China

Jingyuan Shi is a partner in the Shenzhen office of Simmons & Simmons, and is responsible for the TMT practice in the Greater China region. She is a PRC-qualified lawyer and a practising solicitor in England and Wales.

She focuses her practice on the telecoms, media, and technology (TMT) sector. She has in-depth knowledge of the TMT industry from various perspectives, primarily advising on all sorts of corporate and commercial transactions, data compliance issues and general regulatory matters. She is experienced in cross-border work, start-up financing, regulatory compliance (including competition work) and intellectual property matters. Jingyuan is regularly invited to speak at industrial events and contributed to the China chapters of *Lexology Getting The Deal Through – Fintech* (2017–2021) and *Lexology Getting The Deal Through – Telecoms & Media* (2017–2021). Jingyuan holds an LLB from Fudan University and an LLM (IP and IT law) from the London School of Economics and Political Science (Distinction).

Yuchen Lai is a PRC qualified lawyer based at Simmons & Simmons' Shenzhen office.

Yuchen works extensively for international and Chinese TMT companies, investors, financial institutions, asset managers, fintech companies and life sciences companies. She advises on a wide range of compliance issues and has a strong focus on data advice and has in-depth knowledge and rich experience in Chinese and global data compliance projects.

Previously, Yuchen was a senior journalist with a large media organisation in China, focusing on legal reporting. She excels at regulation and policy analysis and providing comprehensive, pragmatic and commercial advice. She holds a BA from Sun Yat-sen University and an MSc from the London School of Economics.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

There have been significant developments in China regarding cybersecurity, protection of personal data and privacy in general in recent years. China, for the purpose of this chapter only, refers to mainland China, without taking into account the laws and practice in Hong Kong SAR, Macau SAR and the Taiwan region.

The Civil Code took effect on 1 January 2021, which sets the fundamental principles for protection of personal data and privacy. The triangulated safeguard for data regulation, namely the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law (PIPL), are ready in position to set the key regulatory framework in China. The Cybersecurity Law took effect in 2017; the Data Security Law took effect on 1 September 2021; and the PIPL took effect on 1 November 2021.

The Cybersecurity Law is the first legislation in China to comprehensively regulate the country's cyber networks. It applies to the construction, operation, maintenance and use of networks, as well as to cybersecurity supervision and management within the territory of China. The Cybersecurity Law is wide in scope, containing an overarching framework targeting the regulation of network security, protection of personal data, and safeguards for national cyberspace sovereignty and security. It is the foundation of other laws, regulations and industrial rules related to cybersecurity and personal data protection. It relates more to data in general rather than focusing on personal data (although there are certain provisions in relation to personal data).

The Data Security Law is the first fundamental law on data security in China. It relates more to data in general rather than focusing on personal data. It sets out the overall principles and structure of China's data security legal regime from a national security and sovereignty point of view. A key concept under this new law is the categorised and hierarchical data protection system. The specific scope and catalogues of 'important data' are required by this law to be formulated and published by regional and sectoral regulators. Cross-border transfer of such 'important data' is subject to specific requirements. Given 'important data' is a key concept used at various places during this chapter, before the aforesaid catalogues are published and for reference purposes at this moment, in one of the draft guidelines (not effective and not mandatory), 'important data' is defined as data collected and generated by organisations and individuals within China that is not a state secret but closely relevant to national security, economic development or public interest.

The PIPL is the first comprehensive law on personal data protection in China. It establishes rules for personal data processing, the protection of sensitive personal data, cross-border transfer, rights of personal data subjects, and obligations of

personal data processors and their entrusted parties when processing personal data. The PIPL borrows many key concepts from the EU General Data Protection Regulation (GDPR), such as extraterritorial effect on overseas processing of personal data of China-based individuals for the purpose of offering products or services to, or for analysing and assessing the behaviour of, such individuals; more legal bases for the processing of personal data, in addition to consent, which used to be the only lawful basis under Chinese law; the concept of data protection impact assessment but with lower triggering thresholds than GDPR. Meanwhile, the PIPL maintains an equal amount of unique features to reflect local regulatory and business needs; for example, legitimate interest is not included as one of the legal bases for processing personal data; it proposes restrictions on the cross-border transfer of personal data by the nature of the transferors.

