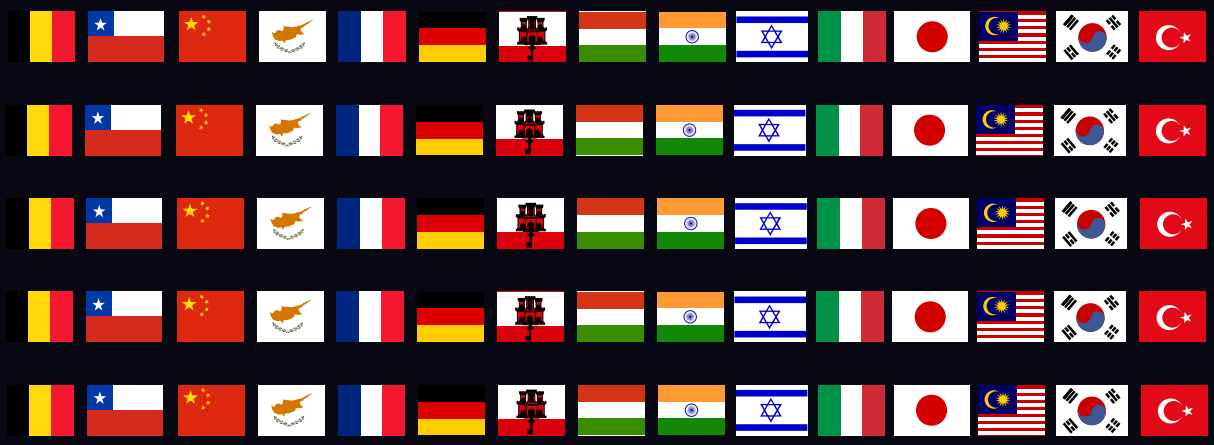
DIGITAL BUSINESS

China



LEXOLOGY
Getting The Deal Through

Consulting editor
Mishcon de Reya LLP

Digital Business

Consulting editors

Ashley Winton

Mishcon de Reya LLP

Quick reference guide enabling side-by-side comparison of local insights into legal and regulatory framework; contracting on the internet; security, including security of payment; domain names; advertising; financial services; defamation; intellectual property; data protection; taxation; gambling; outsourcing; online publishing; dispute resolution; and recent trends.

Generated 28 October 2022

Table of contents

Contributors

China

Jan Holthuis
j.holthuis@burenlegal.com
Buren NV

Li Jiao
l.jiao@burenlegal.com
Buren NV

Amsterdam
WTC - Tower C level 14
Strawinskylaan 1441
1077 XX - Amsterdam
Telephone +31 (0)20 333 83 90
The Netherlands

Shanghai
Room 2505B, ICC-Tower
North Zhongshan Road 3000
200063 - Shanghai
Telephone +86 (21) 6173 03 88
China

LEGAL AND REGULATORY FRAMEWORK

Government approach

How would you describe the government's attitude and approach to digital content and services, digital transformation and doing business online?

The Chinese government now pays attention to Internet issues at an unprecedented new level. Cybersecurity has officially become an important component of China's national security strategy. Internet legislation is at a higher level, with a wider field of application and a deeper degree of adjustment.

The Chinese government attaches weight to both state security and market-based regulatory systems.

Law stated - 22 July 2022

Legislation

What legislation governs digital content and services, digital transformation and the conduct of business online?

First, China has introduced several basic laws for cyberspace governance in recent years, including the E-Commerce Law, the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law. In the meanwhile, the supporting regulations of relevant departments are also being further improved, such as Cybersecurity Review Measures (2021) and Regulations for the Administration of Network Data Security (Draft for Comments).

Business on the internet is conducted under a licensing system in accordance with the Telecommunications Regulations. The Classification Catalogue of Telecommunications Services further defines and classifies the sub-categories of telecommunications business, according to which different types of telecommunications licences apply. Depending on the types, businesses on the internet may require, among others:

- an internet content provider licence;
- an online data processing licence; or
- a transaction processing services licence.

Related business operators can only conduct business after obtaining the corresponding licences.

In addition, conducting businesses on the internet shall also comply with legislation applicable to each specific industry and transaction model, such as the Electronic Signature Law, the Advertising Law 2021 and the Encryption Law.

Law stated - 22 July 2022

Regulatory bodies

Which regulatory bodies are responsible for the regulation of digital content and services, e-commerce, data protection, internet access and telecommunications?

The Department of Electronic Commerce and Information Technology of the Ministry of Commerce is mainly responsible for supervising companies engaged in e-commerce business. As the main implementing department of the E-commerce Law, the State Administration for Market Regulation also plays a crucial role in the supervision of e-commerce operators.

In terms of data security protection, the Ministry of Public Security is mainly responsible for network security protection, while the Cybersecurity Administration of China and the Ministry of Industry and Information Technology (MIIT) are responsible for network security risk assessment. Internet access is also largely regulated by MIIT.

Law stated - 22 July 2022

Jurisdiction

What tests or rules are applied by the courts to determine the jurisdiction for online transactions or disputes in relation to digital businesses in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

For foreign-related disputes, including internet-related transactions or disputes, the courts will apply the Civil Procedure Law and Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law (Amendment 2022) (the 'Interpretation') to make decisions.

As stipulated in the Interpretation of the Civil Procedure Law, the parties involved can reach a consensus on the choice of jurisdiction of a foreign court in the place where the dispute is associated, as long as the choice of forum does not conflict with the provisions on court-level jurisdiction and exclusive jurisdiction.

In the absence of a choice of the parties, the jurisdiction should be determined in accordance with the provisions of the Civil Procedure Law and the Interpretation. For example, with respect to a contract dispute, the competent court shall be the people's court at the place where the defendant is domiciled or where the contract is performed.

