Regulation of cloud computing in China

by *Samuel Yang*, *AnJie Law Firm* and *Practical Law China*

Practice notes | **Maintained** | China, International

An overview of the regulation of cloud computing in China. This note covers the characteristics of cloud computing, including its risks and benefits, the regulatory framework for cloud computing in China and key issues in negotiating cloud computing services.

Scope of this note

In recent years, *China* has been increasing its regulation in areas such as cybersecurity and data security with legislation such as the *Cybersecurity Law 2016* (2016 CSL, with effect from 1 June 2017). Cloud computing is both a rapidly growing market in China as well as subject to this increasing regulatory regime. This note explores the general characteristics of cloud computing, including its risks and benefits, as well as its regulatory framework in China and key issues in negotiating cloud computing service agreements.

(For general information on regulatory developments of cybersecurity and data protection in China, see *Practice note, Quick guide: Cybersecurity and data protection: China*.)

What is cloud computing?

Cloud computing is a style of computing in which dynamically scalable and often virtualised resources are provided as a service over the internet. The cloud is a metaphor for networks, internet, computers, laptops, mobile phones and other ways for users to access data centre operations according to their needs. Cloud computing can be powerful enough to reach 10 trillion operations per second, which can be used in computing-intensive operations such as simulating nuclear explosions and predicting climate change and market trends.

The *Security Guide for Cloud Computing Services* (2016) (Cloud Security Guide) (云计算安全指南2016) issued by the China Academy of Information Communications Technology (CAICT) (中国信息通信研究院) defined cloud computing as:

"a model that provides computing resource services through the network, through which customers, on a dynamic and self-service basis, receive and manage the computing resources provided by the cloud service providers according to their needs. Computing resources include servers, operating systems, networks, software, and storage devices."

Characteristics of cloud computing

The characteristics of cloud computing include:

- **On-demand self-service.** Customers can obtain the required computing resources with limited participation, or even without participation from cloud service providers. In some cases, customers can solely and independently determine the time and quantity of resources that they want to receive.
- **Ubiquitous access.** Through a standard access mechanism, customers can use a computer, laptop, mobile phone, tablet or other terminals to access cloud computing services at any time and in any place.
- **Resource pooling.** Cloud service providers provide resources (such as computing resources, storage resources and network resources) to multiple customers. These physical or virtual resources can be dynamically allocated or redistributed among the customers according to their needs.
- **Fast scalability.** Customers can acquire and release computing resources as needed quickly, flexibly and conveniently. For customers, the resources are "infinite" and they can acquire additional resources at any time.
- **Measurable service.** Cloud computing can automatically control or quantify resources in accordance with a variety of measurement methods (such as pay-per-view or re-charge). The measurements may include, for example, storage space, computing power, network bandwidth or active accounts.

Service models

Cloud computing technology is generally categorised into three different service models:

- **Infrastructure as a Service (IaaS).** This model concerns the provision of computers, networking, storage, load balancing and virtual machines. These services and end-user hardware and software resources can be expanded or contracted according to customer needs.
- **Platform as a Service (PaaS).** In this model, managed service providers help customers by providing work platforms, including execution time, databases, web services, development tools and operating systems, without the need for customers to manually allocate resources.
- **Software as a Service (SaaS).** This model includes software components such as virtual desktops, utility applications, content resource management, email and software. In this model, the cloud service provider is responsible for installing, managing and operating the software, and customers log in and use the software through the cloud.

Deployment models

Depending on how the cloud is deployed, there are four models of cloud computing which meet varying customer requirements:

- **Public cloud.** In this model, standardised applications, resources, storage and other services are provided to a variety of customers on a shared, self-service, "pay as you go" basis. This deployment model typically provides scalable cloud services and can be efficiently set up.
- **Private cloud.** A private cloud is the cloud infrastructure operated solely for a single organisation, that is managed either internally or by a third party, and hosted either internally or externally. In this model, correction, inspection and other security issues need to be taken care of by the organisation itself. In addition, the entire system also requires the organisation's own money to buy, build and manage. This cloud computing model can provide the full benefit and functionality of the service to its owner.
- **Community cloud.** This model is built on a specific group of multiple similar targets, such as companies, that share a common set of infrastructure and the related costs.
- **Hybrid cloud.** A hybrid cloud is a mixture of two or more cloud computing models, such as public and private clouds. The models are independent of each other, but are all included within the cloud, so organisations can take advantage of a tailored mix of cloud computing models.