One key accompanying regulation to the three laws mentioned above is the Regulation on Security Protection of Critical Information Infrastructure that took effect on 1 September 2021. It clarifies the scope of Critical Information Infrastructure (CII) and provides that regulators of key sectors (eg telecoms, energy, transportation, finance, defence, etc) are responsible for formulating CII

identification rules and identifying CIIs. The regulation stipulates obligations for CII operators, including, among others, conducting cybersecurity monitoring, test and risk assessment, formulating and implementing contingency plans, establishing security protection policies for personal information and data; reporting cybersecurity incidents and important matters, and completing cybersecurity review under certain circumstances (see below). Each CII operator must appoint a specialised body to take care of the cybersecurity issues, and key members of this body must go through security background checks.

Another noticeable regulatory update is the amended Cybersecurity Review Rule (which took effect on 15 February 2022), and this amendment was jointly published by the Cyberspace Administration of China (CAC) and 12 other government departments on 28 December 2021. The concept of security review was firstly introduced in the Cybersecurity Law, which requires CII operators to apply for national security review on their procurement of network product and services if it may impact national security. The amended Cybersecurity Review Rule extends the cybersecurity review to data processing activities that impact or may impact national security, by internet platform operators. In particular, an internet platform operator must apply for cybersecurity review over its proposed listing outside of China, if it possesses over one million users' personal data. This will have a severe impact on data-rich technology companies seeking a listing in a foreign country. The substantial parameters for such review are, among others, to verify whether there are risks of theft, leakage, damage or illegal cross-border transfer on 'core data', 'important data' or a large volume of personal data, and following the listing in a foreign country, whether the CII, 'core data', 'important data' or large volume of personal data might be influenced, controlled or maliciously used by a foreign government. 'Core data' is defined under the Data Security Law as such data that relates to national security, lifelines of the national economy, people's livelihood or major public interest. The amendment proposes to extend the statutory review period from 45 working days to three months or even longer.

In addition to mandatory laws and regulations, the Personal Information Security Specification (GB/T 35273-2020), which took effect on 1 October 2020, is a recommendatory national standard. This is a comprehensive and practical guideline for data compliance. Compared with the 2017 version, it has made many significant changes. It adds restrictions on user profiling (eg, user profiling should not have contents regarding race, religion, disability or disease discrimination); it makes specified requirements for personalised display (eg, during e-commerce service, any personalised display of products or services based on the consumer's interest or preference or consumption habits shall be accompanied by options that are not personalised); it adds requirements for third-party access management (eg, built-in

> “When hit with a data security incident, companies must be able to multitask on many pressing issues at the same time.”

security risk assessment mechanism in advance, identification of such third-party access to consumers); it sets rules for appointing data protection officers or similar positions based on the size of the company or volume of user information they process; and it establishes specific rules and guidelines on handling sensitive personal data, including storage, sharing, transfer, public disclosure and incident notice.

On 29 October 2021, CAC published the Draft Measures for Data Export Security Assessments (Draft Security Assessment Measures) for public comments. The Draft Security Assessment Measures set out the procedures, required materials and criteria for security assessments for cross-border data transfer. This draft proposes to expand the applicability scope of security assessment required under the Cybersecurity Law, Data Security Law and the PIPL.

On 14 November 2021, CAC released the Draft Administrative Regulation on Network Data Security (Draft Regulation) for public comments. The Draft Regulation sets out various rules regarding the processing of ‘important data’ and personal data. It has a wide range of extraterritorial applicability, which includes processing data of China-based individuals and organisations: (i) for the purpose of

offering products or services in China; (ii) analysing or assessing the behaviour of China-based individuals and organisations; or (iii) processing 'important data'. The Draft Regulation expands the extraterritorial effect of the PIPL to those processing activities targeting both China-based individuals and organisations.

On 10 February 2022, the Ministry of Industry and Information Technology (MIIT) released the updated Draft Administrative Measures for Data Security in the Areas of Industry and Informatization (the MIIT Draft Regulation) for public comments. This MIIT Draft Regulation applies to the processing of industrial, telecoms and radio data performed within China.

On 16 March 2022, the Standardization Administration of China (SAC) completed another updated draft of the Rules for Identification of Important Data and published it for public comments. According to this latest draft, the definition of 'important data' is revised as 'data in specific areas, groups, regions, or data reaching certain accuracy or scale, once leaked, tampered with or damaged, may directly endanger national security, economic operation, social stability, public health and safety'. The designation of 'important data' shall be consequence (rather than data type) driven.