The place of performance is further clarified by the Interpretation. If the subject matter is payment of money, the place where the party receiving the money is located shall be the place where the contract is performed; if the subject matter is delivery of immovable property, the place where the immovable property is located shall be the place where the contract is performed; as for any other subject matter, the place where the party fulfilling obligations is located shall be the place where the contract is performed. As for a contract with instant settlement, the place of transaction shall be the place where the contract is performed.

With regard to an online sales contract, when the subject matter is delivered through the internet, the place where the buyer is domiciled shall be the place of performance; if the subject matter is delivered by other means, the place of receipt is the place whether the contract is performed.

Law stated - 22 July 2022

Establishing a business

What regulatory and procedural requirements govern the establishment of digital businesses and sale of digital content and services in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

There is no major difference between establishing a digital business and establishing a brick-and-mortar business in China. Most digital business operators shall complete market entity registration formalities, as stipulated in the E-commerce Law. The regulatory and procedural requirements that govern the establishment of digital businesses are as follows.

Choosing business vehicles

To establish a business in China, the first question to be considered should be which business vehicles to choose. The

main business vehicles in China include a limited liability company, a partnership and a company limited by shares. As for foreign-invested enterprises, establishing a representative office instead of a separate legal entity is also available.

Pre-examination and approval procedures

The second step is to confirm whether the enterprise needs to go through the pre-examination and approval procedures. The pre-examination and approval procedures include three considerations:

- whether or not the project involves approval or filing according to the Administrative Measures on Approval and Filing for Foreign Investment Projects, and the Catalogue of Investment Projects Subject to Governmental Approval;
- whether or not the project is involved in the Administrative Measures (Negative List) for Foreign Investment Access; and
- whether or not a preliminary licence for entry into a specific industry is involved – this is not a pre-procedure aimed at foreign investment, but an administrative licence requirement for conducting business in specific industries or activities.

Business registration

If the pre-examination and approval procedures are not required, or the approval documents have been obtained, investors can officially initiate the business registration procedures, including:

- business name registration: the name of a company is subject to pre-approval, and the pre-approved name will be reserved for six months; and
- after the company name is pre-approved, investors can submit documents to apply for registration and obtain a business licence through the local Administration for Market Regulation or the online enterprise registration system.

Relevant identification certificates

After the registration is completed, the foreign-invested enterprise's information will be automatically synchronised to other departments. Investors should then complete the following procedures:

- carve and record official seals in the public security department;
- collect the invoice from the tax department;
- complete social security registration via the online platform;
- apply for foreign exchange registration with the foreign exchange administration department; and
- open a public account in a bank.

After completing these formalities, the enterprise shall check whether additional administrative licensing is required before starting its business.

Law stated - 22 July 2022

CONTRACTING ON THE INTERNET

Contract formation

Is it possible to form and conclude contracts digitally? If so, how are digital contracts formed and are there any exceptions for certain types of contract?

In general, parties can conclude a contract electronically in China. According to article 469 of the Civil Code, the parties may conclude a contract in writing, orally or in some other form. Any electronic data that can show, in material form, the contents that it specifies through electronic data exchange or email and can be accessed for reference and used at any time shall be regarded as a written form. Where the parties conclude a contract in the form of electronic data and subject to the execution of a letter of confirmation, the contract shall be established at the time of execution of the letter of confirmation. Where the information of any commodity or service released by one party via the internet or any other information network meets the conditions of offer, the contract shall be established when the other party selects such commodity or service and submits the order successfully, unless otherwise agreed by the parties.

Only certain types of contracts cannot be concluded electronically, such as documents related to personal relationships (marriage, adoption and succession), conveyance of rights and interests on real estate, and stay of public services.

If the contract is an online sales contract, a click-to-accept process can be adopted. As long as the online contract does not violate the provisions on validity of contract under Chinese law and is deemed a legally valid contract, the contract can be enforced in China. For example, where a term in a contract unconditionally restricts the rights and interests of the parties to a 'click-wrap' contract, the term might be deemed unenforceable.

Law stated - 22 July 2022

Applicable laws

Are there any particular laws that limit the choice of governing law, language of the contract or forum for disputes when entering into digital contracts? Do these distinguish between business-to-consumer and business-to-business contracts?

In the contract law section of the Civil Code, specific provisions are provided for the conclusion and performance of electronic contracts.

The E-Commerce Law is the main piece of legislation in China that regulates conduct of online business activities, including electronic contracts. The Electronic Signature Law is also relevant for online contracting. The Electronic Signature Law recognises that, under prescribed circumstances, electronic data messages can have the same legal effect as an original document or a written document.

In addition, the Process Specification for Online Conclusion of Electronic Contracts, a mandatory national standard approved and issued by the Ministry of Commerce in 2013, stipulates general process guidelines for e-commerce parties to follow when concluding electronic contracts via the internet in China.

Law stated - 22 July 2022

Electronic signatures

How does the law recognise or define digital or e-signatures? Must digital or e-signature providers be registered or licensed in your jurisdiction?

In China, the Electronic Signature Law mainly regulates the conduct of electronic signature and confirms the legal validity of electronic signature. Parties involved in civil activities may agree to use, or not to use, electronic signature and data telex for contracts or other documents and instruments.

Electronic signature usually refers to data incorporated into or associated with any electronic form, which may be used to identify the signatory and indicate the signatory's approval of the information contained in the data telex. 'Data telex' means information generated, sent, received or stored by electronic, optical, magnetic or similar items.

Electronic signatures have the same legal validity as wet-inked signatures or affixation of seal, provided that the electronic signature has satisfied the conditions provided by law. Documents for which the parties involved agree to the use of electronic signature or data telex shall not be denied of legal validity on the ground of electronic signature or data telex being used. However, e-signatures cannot be used in documents or instruments related to personal relationships, conveyance of real estate and stay of public services.

