking Rules, the State Council is tasked with establishing an inter-departmental working mechanism, headed by MOFCOM, to take charge of blocking unjustified extraterritorial applications of foreign legislation and other measures.

If the working mechanism confirms an unjustified extraterritorial application of foreign legislation or another measure, MOFCOM may issue a "Prohibition Order" against the relevant foreign legislation or other measure. A Chinese citizen or entity that has suffered losses from foreign legislation or measures falling within the scope of a Prohibition Order (an "Aggrieved Party") may initiate litigation in China to claim compensation from a third party who benefited from said foreign legislation or measure (a "Benefitting Party"), unless the Benefitting Party has applied for and obtained from MOFCOM an exemption from compliance with a Prohibition Order. The Blocking Rules seem to be another tool in the vein of the Security Review Measures.

Furthermore, on 10 June 2021, the Law of the People's Republic of China on Countering Foreign Sanctions (Anti-sanction Law) was promulgated, effective as of the same day. The Anti-sanction Law follows – and on the surface may suggest a step up from – similar but lower-level legislation, such as the Blocking Rules. Under the Anti-sanction Law, if the (unspecified) relevant State Council departments decide that a foreign nation has violated international law (or even basic norms of international relations) to "contain or suppress" the PRC, or has simply employed "discriminatory restrictive measures" (even based only on the foreign country's own laws) against PRC citizens or to "interfere with PRC internal affairs", the departments may add any of the following to a so-called "countermeasures list":

- any person or organisation who directly or indirectly participated in the drafting, decision-making or implementation of the discriminatory restrictive measures;
- any person or organisation affiliated therewith; and
- any manager, director or officers of any organisation on the list.

Once an individual or organisation is on the list, relevant State Council departments may employ one or more of the following "countermeasures":

- refusing to issue or cancelling visas, banning entry into the PRC, and deportation;
- sealing up, seizing and freezing movable, immovable and other types of property in the PRC; and
- prohibiting or restricting relevant transactions, co-operation or other activities with domestic organisations or individuals.

As a simple (albeit probably extreme) example, if a company participated in or is even closely tied to any "discriminatory restrictive measures" (even vicariously, through its senior management or actual controllers) against the PRC or any PRC party, the Anti-sanction Law provides for the State Council to effectively stop the company's transactions with PRC companies.

Cybersecurity and Data and Personal Information Protection

2021 was probably the most significant year so far in the development of the PRC's framework for cybersecurity and protection of personal information (PI) and data more generally.

On 22 March 2021, the Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Apps (PI-in-Apps Provisions) were issued, effective from 1 May 2021. The PI-in-Apps Provisions derive from and refine the principle, embodied in the Cybersecurity Law, of there being a certain "necessity" before and to the extent that PI is collected and used.

The PI-in-Apps Provisions distinguish 39 categories of common apps, and set out standards for types of PI that can be considered "necessary" for each such category of app to collect and use. As an example, the mobile phone number of registered users and resumes provided by job applicants may be deemed "necessary" PI for online job hunting and recruitment. As another example, "necessary" PI for online shopping includes the mobile phone number of registered users, the name, address and contact number of the recipient of the merchandise purchased, the time, amount and channel of payment, and other payment information. While the PI-in-Apps Provisions do not prohibit app operators from collecting and/or using types of personal information that are not listed as "necessary" by the PI-in-Apps Provisions, they do stipulate that no app operator may refuse to provide basic functions and services to users who do not agree to provide personal information that is not "necessary".

On 10 June 2021, the Data Security Law of the People's Republic of China (Data Security Law) was promulgated, effective as of 1 September 2021. The Data Security Law calls for central and local government authorities to give meaning to the term "Important Data" by issuing catalogues thereof, and also adds to the requirements regarding Important Data, particularly:

- extending the localisation (or cross-border transfer pre-authorisation) requirement to all handlers (not only critical information infrastructure operators, or CIIOs) of Important Data collected or generated in the PRC; and
- expressly requiring all processors of Important Data to carry out a periodic risk assessment of their data handling and submit risk assessment reports to the competent authorities.

On 20 August 2021, the PRC promulgated the long-awaited Personal Information Protection Law (PI Protection Law), which came into effect on 1 November 2021. Its 74 articles comprise both high-level and specific rules for a broad range of issues related to the processing of individuals' PI. On the one hand, its coverage overlaps with several laws, regulations, recommended national standards, etc, released in the last few years, so it may serve as a synthesis of rules while superseding existing conflicting

rules. On the other hand, while it contains new or extended rules, it also leaves some aspects of protecting PI to future implementation rules.

The PI Protection Law includes many provisions apparently imposing concrete responsibilities on parties processing PI, and heightened requirements for those that control large volumes of PI or operate important online platforms. It addresses many concerns that have recently come to be key in China, including automated decision-making and PI cross-border transfers, and may bring some innovations (although still subject to how certain clauses would be implemented, interpreted and applied) – eg, the extra-territoriality standards and the heightened (ie, "specific") consent standard.

In addition, both the PI Protection Law and Data Security Law:

- specify that all organisations and individuals within the territory of the PRC are prohibited from providing any data stored within the territory of the PRC to any foreign judicial or law enforcement bodies without obtaining the prior approval of the competent authorities of the PRC;
- substantially strengthen penalties for non-compliance; and
- provide for certain circumstances in which the processing of the PI/data of natural persons within China done outside China will be subject to the PI Protection Law/Data Security Law.