Photo: shutterstock.com/Eric007

In addition, regional legislators are also actively formulating data-related regulations. As of the date of our response, regional data regulations of Shenzhen Special Economic Zone (effective on 1 January 2022), Shanghai City (effective on 1 January 2022) and Chongqing City (effective as from 1 July 2022) have been published.

From the law enforcement side, the statistics on the official website of the CAC shows that the CAC, together with other relevant government departments, has closed down more than 33,000 applications; blocked more than 2.34 million website links; and frozen more than 3.64 million illegal user accounts, involved in pornographic, gambling, malware or illegal gaming activities. The CAC launched special campaigns for eight months in 2020 to regulate online activities in China.

In particular, the CAC, the MIIT, the State Administration of Market Regulation and the Ministry of Public Security together launched a campaign against illegal collection and processing of personal data via mobile applications that has been running since late 2019. According to statistics published in June 2022, the MIIT has examined over 3.22 million mobile applications in the market, and ordered nearly 3,000 applications to rectify their non-compliant processing activities or suspend services.

In addition to the crackdown on low-profile illegal activities, the CAC also targets some of the high-profile leading players in the market. For example, in early July 2021, the CAC initiated cybersecurity review investigations against several leading transportation and logistics applications in China. The CAC and its local counterparts have continued with various law enforcement campaigns to target violations such as internet violence lately.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The Cybersecurity Law requires network operators to notify competent regulators of cybersecurity incidents including personal data breaches, but it does not go on to provide details about the key factors to be assessed. A set of lower-level regulations and standards provide guidelines in this regard. The reportable incidents usually include cyberattacks, hacking, malware, virus and human or equipment failure that may cause significant damage to the society and general public. Subject to the affected areas and degree of damage, there are different categories of reportable breaches. The key factors or impact of an incident that an organisation must assess include: (i) internet access in geographic areas (eg, single or multiple provinces, or even the entire country); (ii) operation of major websites or platforms (eg,

e-commerce websites with millions of active users); (iii) number of users affected (a minimum of 100,000 users should ring alarm bells); (iv) loss, theft or falsification of state secrets, important or core data that may cause significant damages; and (v) a catch-all scenario applicable to other factors, judged by the discretion of the organisation suffering the breach incident.

Upon initial assessment, if an organisation believes any of the above factors is met, it should immediately report such breaches to regulators. If a breach incident is likely to cause severe harm to the lawful rights and interests of individuals (eg, where sensitive personal data is leaked), the organisation shall inform the affected individuals of such breach incident.

The PIPL requires the processors of personal data (note the definition of personal data processor under Chinese law is essentially equivalent to the concept of a personal data controller under the GDPR) to notify the competent regulator and relevant individuals once a personal data breach is detected. If the processor can take measures to effectively avoid the damage caused by data breaches, then it may decide not to notify the affected individuals. However, if the data protection regulators find the breaches may cause damage to individuals, they can request the processor to notify the affected individuals regardless. There is so far no general hard time requirement on when such report must be done under the PIPL, but we recommend data processors to report as soon as possible if initial assessments point to a report.

In addition, note that there are likely sectorial rules with more specific timing requests on this issue. For example, for financial institutions, according to the Implementation Measures for Protecting Financial Consumers' Rights and Interests, which took effect on 1 November 2020, reports to consumers and the regulators must be made within 72 hours. The Measure for Supervising the Risks of Information Technology Outsourcing Activities by Banking and Insurance Institutions, which took effect on 30 December 2021, provides that banks shall report to China Banking and Insurance Regulatory Commission or its local counterparts within 24 hours of any client personal information breach or data damage/loss during the IT outsourcing activities. The Measures on Reporting, Investigation and Handling of Cybersecurity Incidents for Securities and Futures Sector, which took effect on 4 June 2021, provide that securities and futures institutions must report cybersecurity incidents immediately, and in the event of a severe incident the report shall be updated every 30 minutes. So, in addition to general reporting obligations, an organisation shall closely monitor and follow industry-specific regulations in order to comply with reporting obligations.