At present, Chinese laws only regulate the form, function and effect of electronic signatures without specifying the specific technical means. Therefore, there is no unique format for electronic signature.

Law stated - 22 July 2022

Breach

Are any special forums for dispute resolution or remedies available for the breach of digital contracts?

Common remedies for breach of both electronic and offline contracts are the same, including damages compensation, permanent injunctions and specific performance.

Law stated - 22 July 2022

FINANCIAL SERVICES

Regulation

Is the advertising or selling of financial services products to consumers or to businesses digitally or via the internet regulated? If so, by whom and how?

On 28 July 2015, 10 Chinese central regulatory agencies and industry regulators, including the People's Bank of China, the China Banking Regulatory Commission, the China Insurance Regulatory Commission and the China Internet Information Technology Office jointly released the Guiding Opinions on Promoting the Healthy Development of Internet Finance (the Guiding Opinions), which is the first comprehensive regulation issued by the Chinese government in relation to internet finance.

In the Guiding Opinions, the government set out general rules, basic rules and specific preferential measures relating to internet finance, covering internet payments, online lending, equity crowdfunding, internet fund sales, online insurance services and internet consumer finance.

In late 2021, Chinese financial regulators have demanded fintech firms to rectify prominent issues, including:

- putting all financial activities under supervision;
- requiring that all financial businesses have a certificate; and
- cutting off the improper linkage between payment tools and other financial products.

Also, internet firms are required to strictly control the expansion of non-banking payment accounts to the public domain. They are also required to strengthen the management of key procedures, including the certification of shareholders, ownership structure, and capital, risk isolation and related transactions.

Internet firms should also strengthen the protection mechanism of consumers, including regulating how personal information is collected and marketed, and the text of standard contracts.

Law stated - 22 July 2022

Electronic money and digital assets

Are there any rules, restrictions or other relevant considerations regarding the issue of electronic money, digital assets or use of digital currencies?

Electronic banking

The Electronic Payment Guidelines (No. 1), promulgated by the People's Bank of China (PBOC), is the first document that sets out banks' liability regarding online payment. The Measures for Management of Electronic Banking and the Guidance on Evaluation of Electronic Banking Security issued by the China Banking and Insurance Regulatory Commission generally govern the electronic banking business.

Third-party payment

Third-party payment operators are defined as non-bank institutions that handle internet payments, mobile phone payments, fixed-line payments, digital television payments and other network payment services.

The regulator of third-party payment is the PBOC and its branches. The core of the policy is the Measures for the Administration of Payment Services by Non-Financial Institutions, supplemented by industry self-regulation and supervision by commercial banks. Due to the rapid development of third-party payments, the PBOC has introduced more policies to regulate third-party payments since 2014.

The promulgation of the E-Commerce Law in 2019 brought new requirements to electronic payment service providers, including requirements to:

- notify users of the functions of electronic payment services, use methods, points to note, the relevant risks and fee rates, etc;
- not impose unreasonable transaction conditions;
- ensure the integrity, consistency, trackability and resistance against tampering of electronic payment instructions;
- provide account reconciliation service and transaction records of the past three years to users free of charge;
- promptly investigate and identify the reason for errors in payment instructions, and adopt the relevant measures to correct the error; and
- bear compensation liability where an error causes the user to suffer losses, except where it can be proven that the error in the payment instruction was not caused by the electronic payment service provider.

Law stated - 22 July 2022

Digital and crypto wallets

Are there any rules, restrictions or other relevant considerations regarding the provision or use of crypto wallets or other methods of digitally storing value?

There are no particular rules to restrict developing or supplying crypto wallets or other methods of digitally storing value. However, for the time being, China has a strictly prohibitive attitude towards the issuance and trading of crypto currencies. Financial institutes are forbidden from engaging in financing services and exchange of crypto currencies.

Law stated - 22 July 2022

Electronic payment systems

How are electronic payment systems regulated in your jurisdiction? Is there a specific law regulating third-party access to digital information in bank accounts?

There are mainly two types of electronic payments in China: online banking payment and third-party payment (Alipay, WeChat). Online banking payment is regulated by the Electronic Payment Guidelines (No. 1) issued by the People's Bank of China in 2005. The guidance clarifies the obligations of banks when using electronic payment (which include the application of electronic payment, the initiation and receipt of electronic payment instructions and the measures of safety control and error handlings).

Third-party payment like Alipay and WeChat is in widespread use from metropolis to remote countryside in China. Third-party payment institutions are now under the regulation of the People's Bank of China and its subordinate units. In 2017, the People's Bank of China issued a total of 106 administrative penalty decisions against third-party payment institutions, many of whom were blamed for not being adherent to the administrative measures issued by the People's Bank of China. Besides, with respect to the conditions for third-party payment institutions carrying out business and their business practices, new normative documents in draft version have set up more strict and comprehensive requirements, including but not limited to anti-monopoly regulatory measures, higher paid-up capital and account classification management.

Third-party access to digital information in bank accounts is subject to regulation under the Civil Code, the Personal Information Protection Law, the Commercial Banking Law and the Consumer Rights and Interests Protection Law, as well as departmental regulations such as the Implementation Measures of the People's Bank of China on the Protection of the Rights and Interests of Financial Consumers. Third-party access to personal bank account information requires the individual's consent, with the exception of requirements by law-enforcement departments.

In addition to the laws, the Technical Specification for the Protection of Personal Financial Information provides a technical standard especially for financial institutions entrusting the processing of personal financial information to third parties. It stipulates that the entrustment should not exceed the scope of the consent of the subject of the personal financial information. And it places more detailed demands on the entrusted third-party institution.

