The Legal 500 & The In-House Lawyer
Comparative Legal Guide
China: TMT (3rd edition)

This country-specific Q&A provides an overview to technology, media and telecom laws and regulations that may occur in China.

This Q&A is part of the global guide to TMT. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/practice-areas/tmt-3rd-edition/

Country Author: DaHui Lawyers

The Legal 500

Cloud Li, Partner

cloud.li@DaHuiLawyers.com

Joanna Jiang, Counsel

joanna.jiang@DaHuiLawyers.com

1. **What is the regulatory regime for technology?**

   Technology, as a general matter, is subject to a wide range of laws and regulations in the PRC. Aside from general and widely applicable laws such as the PRC Civil Code, the General Principles of Civil Law of the PRC and the PRC Criminal Law, a collection of laws govern various more specific aspects of technology, including:

   - Intellectual property laws, e.g., the PRC Patent Law, PRC Copyright Law and PRC Anti-Unfair Competition Law (which covers trade secrets);
   - Import and export laws (e.g., the Administrative Regulations on Technology Imports and Exports);
   - Employment laws and regulations to the extent they govern matters such as work-for-hire

and moral rights;

- National and local laws promoting certain aspects of technology (e.g., the PRC Law on Promoting the Transformation of Scientific and Technological Achievements);
- Various sector-specific laws and regulations, e.g., within the PRC telecoms and Internet sectors, the Telecommunications Regulations of the People's Republic of China (Telecoms Regulations) promulgated by the State Council, the Catalog of Telecommunications Businesses (Catalog) issued by Ministry of Industry and Information Technology (MIIT) and the PRC Cybersecurity Law promulgated by the Standing Committee of the National People's Congress, among others; and
- Where a foreign party is involved, the recently promulgated PRC Foreign Investment Law and the recently revised 'Negative Lists'.

2. Are communications networks or services regulated?

Yes. Under the Telecoms Regulations, all telecoms business activities are classified as either 'basic telecoms services' (BTS) or 'value-added telecoms services' (VATS). BTS generally consist in providing public network infrastructure, public data transmission and basic voice communications services, while VATS generally consist in telecoms and information services provided through public network infrastructure. The Catalog provides affirmative definitions and specific descriptions of listed categories of PRC telecoms services, which in turn determine which licenses and permits a service provider must obtain from the MIIT in order to provide such defined services.

3. If so, what activities are covered and what licences or authorisations are required?

A wide range of activities are covered, as listed and categorized in the Catalog. For example, the primary authorisations consist of the 'Basic Telecommunications Service Operating Permit' for BTS and 'Value-Added Telecommunications Service Operating Permit' for VATS, which each further specify the sub-categories of activities that may be undertaken in connection with such permits pursuant to the Catalog and the Telecoms Regulations.

4. **Is there any specific regulator for the provisions of communications-related services?**

   The MIIT is the specific regulator for the provision of communications-related services, although some aspects of Internet/telecoms services may in addition be regulated by other authorities, e.g., the Cyberspace Administration of China (CAC) regulates the content of information disseminated over the Internet.

5. **Are they independent of the government control?**

   No. The MIIT, CAC and most other regulators are departments of the State Council, the principal administrative authority of the PRC government.

6. **Are platform providers (social media, content sharing, information search engines) regulated?**

   Yes. The regulation of such services will depend primarily on where in the Catalog each specific service might fall. For example, information search engines fall under the banner of Internet information services (Category B25 under the Catalog) and are regulated primarily by the MIIT. Social media and content sharing services will likely fall under the same Catalog category but may also involve other regulators, e.g., the National Radio and Television Administration if such services include any audio/video functions.

7. **If so, does the reach of the regulator extend outside your jurisdiction?**

   As an initial matter, regulation has generally remained domestic, even in the case of

legislative actions and technologies deployed to block access to certain foreign websites from within the PRC. However, some observers believe that CAC may currently be attempting to extend its reach outside the PRC, though it remains to be seen whether it will eventually do so in practice. For example, in draft measures recently released pursuant to the PRC Cybersecurity Law, not only are network operators within China who wish to transfer certain data overseas required to place contractual obligations on the recipients of such data, but one article purports to require overseas parties collecting certain data through the Internet to satisfy the PRC's own domestic operator obligations. Notably, these draft measures have not taken effect and it is uncertain whether CAC will ultimately adopt the latter provision in the officially promulgated measures.