> "The amended Cybersecurity Review Rule extends the cybersecurity review to data processing activities that impact or may impact national security, by internet platform operators."

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

When hit with a data security incident, companies must be able to multitask on many pressing issues at the same time. The biggest issues include, but are not limited to, assessment of severity and scope of damage; determination of whether to report the incident to regulators and affected individuals; technical rectification measures to control the incident to minimise damage; complete and swift internal review and investigation of the breach; coordination with outside legal, forensic, technical or public relations counsel to prepare for subsequent actions; cooperation with directives from regulators and the police (if necessary); responses to customer inquiries or complaints; and responses to media reports or coverage.

Any of these issues, if not handled properly, may easily morph into a situation that is out of control, especially in today's social media age. Such an incident is the true test of a company's response strategies, internal policies, management structure, designated staff as well as technical capabilities. The ultimate goal is to

manage potential liabilities on all fronts, manage potential reputational damages, resume normal operation and prevent recurrence of similar incidents.

That said, out of these pressing issues, from a privacy protection perspective companies must concentrate resources to assess damages that may be caused to the privacy of affected individuals and take effective measures as a first priority to contain and control such damage while completing all legally required reporting and other obligations.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Following in the footsteps of the GDPR, China has made tremendous legislative efforts in data and cybersecurity related laws and regulations. Some high-profile pieces of legislation and investigation cases have conveyed strong messages to companies operating in China. We have seen many leading companies make good progress with regard to improving their cybersecurity preparedness.

First and foremost, the best practices are to comply with governing laws and regulations. Therefore, it is advisable to assess a company's actual compliance work against the laws and regulations and take measures to fix any gaps.

In addition to the mandatory laws and regulations, a company may need to comply with national and industry specific cybersecurity standards, including some technical standards as guidelines for their cybersecurity work. Typical examples include the Information Security Technology standards formulated by the National Information Security Standardization Technical Committee.

The Cybersecurity Law encourages companies to take security certifications. By going through the certification process, a company can evaluate its own practices against the certification standards, and make changes accordingly to improve cybersecurity. Internationally recognised certifications including without limitation ISO/IEC 27001 are being widely adopted by Chinese organisations as well.

As the regulatory framework in China on cybersecurity is still at a nascent stage, it is advisable to closely monitor the legislative process and implementations of the laws and regulations and potential impact over a company's business operations.

In terms of implementation of cybersecurity measures, companies need to mobilise resources to cover different areas. For example, they need to upgrade their IT infrastructure to maintain a high degree of cybersecurity; employ sufficient qualified technical staff; draft and implement necessary internal policies, especially an incident response policy; adjust the governance structure by appointing a data protection officer or similar roles; and seek readily available legal, forensic,

technical and public relations advice both in the case of an incident and in their daily operation.

If any incident has escalated to a certain degree, companies tend to form a special task force with in-house legal and technical staff and, if necessary, outside counsel as well, to address such incidents. It will help diffuse the situation in a professional and efficient way before it gets out of control.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Cloud services are one of the fastest growing areas in China in recent years. There are many factors for a company to consider and evaluate before it makes a decision to move data to a cloud hosting environment. These factors include, but are not limited to, security, flexibility, expansion capability, performance, cost, legal compliance, etc. If a company decides to go the cloud, the general recommendation is to assess the possibility of constructing the company's own private cloud system or to deploy hybrid cloud, and only if both are unrealistic, consider the public cloud.

Photo: shutterstock.com/asharkyul

"A customer's credit card number will be stored on the private cloud with higher security protection. In contrast, official website content can be stored on the public cloud with less security protection. Such a hybrid cloud solution may also help the company to meet various compliance requirements balanced with cost concerns."

With respect to special data security and privacy concerns, a company should evaluate such concerns in a larger context to determine the most suitable cloud service. As public cloud services cover a huge volume of users and multiple business models, they are more vulnerable to hacking. Hardware sharing is common for the public cloud. This means competitors using the same cloud services may share the same server. Further, the public cloud may not always meet certain compliance requirements, such as local storage of data. In contrast, a private cloud allows a company to deploy appropriate security measures as it sees fit, which will offer a higher degree of security. It is comparatively easier to meet compliance requirements using a private cloud. But the cost for a private cloud is also higher than the public cloud. Therefore, a company must strike a balance between the competing values of relevant factors in choosing cloud services.