Law stated - 22 July 2022

Online identity

Are there any rules, restrictions or other relevant considerations regarding the use of third parties to satisfy know-your-customer (KYC) or other anti-money laundering (AML) identification requirements?

Pursuant to the China Anti-Money Laundering Law, where a financial institution determines the identity of a customer

through a third party, it shall ensure that the third party has adopted measures for determining customer identity complying with the requirements of this Law. And where the third party has not adopted measures for determining customer identity that comply with the requirements of this Law, the financial institution shall bear the liability of not fulfilling the obligation of determining customer identity. Generally, Chinese law permits the use of third parties to satisfy know-your-customer requirements. In 2022, the People's Bank of China released a regulation requiring financial institutions to assess third parties' risk status and ability to perform the obligations of anti-money laundering and counter-terrorist financing.

Nevertheless, when it comes to customer identity for credit card applications, the Credit Card Business Regulations promulgated by the China Banking and Insurance Regulatory Commission and the People's Bank of China stipulate that banking financial institutions shall accept credit card applications, collect customer information and verify customers' identities via their own channels, instead of relying on an internet platform, webpage or any other electronic channel operated or controlled by any cooperative agent. In cases of inquiries regarding bills or payables via the aforesaid electronic channels, prior consent should be obtained from customers and necessary measures must be taken to ensure the security of customers' personal information.

Law stated - 22 July 2022

DOMAIN NAMES AND URLS

Registration procedures

What procedures are in place to regulate the licensing of domain names or use of URLs? Is it possible to register a country-specific domain name without being a resident in the country? Are there any restrictions around the use of URLs to direct users to websites, online resources or metaverses?

To take ownership of a domain name, applicants for registration shall register (purchase) the possible domain name from the China Internet Network Information Centre (CNNIC) or the qualified registrars accredited by the CNNIC that then shall provide an electronic certification.

There are no filing formalities for domain names in China. However, applicants who use the registered domain name for a website shall fulfil the website filing formalities with the competent department, according to the Administrative Measures on Internet-based Information Services.

It is possible for a resident to register a country-specific domain name in China without that resident being in China. In China, a country-specific domain name refers to a .cn or a .□ □ domain name. The Implementing Rules for the Registration of National Top-level Domain Names 2019 provide that no restriction is imposed against non-residents to register a .cn or a .□ □ domain name. Additionally, the Ministry of Industry and Information Technology also specifies the permitted registrants, either individuals or entities.

Law stated - 22 July 2022

IP ownership

Can domain names or URLs be the subject of trademarks or copyright protection in your jurisdiction? Will ownership of a trademark or copyright assist in challenging a competitive use or registration of a similar domain name or URL?

The Anti-Unfair Competition Law defines the unauthorised use of the main part of another party's domain name, website name, web page, etc, that are influential as misleading acts, which may cause the public to misidentify the

goods concerned as another party's goods or to associate the goods concerned with those of another party, which therefore constitute unfair competition acts.

Law stated - 22 July 2022

ADVERTISING

Regulation

What rules govern online advertising?

The governing rules are the following.

- Legislation: the Advertising Law 2021, as amended.
- Administrative regulations:
  - the Interim Measures for Administration of Internet Advertising 2016; and
  - the Provisions on the Governance of Network Information Contents Ecosystem 2019.
- Self-regulatory codes: the China Advertising Association is the industrial self-discipline association for advertising, which formulated and promulgated self-regulatory codes for the advertising industry (eg, the Self-Regulation of the China Advertising Association and the Self-Discipline Pact).

Law stated - 22 July 2022

Targeted advertising and online behavioural advertising

What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

Online advertising is defined as commercial advertisements that directly or indirectly promote goods or services through websites, web pages, internet applications and other internet media in the forms of texts, pictures, audios, videos, etc.

Online editorial content can be regarded as online advertising provided that there is a paid promotion of goods or services, directly or indirectly, for profit. According to the Advertising Law 2021, commercial advertising shall involve the activities carried out by sellers of goods or service providers to promote their goods or services, directly or indirectly, through a certain medium and form. Therefore, editorial content shall be caught by the rules governing advertising only if it can meet this condition.

Law stated - 22 July 2022

Misleading advertising

Are there rules against misleading online advertising?

The rules against misleading online advertising are mainly set forth in Anti-Unfair Competition Law 2019, the Advertising Law 2021 and the Interim Measures for Administration of Internet Advertising 2016.

Under the Advertising Law 2021, a wider variety of advertisements are now vulnerable to scrutiny for false advertising. Advertisers are now required to substantiate all claims and statements regarding their truthfulness to avoid non-compliance. The use of technical or digital methods to create or enhance the true effect of a product or service in

advertisements, in particular, is penalised as false advertising.

There are no explicit standards governing which evidence advertisers should keep in relation to advertisement substantiation.

While the above rules are applied centrally, there are still some strict rules regarding specific areas of online advertising.

Law stated - 22 July 2022

Restrictions

Are there any digital products or services that may not be advertised online?

General rules in the Advertising Law 2021 include that the following shall not be advertised:

- narcotic drugs;
- psychotropic substances;
- toxic drugs for medical use;
- radioactive pharmaceuticals and other special drugs;
- drug precursor chemicals; and
- pharmaceuticals, medical machinery and treatment methods for drug abuse rehabilitation.

Prescription drugs other than those stipulated in the above list may only be advertised in medical or pharmaceutical professional journals that are jointly designated by the health department of the State Council and the drug regulatory department of the State Council.

Special rules in Interim Measures for Administration of Internet Advertising 2016 state that it is not allowed to design, produce, act as agents for or publish on the internet any advertisements for goods or services the production, sales or provision of which are prohibited by laws and administrative regulations, or any advertisements for goods and services that are prohibited from being published. It is also prohibited to publish advertisements for prescription drugs and tobacco via the internet.