8. Does a telecoms operator need to be domiciled in the country?

No law or regulation explicitly provides that telecoms operators need to be domiciled in the country. In practice, however, many foreign service providers without onshore entities (and thus not legally eligible to host content or services on onshore servers, which requires at least an ICP filing by an onshore entity) experience service accessibility and network transmission issues.

9. Are there any restrictions on foreign ownership of telecoms operators?

In general, the PRC has been gradually opening up more and more telecoms services to foreign investment. For example, under the most recently revised Negative Lists (effective 30 July 2019), there are now no longer any foreign investment restrictions applicable to call centre services in the PRC. However, there is still a complicated framework of foreign-ownership restrictions on telecoms operators (per the Catalog, the Negative Lists and other related regulations). For example, foreign stakes in BTS categories are statutorily restricted to 50% or less. The prohibitions and restrictions applicable to foreign participation in VATS sectors, in addition to being divided by categories and subcategories, are divided in terms of whether the foreign party seeking to participate in such activities is a qualified service provider established in

Hong Kong or Macau, whether the investment is being made in a foreign trade zone of China or whether neither of the two preceding situations applies.

10. Are there any regulations covering interconnection between operators?

Yes. The Telecoms Regulations provide the general framework to regulate such interconnections, including that the interconnection of telecommunications networks must be effected on the basis of the principles of technical feasibility, economic sense, fairness, impartiality and mutual complementation. The Administrative Provisions on the Interconnection between Public Telecoms Networks (Interconnection Provisions) provides further detailed provisions and procedures for interconnections between telecommunication networks. For example, the Interconnection Provisions prohibit a telecoms operator from rejecting any interconnection request from another telecoms operator and from restricting users from selecting any telecoms service of another telecoms operator.

11. If so are these different for operators with market power?

Yes. Under the Interconnection Provisions, an operator will be deemed ‘dominant’ if it controls necessary telecoms infrastructure and operates a fixed local telephone business which accounts for 50% or more of the market share of the same type of business within the scope of local networks such that the operator would have substantial influence over other business operators’ access into the telecoms market. Certain rules apply only to such dominant telecoms operators, including requirements to provide non-dominant telecoms operators with information on network functions, equipment configuration as well as other aspects related to the interconnection; to provide accommodative coordination and allow the use of communication facilities by non-dominant service providers without any unreasonable additional terms; and to provide, at the request of a non-dominant operator, a telephone number inquiry service to consumers of the other party’s networks.

12. What are the principal consumer protection regulations that apply specifically to telecoms services?

The PRC Cybersecurity Law, the Telecoms Regulations, the PRC Law on the Protection of Consumer Rights and Interests (PRC Consumer Protection Law) and other related laws and regulations include consumer protection provisions. For example, the PRC Cybersecurity Law provides for the protection of personal (sensitive) information as it is collected, processed, stored and transferred by telecoms operators. Among other things, it affords consumers the right to request operators to correct or delete such consumers' personal information (see further below, Question 15). The Telecoms Regulations provide general protections to consumers, e.g., that telecoms operators must supply services on time and collect opinions from users. Further, the Administrative Measures for the Licensing of Telecommunications Businesses require telecoms operators who discontinue their operations to notify their customers, to reach agreements with them regarding arrangements after discontinuance and to collect their opinions accordingly.

13. What legal protections are offered in relation to the creators of computer software?

The PRC Copyright Law and associated regulations (e.g., the Regulations on Computer Software Protection) grant copyrights over computer software to its author/creator (unless otherwise agreed), along with the rights of publication, authorship, modification, distribution and communication. The PRC Anti-Unfair Competition Law also includes protective provisions for trade secrets, which cover know-how and source code. For example, businesses are prohibited from disclosing, using or allowing others to use trade secrets in violation of confidentiality and from obtaining others' trade secrets by theft, bribery, intimidation, electronic intrusion or other improper means.