On 28 December 2021, the CAC published the revised Measures for Cybersecurity Review, taking effect on 15 February 2022. Under the revisions, cybersecurity review now applies to the following circumstances:

- when CIIOs intend to purchase any network product or service that affects or may affect state security;
- when any data processor carries out any data processing activities that affect or may affect issues of national security, even if such parties are not CIIOs; and
- when any company with the PI of more than one million users intends to conduct a stock listing outside the country.

Anti-monopoly

2021 marked the beginning of the 14th Five-Year Plan and also a "new era" of PRC antitrust enforcement. The National Economic Conference and central government have repeatedly emphasised the strengthening of antitrust enforcement power and preventing disorderly expansion of capital.

Starting in December 2020, parties that had made transactions in the past but had not completed the requisite filings for them were identified and retroactively punished. Most were internet companies with variable-interest-entity (VIE) structures. From January to August 2021, 49 historical fail-to-file transactions were investigated and those responsible were punished by China's antitrust agency, in contrast to the mere dozen such cases in the four years before that enforcement push.

On 7 February 2021, the Anti-monopoly Guidelines of the Anti-monopoly Commission of the State Council for the Platform Economy Sector (AML Guidelines) were issued, expressly stating that transactions involving VIEs are subject to merger control in China in the normal way. They also represent a comprehensive guide to how the State Administration for Market Regulation (SAMR) intends to regulate anti-competitive behaviour among businesses such as those operating e-commerce platforms, live-streaming platforms and other online platforms (Platform

Economy), and signal SAMR's determination to make the regulation of anti-competitive behaviour in the Platform Economy a priority, covering calculations of turnover, details of various monopoly agreements, requirements for using algorithms and the definition of a market in the Platform Economy.

China is also accelerating the revision process of its Anti-monopoly Law (AML) and placing special focus on monopolies in the internet field. On 23 October 2021, draft amendments to the AML were released for public comment, re-affirming a strong regulatory attitude toward the new economy, especially the internet sector, from a legislative perspective. The draft amendments to the AML include not only a general principle that operators must not abuse data and algorithms, technology, capital advantages or platform rules to eliminate or restrict competition, but an additional provision specifically providing that it will be an abuse of a dominant market position for an operator with a dominant market position to use data and algorithms, technologies or platform rules to set up obstacles to impose unreasonable restrictions on other operators.

Intellectual Property

On 1 June 2021, the fourth amendment to the Patent Law of the People's Republic of China (Patent Law) took effect. Consisting of revisions or additions involving more than two dozen articles of the Patent Law, the changes affect the rights and procedures for both obtaining and protecting patents, most notably the wider scope and term of design patents and heightened damages for infringement. The amendment is also overwhelmingly geared toward augmenting patent applicants' and patent holders' rights, although some provisions are aimed as much if not more toward alleged infringers and commercial parties generally. Perhaps most importantly, the majority of changes are meant to bolster the legitimate interests of patent applicants and patent holders.

The Interpretation on the Application of Punitive Damages Responsibility in Civil Cases relating to Infringement of Intellectual Property Rights (Interpretation of Punitive Damages), which came into effect on 3 March 2021, represent a further addition to the punitive damages for intellectual property infringement. Although punitive damages were already provided for by PRC legislation concerning intellectual property, the Interpretation of Punitive Damages seeks to provide the framework for courts to determine whether to award punitive damages, and in what amount. In principle, punitive damages are awardable only for "severe violations" of intellectual property rights. As the Interpretation of Punitive Damages is geared towards augmenting protections for intellectual property right-holders, where an intellectual property portfolio is a company's most valuable asset, as is often the case in the TMT sector, it is crucial to evaluate and manage the potential benefits and risks associated with intellectual property rights when carrying out or investing in businesses in China.

Contributed by: *Cloud Li, Joanna Jiang and Dimitri Phillips,* ***DaHui Lawyers***

DaHui Lawyers combines in-depth knowledge of China's legal and business landscape with extensive international experience. It has particular strength in new economy industries and complex cross-border transactions. DaHui has become a go-to firm for multinational companies in the highly regulated Chinese technology, media and internet/telecoms sectors, where its expertise has led to it becoming a key adviser and strategist to clients of all types and sizes in China's emerging but challenging market, providing the most effective and solution-oriented services tailored to clients' diversified business needs. The firm's TMT team consists of 13 partners and 63 fee earners.

AUTHORS

Cloud Li is a partner of DaHui Lawyers' TMT practice. He has represented European and North American multinationals, large Chinese state-owned and privately held companies, and numerous private equity funds in various TMT-related M&A, investments, disputes, compliance and general corporate matters. Cloud has acted for some of the largest and most established participants in China's TMT sector.

Joanna Jiang is a partner of DaHui Lawyers' corporate and TMT teams. She focuses on advising businesses in the information technology and telecoms, media, entertainment and healthcare industries on market entry as well as regulatory and transactional matters. Joanna has deep and extensive expertise in data and privacy protection, especially assisting clients to understand current and potential future requirements and risks, developing and helping to implement localised data compliance guidelines and systems, conducting data compliance due diligence and audits, handling government routine procedures and exceptional inquiries relating to data compliance, etc.

Dimitri Phillips is a member of DaHui Lawyers' dispute resolution, compliance and corporate/M&A practice groups. He handles a range of issues for foreign companies doing or seeking to do business in China, as well as Chinese companies operating abroad. Dimitri has advised clients on litigation, international arbitration, compliance, inbound and outbound investment and general corporate matters.

DaHui Lawyers

China World Tower A
1 Jianguomenwai Avenue
Beijing
100004
China

Tel: +86 10 6535 5888
Fax: +86 10 6535 5899
Email: richard.ma@dahuilawyers.com
Web: www.dahuilawyers.com