Law stated - 22 July 2022

Hosting liability

What is the liability of content providers and parties that merely host the content, such as ISPs? Can any other parties be liable?

Article 45 of the Advertising Law 2021 stipulates that internet information service providers shall curb the posting and publishing of illegal advertisements through their information transmission and distribution platform of which they are aware or should be aware.

For any violation of these provisions, the State Administration for Market Regulation shall confiscate the illegal income. Where the amount of the illegal income is 50,000 yuan or above, a fine ranging from one to three times the amount of the illegal income shall be imposed simultaneously. Where the amount of the illegal income is less than 50,000 yuan, a fine ranging from 10,000 to 50,000 yuan shall be imposed simultaneously. In serious cases, the relevant authorities shall order the offender to stop the relevant businesses.

Law stated - 22 July 2022

Email marketing

What regulations and guidance apply to email, SMS and other distance marketing?

Email, SMS and other distance marketing are supervised by the Interim Measures for the Administration of Internet Advertising and the Advertising Law.

Unsolicited marketing is not allowed in China. The Interim Measures for the Administration of Internet Advertising and the Advertising Law explicitly prohibit advertisers from attaching advertisements to, or including advertising links in, replies to emails sent by users without their permission.

Also, the Advertising Law regulates the sending of advertisements by means of electronic messages, requiring any entity or individual to obtain the consent or request of the person concerned before sending the advertisement, and to provide the recipient with a means to refuse to continue receiving the advertisement after it has been sent. Otherwise, the advertiser shall be subject to administrative liability, which includes orders for corrections and fines.

In the draft revision for the Interim Measures for the Administration of Internet Advertising released in 2021, it further specifies that no advertisements or links to advertisements shall be attached to emails or internet instant messaging, and no internet advertisements shall be sent to users' vehicles, navigation devices, smart home appliances, etc without the consent or request of the person concerned. Otherwise, advertisers, operators and publishers of advertisements shall bear administrative liabilities, which include orders for corrections, confiscation of illegal income and imposition of fines.

Law stated - 22 July 2022

ONLINE PUBLISHING

Content liability

When would a digital platform or online content provider be liable for mistakes in information that it publishes online? Can it avoid liability? Is it required or advised to post any notices in this regard?

The internet service provider (ISP) shall not bear liability for infringement when the relevant copyright owner fails to issue a warning or provide any other information that is sufficient to make the ISP aware of such an infringement. The necessary measures taken by the ISP include the technical approaches that may directly prevent the occurrence of infringement consequences, such as deleting infringing content, breaking links and filtering keywords.

After receiving the notice, if the ISP still does not remove the infringing link within a reasonable period resulting in the further expansion of the damage, it will bear the legal responsibility for such additional damages.

Law stated - 22 July 2022

ISP liability

Are internet service providers (ISPs) liable for content displayed on their sites? How can ISPs limit or exclude liability?

Article 1,195 of the Civil Code provides that, if an internet user has engaged in tortious conduct through the internet, the injured party shall have the right to notify the ISP and request that it take necessary measures such as deleting content, screening content or denying services to the offending individual. Where an ISP fails to take necessary measures in a

timely manner after being notified of such offences, it shall bear – jointly and severally with the internet user – liable for increased damages caused by the failure of the ISP. The provision provides ISPs with a safe harbour from defamation claims if they implement the aforementioned notice and takedown procedures.

Law stated - 22 July 2022

Shutdown and takedown

Can an online content provider or ISP shut down a web page containing defamatory material without court authorisation?

Yes, shutting down a web page containing defamatory material could be one of the requisite measures according to article 1,195 of the Civil Code. It is an ISP's obligation to take requisite measures if the injured party sends a notice of infringement to the ISP, providing the preliminary evidence of infringement and its true identity information. With respect to which specific requisite measure or measures shall be taken, the ISP shall, based on the preliminary evidence for infringement and the type of services, make the decision accordingly.

Law stated - 22 July 2022

INTELLECTUAL PROPERTY

Data and databases

Are data and databases protected by IP rights?

If the website provider owns the copyright on the database, then the website provider has the right to ask others to stop using or copying the data in the database.

Law stated - 22 July 2022

Third-party links and content

Can a website, digital platform or other online content provider link to third-party websites or platforms without permission?

Yes. Legal practice in China deems that the link itself does not contain any content and therefore is not subject to the control of the right to network dissemination of information. In 2012, the Supreme People's Court published the Provisions on Several Issues Concerning the Application of Law to Trial of Civil Dispute Cases of Infringement of the Right to Network Dissemination of Information, stipulating that the internet service provider (ISP) whose conduct constitutes joint infringement with other parties shall bear joint and several liabilities, but also providing an exemption for the ISP if it only provides a link.

However, for built-in deep linking behaviour, it is a different case. Deep linking is a technical means that allows users to directly see the content of the linked website on the linking website without a webpage transition.

Law stated - 22 July 2022

Can a website, digital platform or other online content provider use third-party content, obtained via automated scraping or otherwise, without permission from the third-party content provider?

No. Where a network user or an ISP provides works, performances, and audio and video products via an information

network without the permission of the right holder for network dissemination of information, such provisions shall be deemed an infringement of the rights to network dissemination of information. Meanwhile, making available works, performances, and audio and video products in the information network by means of uploading to a network server, setting up shared files or using file-sharing software, etc, that enables the general public to download, browse or by other means obtain them at any desired time and location shall be deemed constitutions of the aforesaid provisions.

Law stated - 22 July 2022

Metaverse and online platforms

Are there any particular difficulties with establishing or defending copyright, database rights and trademarks on a metaverse from your jurisdiction?

The legislation for the metaverse and virtual property is still under development. At the current stage, intellectual property protection in the metaverse faces a few difficulties.