14. Do you recognise specific intellectual property rights in respect of data/databases?

No. However, the PRC Copyright Law may provide the same rights as referred to above (Question 13) to selective collections of data (or datasets) and database software. Moreover, databases and relevant data therein may be deemed trade secrets and protected under the PRC Anti-Unfair Competition Law (see Question 13 above).

15. What key protections exist for personal data?

Personal information, defined as information that may alone or in combination with other data identify a person, is protected primarily by the PRC Cybersecurity Law (supplemented by a number of national standards, including the Information Security Technology - Personal Information Security Specification and the Information Security Technology - Guideline for Personal Information Protection within Information Systems for Public and Commercial Services). Key protections include the requirement to obtain consent from data subjects for the collection as well as further uses of the personal information, the requirement on some operators to undergo security assessment procedures prior to an overseas transfer (see below, Question 16) and such further general principles as 'legitimacy, rightfulness and necessity' in the collection and use of personal information. The PRC Consumer Protection Law sets similar requirements on the collection of consumer information by business operators. Other high-level laws, e.g., the PRC Tort Law, the PRC Civil Code and the PRC Criminal Law, provide general privacy protections.

16. Are there restrictions on the transfer of personal data overseas?

Under the PRC Cybersecurity Law, aside from the requirement applicable to all operators to obtain consent from data subjects, a 'critical information infrastructure operator' (CIIO, i.e., in essence, an entity involved in important industries or undertakings with the potential to seriously impair national security, the national economy, people's livelihoods or other public interests) is also subject to certain 'security assessment' procedures before transferring data with personal information (or other important data) overseas. While there are no currently binding rules establishing the specifics of such security assessments, draft regulations detail a multi-part security assessment procedure and set out additional obligations, including the need for certain

contractual arrangements with the recipients of such data transfers.

17. What is the maximum fine that can be applied for breach of data protection laws?

The maximum fine is currently RMB 1 million if no illegal gains result from such breach. If illegal gains do result, such gains will be confiscated and the fine will be one to ten times the illegal gains from the breach.

18. What additional protections have been implemented, over and above the GDPR requirements?

As an initial matter, the data protection regime is in a relatively early phase of development in China. The PRC Cybersecurity Law, promulgated in 2017, is comprised mostly of general or high-level provisions, while implementing regulations have so far not included very specific provisions or are non-mandatory or still in draft form. Nevertheless, some additional protections are already indicated. A major one is the requirement that certain data collected or generated by CIIOs be stored in China (i.e., on servers physically located onshore). More subtly, while the GDPR contains some requirements on proper storage of biometric data, a non-mandatory national standard under PRC law specifies that for personal biometric information, technical measures should be used to process the data before storage, e.g., storing only a digest of the data.

19. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

Cloud-based services are specifically listed in the Catalog within the category of Internet resource collaborative (IRC) services, itself a sub-category of Internet data centre (IDC) VATS activities. Cloud-based service providers should obtain the

corresponding license from the MIIT pursuant to the Telecoms Regulations. Another set of major obligations applicable to cloud-based service providers consists of rules concerning the collection and use of personal information (see above, Questions 15 and 16), and it is likely that at least some major cloud-based service providers could be deemed CIIOs under the PRC Cybersecurity Law and thus be subject to additional obligations.

20. Are there specific requirements for the validity of an electronic signature?

An electronic signature is defined within the PRC as the data that is incorporated in or attached to a data message in electronic form and is used to identify a signatory's identity and to indicate the signatory's acknowledgement of the contents contained thereof. An electronic signature must meet the following requirements in order to be valid under PRC law:

- at the time that the data was used to make the electronic signature, it was owned exclusively by the electronic signatory;
- at the time of signing, the data used for the electronic signature was controlled exclusively by the electronic signatory;
- any alteration to the electronic signature after signing can be determined; and
- any alteration to the content and form of the data message after signing can be determined.

A valid electronic signature has the same legal effect as a seal or hand-written signature.

21. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

There is no PRC law or regulation providing for the automatic transfer of employees,

assets or third-party contracts in the event of an outsourcing of IT services.