Benefits of cloud computing

The main benefits of cloud computing include:

- **Reducing overhead and energy consumption.** The use of cloud computing services can convert hardware and infrastructure construction funds into on-demand services. Customers only pay for the resources used and do not need to bear the cost of building and maintaining the infrastructure, therefore avoiding incurring capital investment. Cloud service providers use a variety of technologies, such as cloud infrastructure, virtualisation, dynamic migration and workload consolidation, to improve resource utilisation so that free resource components can be shut down to reduce energy consumption. Multi-tenant sharing mechanisms and the centralised sharing of resources can meet the peak demand for multiple customers in different time periods, therefore avoiding wasting resources due to capacity design and impact on

performance by peak demand. Cloud services reduce operating costs and energy consumption effectively, and therefore are considered to be environmentally friendly.

- **Enhancing business flexibility.** Customers using cloud computing services do not need to build a dedicated information system. This shortens the business system construction cycle, enables customers to focus on business functions and innovation, and improves business response speed and quality of service.
- **Improving availability of business systems.** The resource pooling and scalability of cloud services enable customers to expand their business systems dynamically to meet the rapid expansion of their business and avoid the interruption of customer service systems due to sudden increases in demand. The backup and multi-copy functions of cloud computing can improve the robustness and availability of business systems and avoid data loss and business failures.
- **Access to professional services.** Cloud service providers have professional staff and can update or adopt advanced technologies and equipment in a timely manner. The professional technical, management and personnel support of cloud service providers can give access to a higher level of advanced technical services.

Risks of cloud computing

Major risks for customers using cloud computing solutions include:

- **Weakened ability to control data and business systems.** In the cloud computing environment, customers migrate their data and business systems to cloud service providers' cloud computing platforms, thereby losing the direct control over these data and business systems.
- **Difficulty in dividing responsibility between customer and cloud service provider.** In the cloud computing environment, the responsibility for customer management and the responsibility for the customer's data security are accorded to different persons, and it is not easy to delineate the responsibility between them. Furthermore, different service patterns and deployment patterns and the complexity of the cloud computing environment also increase the difficulty of dividing the responsibility between cloud service providers and customers. In addition, cloud service providers may also purchase services from other cloud service providers which will lead to more difficulty in defining their responsibility.
- **Jurisdiction issues.** The actual storage location of the data is often outside the customer's control. Authorities in some countries may require cloud providers to provide access to these data centres in accordance with their national laws, and may even require the providers to provide access to data stored in other countries' data centres, which changes the jurisdictional relationship between an organisation and its data. (For more information on the Chinese regulatory regime on data transfers from China to other jurisdictions, see *Practice note, Cross-border data transfers: China*.)
- **Challenges to ownership of customer data.** Customer data which is migrated to the cloud computing environment and the data which is generated and accessed in subsequent processes are both under the cloud service providers' control, and the providers are able to access or use the customer data. In contrast, customers may need to be authorised by the cloud service providers to access, use and manage their own data. If there is no clear regulation, the customer's ownership and control of its own data is difficult to be guaranteed.
- **Data protection is more difficult.** Cloud computing platforms use virtualisation and other technologies to achieve multi-customer shared computing resources. Because the barriers and other protections between virtual machines are vulnerable to attack, the risk of unauthorised data access across virtual machines is

significant. As the complexity of cloud computing platforms increases, it is more difficult to implement effective data protection measures against the risks of unauthorised access, tampering, disclosure and loss of customer data. The Chinese government is also planning a new Data Security Law, see *Legal update, NPC Standing Committee circulates draft Data Security Law*.