First, the rules for evidence collection and burden of proof concerning infringement of intellectual property rights (IPR) in the metaverse are unclear. For instance in commercial practice, virtual reality (VR) service providers usually only conduct formal review and ignore substantive review, leading to the problem of copyright infringement where many VR applications are copied illegally.

Second, the general laws applied for IPR infringement may become inapplicable for IPR infringement in the metaverse. For example, 'without the consent of the trademark registrant, replaces his registered trademark and puts the goods with the replaced trademark back on the market' is stipulated as an act of trademark infringement according to the Trademark Law. However, it becomes difficult to identify such acts since only virtual products, not physical objects, exist in the metaverse.

Third, according to the current IPR protection law system, a trademark is only protected within the territory where the trademark is registered. However in the metaverse, the territoriality of IPR protection may be challenged.

Law stated - 22 July 2022

Exhaustion of rights and first-sale doctrine

Does your jurisdiction recognise the concept of exhaustion of rights or the first-sale doctrine? If so, how does it apply to digital products? Can rights be exhausted by placing the digital product on a metaverse or other platform in another territory?

The principle of exhaustion of rights has been recognised by PRC law in some areas.

For example, in new plant variety rights protection, the Supreme People's Court proposed that, after the variety right-holder authorises or licenses the plant variety material to be sold, it shall not claim that the production, propagation or sale of such plant material by others constitutes infringement (exceptions apply). Similarly, the PRC patent law stipulates that once the patented products are sold by the patentee or its licensee, the use, offer for sale, sale and importation of such products no longer constitute infringement of the patent right.

Regarding digital products, the Copyright Law and Regulations on Computer Software both indicate that for legally distributed copies of software, the right-owner's distribution right has been exhausted.

In April 2022, the PRC's first non-fungible token (NFT) infringement case was decided by Hangzhou Internet Court. The judgment denied application of the principle of exhaustion of rights for NFT digital products. It reasoned that the principle is based on the inseparability of the work itself and its tangible carrier. Since the distribution of NFT digital

works does not lead to the distribution of their tangible carriers, NFT digital works do not meet the prerequisite to apply the exhaustion of rights principle.

In addition, the original purpose of the exhaustion of rights principle is to balance the conflict of interests between the copyright owner and the legitimate buyer, but NFT digital works can be copied without cost and in unlimited quantities, so unauthorised duplicates and distribution would seriously harm the interests of the copyright owner.

This case is a preliminary exploration of Chinese justice in the field of the metaverse. As discussion over the topic grows, more authoritative legislation is expected in the near future.

Law stated - 22 July 2022

Administrative enforcement

Do the authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

The term 'dawn raid' is not directly incorporated into Chinese law, but the most similar existing concepts are administrative or criminal investigations (inspections), which allow law enforcement to conduct on-site inspections as well as search corporate records and files to gather information and evidence on suspected violations of law.

In administrative procedures, which are usually initiated by a complaint filed by the intellectual property (IP) right holder, the competent administrative authorities – such as the Copyright Bureau in a case of copyright infringement – do not have the power to issue a freezing injunction. However, in terms of dawn raids, the administrative authorities may, when investigating the suspected infringement;

- question the relevant parties;
- investigate the matters relating to the alleged illegal acts;
- conduct on-site inspections of premises and articles of the parties concerned that involve alleged illegal acts;
- inspect and make copies of contracts, invoices, account books and other relevant materials relating to the alleged illegal acts; and
- seal up or seize the premises and articles involving the alleged illegal acts.

Law stated - 22 July 2022

Civil remedies

What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

Civil remedies rendered in a civil judgment may include ordering the infringers to stop infringement, eliminate impact, apologise or compensate losses to IP owners.

Search orders and freezing injunctions are available under different circumstances. Freezing injunctions are available as a preservation measure before and during the litigation.

After the civil judgment comes into effect, the IP owner may file an application for enforcement with the enforcement division of the court.

If the infringer does not perform the obligations ordered in the civil judgment, the court shall have the right to enquire about the infringer's properties and issue freezing injunctions. If the infringer does not perform the obligations ordered in the civil judgment and conceals its properties, the court shall have the right to issue a search order signed by the president of the court. The court shall also have the right to conduct a search on the infringer and its residence or the

place where the property is concealed.

Law stated - 22 July 2022

DATA PROTECTION AND PRIVACY

Definition of 'personal data'

How does the law in your jurisdiction define 'personal data'? Are any other categories of personal data defined in the law? If so, what additional rules apply to the processing of such categories of personal data?

The Personal Information Protection Law (PIPL), effective as of 1 November 2021, defines personal information and personal data as:

> *'all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously. The processing of personal information includes the collection, storage, use, processing, transmission, provision, disclosure and deletion, etc. of personal information.'*

Sensitive personal information refers to the personal information that is likely to result in damage to the personal dignity of any natural person, or damage to his or her personal or property safety once disclosed or illegally used, including information such as biometric identification, religious belief, specific identity, medical health, financial account, whereabouts and previous location history, as well as the personal information of minors under the age of 14.

Additional rules apply to the processing of sensitive personal data including, subject to the individual's separate consent (written consent is required in some cases), the need to inform the individual of the necessity of processing his or her sensitive personal information and the impact on his or her personal rights and interests. The consent of a minor's parents or other guardians in the case of processing the personal information of a minor under the age of 14 must be obtained.

Information processed anonymously is currently not regulated.

Law stated - 22 July 2022

Registration and appointment of data protection officer

Do parties involved in the processing of personal data have to register with any regulator to process personal data? Does the law prescribe the appointment of a data protection officer?