In China, leading public cloud service providers include Alibaba, Tencent, Huawei, China Telecom and AWS. Although private cloud service providers, such as Huawei and Lenovo, are also available, the main users of private-only cloud services are comparatively limited to financial institutes in China. For companies with data security and privacy concerns, they tend to separate data into different categories based on the security grades. For example, a customer's credit card number will be stored on the private cloud with higher security protection. In contrast, official website content can be stored on the public cloud with less security protection. Such a hybrid cloud solution may also help the company to meet various compliance requirements balanced with cost concerns.

A company shall closely monitor sector-specific regulations and standards with respect to cloud deployment. For example, the MIIT has published multiple recommendatory standards (non-binding) for the telecoms sector since mid-2021. The People's Bank of China (PBOC) has also published three recommendatory standards regarding cloud computing for financial institutions in late 2020.

Subject to its business model, a company shall closely monitor data security and privacy related laws and regulations. It shall design its core products or services from the beginning of its operation with a concept of categorised separation of data in accordance with applicable laws and regulations. This will prove more efficient and cost-effective for the company when it decides to go on the cloud later.

As most tech companies operate across national borders, cross-border transfer of data is a key concern. Companies in certain sectors (eg, financial institutions, credit business agencies, insurance companies, medical institutions, ride-hailing service providers, and smart cars) are subject to data localisation requirements. In particular, CII operators may only transfer personal data and 'important data' out of China if they have completed the security assessment organised by the supervisory authority. The party initiating such transfer shall be the responsible party to carry

out the security assessment with the other parties to provide necessary assistance. However, the detailed implementation rules for such security assessment are still pending at the time of writing (see question 1).

Another notable concern is that cloud services are not entirely open for foreign investors in China. Foreign cloud service providers may need to cooperate with local partners to step into the China market. Therefore, users of cloud service providers with a foreign background need to consider the business model of the service provider and consider whether it will have any impact on the services requested.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The Chinese government takes serious cybersecurity threats and criminal activity seriously.

The CAC is the main regulator with first-hand knowledge of market trends and cybersecurity threats through law enforcement activities, based on which it will lead the promulgation of new or amended regulations to address such concerns.

Owing to the rapid development of mobile technologies, CAC and other competent regulators such as the MIIT, the Ministry of Public Security and the State Administration of Market Regulation have focused their law enforcement efforts in regulating mobile applications in recent years. These regulators have the authority under the law to request application stores to suspend or remove download channels for illegal applications.

If any criminal offence leads are discovered during their investigation or review, such cases will be referred by the CAC to the police to initiate criminal investigations. Individual citizens or entities, especially those victims of cybersecurity threats, are also encouraged to report crimes to the authorities.

The National Computer Network Emergency Response Technical Team/Coordination Center of China (also known as CNCERT/CC) publishes annual cybersecurity reports in China. In its 2021 half year report published in July 2021, CNCERT summarised the overall cybersecurity conditions in China, specific areas of cybersecurity issues (eg, malware, website security, cloud platform security, industrial control system security) and government responses and handling of security breaches. Law enforcement actions against cybersecurity threats are increasing, with targeted campaigns on a regular basis. Civil lawsuits and public interest lawsuits against cybersecurity breaches are also increasing.

There are likely to be criminal liabilities for data violations. According to China's Criminal Law, criminal penalties for computer hacking-related offences range from three- to five-year, or even longer, imprisonment sentences. For other crimes (eg,

fraud, theft and embezzlement) conducted via cybersecurity breaches, penalties for the same crimes (conducted in a traditional offline matter as set out in the Criminal Law) will also apply. In addition, the Draft Law on Anti-Telecom and Internet Fraud was submitted to the Standing Committee of the National People's Congress for first reading in October 2021 and the second reading is scheduled in late June 2022. This new Law aims at preventing and combating relevant crimes by telecoms, finance and internet regulations.