- **Data residue.** Storage media that store customer data are owned by the cloud service providers, and customers do not manage or control the storage media directly. When customers exit the cloud computing services, the cloud service providers should completely delete the customers' data, including the backup data. However, to date there are no valid mechanisms, standards or tools in place to verify that the cloud service providers have fully deleted these data. The data may still partially or even completely remain on the cloud computing platform after the client exits the cloud computing service.
- **Potential dependence on specific service providers.** Due to the lack of uniform standards and interfaces, customer data and services on different cloud computing platforms are difficult to migrate between platforms, as well as to migrate back from a platform to the customer's data centre. In addition, cloud service providers, for their own benefit, are often reluctant to provide portability for customers' data and business. This potential dependence on specific cloud service providers may cause the customer's business to break down with an interruption to the provision of cloud services that, if severe enough, could result in data and business migration to other cloud service providers at a high cost. Another factor in the potential over-reliance on specific service providers is that the cloud computing service market is still maturing, with limited cloud service providers to choose from.

Cloud computing market development in China

China's cloud computing market is maintaining an overall trend of rapid development with the following features:

- Public cloud services are expanding gradually from the internet sector to the industry market.
- The hardware market dominates the domestic private cloud market.
- Cloud services, and IaaS in particular, are fully embraced by domestic enterprise users. The domestic IaaS market is the first choice for small and medium enterprises for information technology (IT) resources construction in the fields of games, video and mobile internet.
- PaaS services have become an important platform and the first choice for internet enterprises due to the low cost, fast deployment, and rich application programming interfaces (APIs) for developers. From the user application perspective, the market is demanding changes to services from initial search or map engine services and web services to big data analysis, security monitoring and other more complex services.
- SaaS services account for the majority of the cloud computing market demand.

Regulatory framework of cloud computing in China

There were no specific laws and regulations regulating cloud computing services in China before the promulgation of the *Circular of the Ministry of Industry and Information Technology on Issuing the "Classified Catalogue of Telecommunications Services" 2015* (2015 Telecoms Catalogue, with effect from 1 March 2016) by the *Ministry of Industry and Information Technology* (MIIT). Although the 2015 Telecoms Catalogue also does not define "cloud

computing" or "cloud service", it is generally accepted that the term "internet resource co-ordination services" (IRCS) (互联网资源协作服务业务) in the catalogue refers to cloud services.

For more general information on the regulatory framework of telecommunications in China, see *Practice note, Regulation of telecommunications sector in China: Regulatory framework for telecoms sector*.

Internet resource co-ordination services

According to the *2015 Telecoms Catalogue*, IRCS means:

"the data storage, internet application development environment, internet application deployment and operation management and other services provided for users through internet or other networks in the manners of access at any time and on demand, expansion at any time and co-ordination and sharing, by using the equipment and resources built on database centres" (*section B11*).
In addition to the catalogue, the MIIT also released the *Notice on the Regulation of Cloud Service Market's Business Conduct (Draft for Public Comment)* (Draft Notice) (关于规范云服务市场经营行为的通知（公开征求意见稿）) in November 2016, which expressly states that "cloud service" is one type of IRCS mentioned in the 2015 Telecoms Catalogue (*Article 1*).

Licences required for operating cloud services

Under the *2015 Telecoms Catalogue*, IRCS is a type of Internet Data Centre Service (IDC) (互联网数据中心业务), which are categorised as value-added telecoms services (VATS). Providing VATS in China requires a telecoms licence (VATS licence) (see *Practice note, Regulation of telecommunications sector in China: Telecoms licensing*). Accordingly, the operation of cloud services in China requires a VATS licence dedicated for IDC business, which is also known as an IDC licence.

The description of the term "IRCS" in the 2015 Telecoms Catalogue is broad and generally understood to cover all types of cloud services, namely IaaS, PaaS and SaaS. Accordingly, in theory the operation of all these types of cloud services requires a VATS license dedicated for IDC business. However, according to the MIIT's 2017 *interpretation* the operation of certain types of SaaS services does not require a VATS license if those services are regarded as "pure software services" and do not involve other VATS under the 2015 Telecoms Catalogue.

Foreign investment restrictions

In theory, subject to some foreign capital ratio restrictions, *foreign-invested enterprises* (FIEs) can apply for an IDC licence according to the *Provisions on the Administration of Foreign-Invested Telecom Enterprises 2008* (2008 Foreign-Invested Telecoms Regulations, revised in 2016). The 2008 Foreign-Invested Telecoms Regulations state that a *foreign-invested telecommunications enterprise* (FITE) operating VATS may not have foreign investors' capital contribution exceeding 50% (*Article 6*). In addition, the regulations also require that an FITE providing VATS has registered capital meeting the following minimum capital requirements:

- At least RMB10 million if the FITE's operation is nationwide or cross-provincial.
- At least RMB1 million if the FITE's operation is within a single province.