The Cyberspace Administration of China (CAC) is the competent authority for leading and coordinating the supervision of personal information processors. Meanwhile, other government departments including the Ministry of Industry and Information Technology, the Ministry of Public Security and the State Administration for Market Regulation (SAMR) are responsible for protecting, supervising and administering the protection of personal data within the scope of their respective duties. Currently, there is no regulatory registration system designed for personal information processors. However, this does not mean personal information processors in China can avoid supervision.

The Personal Information Security Standards 2020 regulate the personal information protection officer system. Where a personal information processor meets any of the below thresholds, it shall designate a personal information protection officer:

- if it processes personal information as its main business and has more than 200 employees;
- if it processes the personal information of more than one million people or expects to process the personal information of more than one million people within the next 12 months; or
- if it handles the sensitive personal information of more than 100,000 people.

Law stated - 22 July 2022

Extraterritorial issues

Can data protection laws and regulatory powers apply to organisations or individuals resident outside your jurisdiction? Is there a requirement for such an organisation or individual to appoint a representative in your jurisdiction?

The PIPL shall apply to all processing activities of personal information that occur in China. The PIPL also applies to the processing activities of personal information that occur outside China if:

- the purpose of such processing activity is to provide products or services to a natural person within China; or
- the activities of the natural person within China are analysed and evaluated.

Where a personal information processor needs to transfer personal data outside China, it shall:

- get the certificate issued by a specialised agency appointed by the CAC;
- pass the security evaluation organised by the CAC; and
- enter into a contract with the overseas recipient under the standard contract formulated by the CAC.

In addition, the personal information processor shall take necessary measures to ensure that the overseas recipient also satisfies Chinese standards.

Foreign national residents within China will also be protected by the PIPL.

Law stated - 22 July 2022

Bases for processing

What are the commonly asserted reasons or bases for processing personal data and for exporting or transferring personal data to another jurisdiction?

With globalisation and the booming of the internet economy, there are many scenarios in which enterprises transfer domestic personal information across borders to foreign countries. The following are the most commonly seen:

- global enterprises require their subsidiaries, branches or representative offices in the PRC to transfer management information, such as personal information of employees, to the headquarters abroad;
- companies collect personal information during business operations in the PRC, and then share it with their foreign parent companies;
- cross-border e-commerce operators store personal information on servers outside the PRC, or outsource their personal information processing to companies abroad;

- cross-border service providers, such as of insurance, medical care, tourism and study consultancy, collect personal information in the PRC and store it on a server abroad or provide it to foreign companies; and
- enterprises provide investigation and evidentiary materials involving personal information to offshore government departments and parent companies, for the purpose of anti-fraud investigations, offshore litigation and arbitration bodies.

Law stated - 22 July 2022

Data export and data sovereignty

Are there any rules, restrictions or other relevant considerations concerning the export or transfer of personal data to another jurisdiction? Are there any data sovereignty or national security rules which require data, data servers or databases to remain in your jurisdiction?

The Security Assessment Measures for Outbound Data Transfers have been formulated specifically for the regulation of data export, and will take effect from 1 September 2022. Meanwhile, the Personal Information Protection Law, Data Security Law and Cybersecurity Law supervise the export or transfer of personal data to another jurisdiction.

Under the Security Assessment Measures for Outbound Data Transfers, to provide data abroad under any of the following circumstances, a data processor must declare a security assessment for its outbound data transfer to the Cyberspace Administration of China (CAC) through the local cyberspace administration at the provincial level:

- where a data processor provides critical data abroad;
- where a key information infrastructure operator or a data processor processing the personal information of more than one million individuals provides personal information abroad;
- where a data processor has provided personal information of 100,000 individuals or sensitive personal information of 10,000 individuals in total abroad since 1 January of the previous year; and
- in other circumstances prescribed by the CAC for which declaration for security assessment for outbound data transfers is required.

According to the security assessment result, the CAC may rule the data provider to terminate the data export.

Law stated - 22 July 2022

Sale of data to third parties

May a party sell or transfer personal data to third parties, such as personal data about users of an online service or digital platform?

The sale of personal data is strictly prohibited in China. Serious cases would be subject to criminal punishment.

Law stated - 22 July 2022

Consumer redress

What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

The right to personal information mainly includes the following subsidiary rights.

- The privacy disposition right: the right of a person to directly control and dominate his or her personal data. The person also has the right to decide whether, and in what manner, purpose and scope, his or her personal data will be collected, processed and used.
- The privacy secrecy right: the right of a person to request that information be kept confidential by the information processing subject.
- The inquire right: the right of a person to enquire about his or her personal information and the processing thereof, and to request a response. The control of information must begin with knowing what personal information is collected, processed and used, and whether the information is kept complete, correct and up to date in the process.
- The correct or supplement right: the right to request the subject of information processing to correct and add to personal information that is incorrect, incomplete or, from time to time, new.
- The deletion right: the right to request the information processing subject to delete personal information for legal or agreed reasons.

The protection of personal information is applicable to the activities of processing the personal information of natural persons in China and applies to the principle of territoriality, without distinguishing by nationality.

Law stated - 22 July 2022

DOCUMENT DIGITISATION AND RETENTION

Digitisation

Do the rules in your jurisdiction require any particular document or record types to be kept in original paper form and not converted solely to a digital representation?

China encourages and supports the digitisation of archives. The general law governing document retention, the Archival Law, does not require any particular document or record types to be kept in original paper form and not converted solely to a digital representation. Instead, it emphasises that electronic archives and archives carried in traditional forms have the same legal effect, and in the case of digitalised archives, the original archives shall be properly kept.

Law stated - 22 July 2022

Retention

Do the rules in your jurisdiction stipulate a minimum or maximum period for which documents or other record types should be kept?

The National Archives Administration of China formulates regulations for different authority systems, stipulating minimum retention periods or permanent retention for different types of documents.