22. If a software program which purports to be a form of A.I. malfunctions, who is liable?

As an initial matter, taking two common scenarios involving commercial use of software, the party that sells/distributes the software program to end users or provides the software program as a service would normally be liable for any malfunction of the software, though contract provisions may result in the software developer (to the extent it is not the seller/distributor or service provider) or another party bearing liability.

23. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?

a) obligations as to the maintenance of cybersecurity;

The PRC Cybersecurity Law provides a general principle that operators should take measures to secure the safety of networks and that individuals and organizations may neither engage in activities endangering cybersecurity, including illegally invading or interfering with others' networks (see further below, Question 23(b), nor provide programs or tools specifically used for activities endangering cybersecurity. Further, under PRC law, cybersecurity includes network operation security and network information security.

For network operation security, all network operators must, among other things:

- formulate internal security management systems and operating instructions, determine the persons responsible for cybersecurity and implement cybersecurity protection measures;
- take technological measures to prevent computer viruses, network attacks, network

intrusions and other actions endangering cybersecurity; and

- take technological measures to monitor and record the network operation status and cybersecurity incidents, preserving relevant web logs for no less than six months.

CIIOs have additional obligations, including to:

- set up independent security management institutions, designate persons responsible for security management and review their and other key personnel's security backgrounds;
- periodically conduct cybersecurity education, technical training and skill assessments;
- formulate contingency plans for cybersecurity incidents and periodically carry out drills; and
- make disaster recovery backups of important systems and databases.

For network information security, all operators must follow the principles of 'legitimacy, rightfulness and necessity', disclose their rules of data collection and use, clearly express the purposes, means and scope of collecting and using the information and obtain data subjects' consent, including to provide the personal information to others. Operators must adopt technical and any other necessary measures to ensure the security of the personal information they have collected and to prevent such information from being divulged, damaged or lost.

b) the criminality of hacking/DDOS attacks?

Illegally invading others' networks, interfering with the normal functions of others' networks and stealing cyber data or providing tools for such actions is prohibited. The PRC Criminal Law includes provisions specifically aimed at activities such as hacking. For example, the following acts in relation to hacking/DDOS attacks are subject to criminal liability:

- invading computer information systems in the fields of state affairs, national defence construction or sophisticated science and technology;
- invading any other computer information system to obtain data stored, processed or transmitted in the system or to exercise illegal control over it;
- deleting, altering, adding or jamming the functions of any computer information system, making the system impossible to operate normally and causing serious consequences;

- deleting, altering or adding the data stored in or handled or transmitted by the system, causing serious consequences; and
- intentionally creating or disseminating destructive programs, such as computer viruses, thus affecting the normal operation of a computer system and causing serious consequences.

24. What technology development will create the most legal change in your jurisdiction?

The various technological developments in cross-border e-commerce, blockchain, cloud computing and Internet of Things are likely to create the most legal change in the PRC in coming years.

25. Do you believe your legal system specifically encourages or hinders digital services?

As reflected by their unparalleled development in China over the past decade, the PRC legal system encourages digital services. Even cutting-edge additions to digital services (such as blockchain) have already been adopted widely in China's e-commerce landscape. Giants such as JD and Alibaba regularly extend their offerings, e.g., recently announcing plans to apply blockchain technology to their logistics services so suppliers and consumers can better trace products through production, transportation and storage. Other examples in this field include China's Ping An bank and Ant Financial, which both announced blockchain-based applications to maintain ledgers for cross-border transactions. The Nanjing local government even established an RMB 10 billion investment fund to invest in blockchain projects.

26. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

There are currently no PRC laws or regulations specifically regarding the creation,

development or use of artificial intelligence (AI). However, that does not mean AI is wholly unregulated (or wholly prohibited). Given that the operation of AI generally calls for large data sets, those developing and implementing AI services will be subject to the requirements of the PRC Cybersecurity Law and associated regulations. While China's cybersecurity regime is in a relatively early phase of development, China thereby also has advantages such as flexibility in further developing the regulatory framework applicable to AI in tandem with the development of the technology itself. At the same time, China will have to update other, older laws, such as the PRC Copyright Law, which currently does not appear to protect work and content created via AI.