(*Article 5*.)

However, as IDC services were not part of the scope of VATS to be opened up to foreign investment that China made at its accession to the WTO on 11 December 2001, IDC licences have only been granted to Chinese companies and their joint ventures with Hong Kong and Macau investors, and not to companies invested in by investors from other jurisdictions. Although Hong Kong and Macau investors are to some extent also treated as foreign investors by Chinese authorities, their eligibility for IDC licences was specially granted in the Closer Economic Partnership Arrangements (each, a CEPA agreement) entered into by China in 2003 with Hong Kong and Macau, respectively. Each CEPA agreement allows Hong Kong and Macau investors to set up joint venture enterprises with Chinese investors in China to provide IDC services. Hong Kong and Macau service suppliers' shareholding in these joint ventures may not exceed 50% and there is no geographic restriction for the provision of the IDC services within China. For more information on the preferential policies for Hong Kong and Macau service providers under other CEPA arrangements, see *Practice note, Regulation of telecommunications sector in China: Preferential policies under CEPAs*.

Except for these special rules for Hong Kong and Macau, foreign investors from other jurisdictions are not eligible for the application of an IDC licence. According to the *MIIT website*, as of 14 August 2020 there are only twenty Sino-Hong Kong joint ventures which have been granted the VATS licence for the operation of IDC services.

Work-around arrangements for foreign investors

As most foreign-invested companies are not eligible to apply for the IDC licence, they are not allowed to operate cloud services in China under their own names. Foreign cloud service providers have to co-operate with Chinese IDC licence holders to provide cloud services to their customers. These types of co-operation are mainly based on contractual arrangements between the foreign cloud service providers and relevant Chinese IDC licence holders, such as technology licensing, brand licensing and other contractual arrangements, to ensure the foreign cloud service providers can participate in the relevant decision-making process.

However, some types of contractual arrangements between foreign cloud service providers and the relevant Chinese VATS licence holders seem to raise issues of concern to the MIIT, and the Draft Notice appears to have been issued to correct those suspect arrangements. According to the Draft Notice, foreign investors are required to strictly comply with the *2008 Foreign-Invested Telecoms Regulations* and the CEPA agreements and other relevant policies concerning IDC services, and to apply for the establishment of FITEs and obtain the corresponding VATS licences before they can operate cloud services in China (*Article 3*). In addition, the Draft Notice specifically requires Chinese licensed cloud service providers to report their technical co-operation with "relevant entities" to the MIIT, and in the course of such co-operation the licensed cloud service providers should not:

- Lease or assign their telecoms service licences to the counterparties in any form, or provide resources, venues, facilities or other conditions to the counterparties for their illegal operation.
- Allow the counterparties to sign contracts with customers directly.
- Allow the cloud services to be provided only under the trade marks and brands of the counterparties.
- Illegally provide users' personal information and network data to the counterparties.
- Engage in any other illegal acts.

(*Article 4*.)

The Draft Notice also requires cloud service providers to establish their cloud service platforms in China. When cross-border connectivity is needed, the relevant servers should be connected to overseas networks through the

international internet gateways approved by the MIIT. It is forbidden to establish or use other channels for cross-border connectivity through private lines, virtual private networks (VPNs) and other means (*Article 7*). When providing services to domestic customers, service facilities and network data should be kept within China and cross-border operation and maintenance and data flow should comply with the relevant regulations (*Article 9(4)*).

These restrictions on the co-operation between licensed cloud service providers and their contractual counterparties indicate that foreign cloud service providers, when co-operating with Chinese licensed cloud service providers, can only play a subordinate role and that any attempt to "control" the Chinese counterparties would likely be challenged by the MIIT.

Security assessment measures for cloud computing platforms

On 2 July 2019, the MIIT together with other ministries jointly issued the *Measures on Security Assessments for Cloud Computing Services 2019* (Measures) (云计算服务安全评估办法), with effect from 1 September 2019. The Measures intend to further flesh out the provisions of the *2016 CSL* by improving the security and controllability of cloud computing services procured and used by the Communist Party and government organs and operators of critical information infrastructure (CII). The Measures provide that a cloud computing services provider may apply to conduct a security assessment for a cloud platform, and must submit to the security assessment office a declaration form, as well as a cloud computing service system security plan, reports on the continuity of the business, the security of the related supply chain and the feasibility of customer data migration, and other materials.