The Supreme Court and Supreme Procuratorate jointly issued the Judicial Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to the Information Network, which took effect on 1 November 2019. These judicial interpretations include quantified thresholds for punishable criminal offences, which provide guidelines to the police and prosecutors nationwide. The Supreme Court and provincial high courts regularly publish model cases in relation to cybersecurity crimes to raise public awareness and deter future offences. Although China does not have a case law tradition, to some degree these model cases also serve as precedents for lower-level courts to

"The Supreme Court and Supreme Procuratorate jointly issued the Judicial Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to the Information Network, which took effect on 1 November 2019."

rule on cases. As cybersecurity crimes tend to involve a large number of victims, the police and prosecutors usually take priority in handling these crimes.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

The risk factors vary for different M&A deals. For asset or equity deals with high privacy and data security concerns (eg, purchase of software with heavy collection of user data or the equity of a hotel chain with large customer check-in data or equities of a manufacturer with a large number of employees worldwide, among many other examples) privacy and data security liabilities should be a key, if not a deal-breaking, factor.

There are several steps to follow in order to minimise potential risks. First, a proper legal and technical due diligence must be done by the buyer. This is especially important for foreign investors who are not necessarily familiar with the relevant data implications in the China market. Often this exercise should be done against not only the Chinese law, but also the relevant laws to all the jurisdictions involved (eg, the portfolio companies have a cross-border structure established for capital financing reasons, or the investors have limited partners from different jurisdictions) which may trigger, among other things, cross-border data transfer concerns (again China has strict rules around cross-border data transfer). Note the due diligence findings may prove a no go, and if that is the case, of course the earlier the finding is made, the better for both parties. Second, subject to the due diligence findings, some rectification measures shall be taken either before signing, or as closing conditions or post-closing covenants (depending on circumstances). The buyer should consider requesting a reduction in the valuation of the target, escrow arrangement, etc, to hedge against potential liabilities. Certain representations and warranties should be customised with certain carveouts to reflect the due diligence findings. Third, subject to the magnitude of potential legal liabilities due to violations of privacy and data security, the buyer may insist on special compensation (which can be as severe as, for example, reversing the deal or down to the personal liabilities of the individual sellers) or offset of remaining payments (in the case of a payment schedule in several tranches with some payable after closing). Fourth, the buyer should consider relevant insurance policies to cover liabilities for privacy and data security violations.

From the seller's perspective, it is important to shortlist credible buyer candidates. Once serious negotiations have commenced with selected buyers, the seller shall provide full disclosure to the buyers under a satisfactory confidentiality agreement. Properly documented full disclosure is the right defence for any subsequent

buyer claim after closing. Further, as a general rule in M&A deals, the seller should consider setting certain time limits to provide any compensation, including for privacy and data security violations. Needless to say, operating in a compliant way (especially navigating the dynamic Chinese data law) from day one is important for the seller.

Jingyuan Shi
jingyuan.shi@simmons-simmons.com

Yuchen Lai
yuchen.lai@simmons-simmons.com

Simmons & Simmons
Hong Kong and Shenzhen
www.simmons-simmons.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Each law firm has its own focused practices. Clients should seek cybersecurity advice from lawyers who have a long-term track record of experience in navigating cybersecurity and data protection with a legal and a sectorial eye where relevant to the client. As cybersecurity often goes beyond national borders and more importantly nowadays data legislations from the key economies globally are influencing each other so heavily (especially the GDPR's impacts globally), lawyers with international practice and experience can offer more solid advice and input from a comparative perspective. Clients should evaluate a lawyer's observations on the latest legal and regulatory development for cybersecurity from international and regional perspectives as good lawyers are always on top of the latest legal developments. Last but not least, reputation or comments on lawyers generated from previous deals may also be key attributes clients should look for.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

There are multiple layers of laws and regulations on cybersecurity and privacy in China. Some have only recently been adopted and without any detailed implementation rules, some may be in the draft stage, and the cybersecurity and privacy related legal framework is evolving at extremely fast pace, with new legislations or drafts coming out almost every month. We anticipate that this trend will continue in the next couple of years. In addition, multiple regulators may be in charge of the supervision of the same issues from different perspectives. Therefore, a client needs expert advice to help correctly analyse their case and navigate in the complex legal and regulatory framework for cybersecurity and privacy compliance in China.

How is the privacy landscape changing in your jurisdiction?

The triangulated safeguard for data regulation, ie Cybersecurity Law, the Data Security Law and the Personal Information Protection Law, are all in place. Lower-level implementation regulations and recommendatory national standards will be drafted or amended accordingly. Key regulators will finalise their internal guidelines on law enforcement where applicable. All of these changes will shape the privacy