For more information on the measures, see *Legal update, CAC and others issue security assessment measures for cloud computing services platforms*.

Key legal issues in negotiating cloud service contracts

Cloud service providers often do not allow changes to their standard terms and conditions. Considering the multi-tenant shared operating model and the multiple components involved in cloud solutions (except for private cloud), proposed changes from different customers may vary greatly. Therefore, it is not economical for cloud service providers to spend time and resources negotiating with customers, especially small and medium-sized customers, to customise their contracts.

Where cloud service providers are willing to discuss changes to their terms and conditions (normally with large corporate customers that have stronger bargaining power), customers are recommended to do their due diligence first to understand any potential legal compliance issues with the proposed cloud solutions or if any gaps exist between the customers' expectations and the proposed cloud solutions. Customers then need to prioritise the areas they want to mitigate against these issues and deal with them accordingly. The areas of data protection and cybersecurity, intellectual property (IP) rights and service performance are perhaps among the most important for all cloud computing contracts.

Personal privacy and cybersecurity issues

Personal privacy and cybersecurity issues have become some of the primary factors that customers need to take into account in deciding whether to migrate their IT infrastructure to the cloud. The service calculation mode, dynamic virtualisation management and multi-tenant shared operating model of cloud computing services pose a serious challenge to the security and privacy of personal and business data. Both customers and cloud service providers must comply with applicable laws governing personal privacy protection and cybersecurity.

Although still at an early stage, various Chinese laws and regulations have imposed some fundamental principles for the protection of personal privacy and cybersecurity (for example, see *Practice note, Data privacy in China* and *Security assessment measures for cloud computing platforms*). Before entering into a cloud service contract, the customer needs to ensure that the transfer of personal data to the cloud service provider has been notified to the relevant personal data subjects and that the subjects have consented to the transfer. As the cloud service customer is primarily responsible for the security and personal privacy of its own customers' data, it needs to ensure that personal data and other customer data are handed over to cloud service providers with sound and robust safeguards. The cloud service provider has the responsibility to ensure the safety of customer data, including personal data processed on behalf of the customers.

The *Provisions on Protecting the Personal Information of Telecommunications and Internet Users 2013* issued by the MIIT require that telecommunications business operators and internet information service providers be responsible for the security of users' personal information as collected and used during the provision of services. This obligation applies to cloud service providers. Accordingly, in a cloud service contract the customer should require the cloud service provider to abide by all relevant legislation in the personal data protection and cybersecurity areas. The contract should stipulate that the cloud service provider must not release any information to a third party, even when they are requested to disclose the information by a foreign government. Moreover, the customer should require the cloud service provider not to access, revise, release, use, transfer or destroy any data from the customer without the customer's consent. (For more information, see *Practice note, Data privacy in China: Data privacy principles*).

In addition, when entering into a cloud services contract both the customer and the cloud service provider need to take into account regulations restricting data flow to foreign jurisdictions. This restriction typically applies to those industries which are considered to concern the national security of China. For example, the *2016 CSL* requires operators of CII to store within China personal information and important business data that was collected in China. However, these may be transmitted abroad on successful completion of a security assessment by the relevant authorities (*Article 37*). The cloud service customer therefore needs to assess whether its IT infrastructure can be regarded as CII and if so, it will need to take the relevant requirements into account in the selection of a cloud service provider, and work with the provider to put in place technical and management measures and contractual terms to ensure that the data flows are compliant.

For more information on the 2016 CSL, see *Legal update, China passes Cybersecurity Law*.

For more information on cross-border data transfers, see *Practice note, Cross-border data transfers: China*.

For more information on the protection of personal data privacy in China generally, see *Practice notes, Data privacy in China* and *Data breach notification in China*.

IP protection issues

Cloud computing can raise complex IP issues. On the one hand, IP rights are specific to jurisdictions. IP laws vary among jurisdictions, so a protectable IP right in one jurisdiction may not be protected equally, if at all, in another jurisdiction, and an infringement of IP rights in one jurisdiction may not be an infringement in another jurisdiction. On the other hand, cloud computing is meant to break boundaries and work across jurisdictions, as in the cloud computing environment technology and data are frequently used beyond national borders. This tension can be a significant issue for both cloud service providers and their customers. Both parties should be clearly aware of the specific differences in IP laws that are relevant to their business operations, and should actively manage those discrepancies through their contractual arrangement with each other or through other means, to mitigate the risks of infringing the IP rights of third parties or suffering infringement of their own IP rights.

Another reason for the complexity of IP rights is that cloud computing solutions include multiple components and the relevant IP rights may belong to different licensors. The cloud service provider which signs the contract with a customer may not have the right to license or sublicense all of these IP rights to the customer. A defect which exists in any part of the licensing chain from the original licensor to the customer may present licensing risks and potential liabilities to the customer. Even if the cloud service provider has the right to license or sublicense the necessary IP rights to the customer, the customer may face the risk of service interruption if an essential IP licence in the cloud solution expires and the cloud service provider fails to renew it or provide an alternative solution. To mitigate these risks, the customer should seek full IP right indemnities from the cloud service provider for all service offerings in the cloud solution, while the cloud service provider may try to defend its position by only providing limited indemnities, or by leaving room for it to seek alternative solutions to replace the IP-flawed solutions without providing any indemnities to the customer.

Service performance

In a typical software licensing agreement or hardware sale agreement, there normally is no measurement, or only very simple measurements, provided to determine whether the product performs "normally". Moreover, due to the vague standards of good performance, usually no compensation is provided to the customer if the software or hardware does not perform well enough. However, as cloud computing is provided as a service covering hardware, software, network and maintenance, there are several more measurable parameters which can be used to determine if the cloud service is provided up to certain standards. It is therefore possible, and necessary, to set up a mechanism of service performance measurement for cloud services and corresponding compensation payable to the customer for poor performance. This mechanism is now a common practice in the cloud industry and is known as a service level agreement (SLA).

The measurements under an SLA can include availability of the service (normally in the form of the percentage of usable time against a certain period of time), the cloud service provider's response time for customer fault reports, time needed to fix problems (known as mean time to repair or MTTR) or other specific measurable parameters depending on the nature of the cloud services provided. Accordingly, if the cloud service provider fails to meet the relevant parameters set out in the relevant SLA, then a calculated compensation (known as service credits) will be paid by the cloud service provider to the customer. The customer should analyse the measurable parameters in its contracted cloud service and seek to agree with the cloud service provider on the applicable service credits and other SLA provisions.

Given that customers may have migrated their essential operating systems and applications to the cloud, they may not tolerate any outage or interruption of the cloud service. A "business continuity" clause deals with how the cloud service provider should act to ensure that the customer can still use the contracted services in the event of an outage or interruption of service. This normally involves the customer requiring certain visibility, as a contractual right, of the cloud service provider's business continuity plan (BCP). The customer may also require that the provider's BCP and any changes to it should be discussed with and approved by the customer to ensure that the customer's own BCP requirements will be integrated as part of the cloud service provider's BCP practice.

Governing law and applicable law

Cloud service providers and their customers are sometimes located in different jurisdictions, and the operation of the cloud service may also involve other jurisdictions. Therefore, governing law issues should be carefully considered taking into account, for example, whether the law of the relevant jurisdiction has a different set of rules for the handling of personal data and business data from the principles agreed by the parties in the agreement. For example, the data protection rules of the EU are generally stricter than those in China (for more information, see *Practice notes, Data privacy in China* and *Overview of EU General Data Protection Regulation*).

The concept of applicable law is different from the governing law of the agreement, and knowing this is especially important for a customer entering into a cloud service contract. Depending on the jurisdictions where the cloud service provider operates, the laws and regulations of multiple jurisdictions may be applicable to the cloud service. While it is generally still a good practice for the customer to require the cloud service provider to comply with all applicable laws, the customer should assess whether it will become subject to the laws of a specific jurisdiction because its data will be processed or stored there. If those laws would present challenges to the secrecy and security of its data, the customer may need to consider whether technical measures should be put in place by the cloud service provider to prevent, if possible, the data from being stored or processed in that jurisdiction to avoid the application of its laws.

END OF DOCUMENT