For example, the National Archives Administration of China and the Supreme People's Court collaboratively promulgated the Measures for the Administration of Litigation Archives of the People's Courts in 2013, which stipulate three retention periods: at least 20 years, at least 60 years and permanent retention. Those litigation archives with long-term value for investigation and utilisation shall be classified as permanent retention, such as those pertaining to cases with a death sentence. Those litigation archives with relatively long-term value for investigation and utilisation shall be classified to be kept for at least 60 years, such as those pertaining to cases with fixed-term imprisonment sentences of 5–15 years. Those litigation archives with short-term value for investigation and utilisation shall be classified to be kept

for at least 20 years, such as those pertaining to cases with fixed-term imprisonment sentences of less than 5 years.

Law stated - 22 July 2022

DATA BREACH AND CYBERSECURITY

Security measures

What measures must companies take to guarantee the cybersecurity of data, communications, online transactions and payment information? Does any regulation or guidance provide for a particular level of cybersecurity or specific procedures to avoid data breaches? Are there any commonly used cybersecurity standards?

E-commerce business operators

The E-Commerce Law sets out the following requirements which should be met by E-commerce business operators:

- collect and use the personal information of their users compliant with the provisions of laws and administrative regulations on the protection of personal information.
- adopt technical measures and other requisite measures to ensure secured and stable operation of their network, prevent cybercrime activities, deal with cyber security incidents effectively, and ensure the security of e-commerce transactions.
- formulate cyber security incident emergency plans, and forthwith trigger the emergency plans upon the occurrence of a cyber security incident, adopt the corresponding remedial measures, and report to the relevant competent authorities.

Internet service providers

The Cybersecurity Law provides more requirements for internet service providers (ISPs) to ensure the security of internet transactions. ISPs must:

- provide network products and services satisfying the mandatory requirements in the applicable national standards;
- not install malware;
- immediately take remedial action against any risk such as security defects or bugs that are found, inform users of the risk and report the case to the competent authority;
- provide consistent security maintenance for the ISP's products or services;
- expressly notify and obtain the consent of users if the products or services provided by the ISP collect user information; and
- comply with provisions of the Cybersecurity Law as well as the relevant laws and administrative regulations governing the protection of personal information if the personal information of users is involved.

Network operators shall develop an emergency plan for cybersecurity events to promptly respond to security risks such as system bugs, computer viruses, network attacks and network intrusions. For an event that threatens cybersecurity, the operator concerned must initiate the emergency plan, take corresponding remedial actions and report the event as required to the competent authority.

Network operators shall take technical and other necessary measures to ensure the security of the personal information that it collects, and to protect such information from disclosure, damage or loss. In cases of disclosure,

damage or loss (or possible disclosure, damage or loss) of such information, the network operator shall take immediate remedial action, notify users in accordance with the relevant provisions and report to the competent authority.

Network operators shall strengthen the management of the information released by their users. If the operator finds any information that is prohibited by laws and administrative regulations from release or transmission, it shall immediately cease transmission of such information and take measures such as deletion to prevent the dissemination of such information. The operator shall also keep a relevant record and report the case to the competent authority.

Encryption is not a mandatory security measure.

Law stated - 22 July 2022

Data breach notification

Does your jurisdiction have data breach notification laws that apply to digital business? If so, which regulators should be notified and under what conditions should affected individuals be notified?

Both the Cybersecurity Law and the PIPL regulate that, in the case of a data breach, the network operator (ie, the information processor) shall be obliged to take immediate remedial actions, notify the users and report to a competent authority.

Currently, there is no detailed data breach notification system specific to e-commerce that is regulated by laws and regulations.

Law stated - 22 July 2022

Government interception

Are the authorities permitted lawful access to data? If so, what types of company are required to provide data to the authorities and under what circumstances?

There is no specific rule on whether authorities can require private keys to be made available. However, according to article 31 of the Cryptography Law, cryptography administrations, related authorities and the staff thereof shall not require commercial cryptography-related agencies and commercial cryptography testing or certification agencies to disclose their source codes or other proprietary cryptography-related information.

Certification authorities are permitted and operate under a licensing system. Certification authorities can only provide service after going through the approval of the Ministry of Industry and Information Technology (MIIT) and the Ministry of Commerce. For the provision of an electronic authentication service without a licence, MIIT will order the providers to stop the illegal act and illegal income (if any) shall be confiscated.

Encrypted communications are mainly regulated under the Electronic Signatures Law, the Cryptography Law and the Administrative Measures on Electronic Certification Services.

Law stated - 22 July 2022

GAMING

Legality and regulation

Is it permissible to operate an online betting or gaming business from your jurisdiction? Is any regulatory consent or age, credit or other verification required?

The Chinese mainland is staunchly opposed to gambling. Both online and offline gambling are illegal, with both punishable by criminal penalties and detention.

Law stated - 22 July 2022

Cross-border gaming

Is it permissible to advertise, or provide access to, an online betting or gaming business located in another jurisdiction or in a metaverse?

No. Online betting is illegal in China. Advertising and providing access to online betting with earnings of not less than 20,000 yuan constitute a joint offence with the crime of running a casino.

As for operation of a gaming business in another jurisdiction, PRC laws require the operator to obtain authorisation from the copyright owner, and approval from competent copyright administrative departments and provincial publication bureaus. Unapproved advertisement or access services will be curbed, the operator's internet service will be stopped and its website will be shut down. Operation without legal authorisation from the game's copyright owner will be investigated by the National Copyright Administration. Serious infringement of copyright may constitute a criminal offence.

Regarding gaming businesses on the metaverse, clarifying legislation is yet to come. However, since the metaverse is closely intertwined with virtual currency, whose legitimacy has been denied by existing regulation, metaverse gaming in China faces considerable difficulties. Operations relevant to virtual currency could constitute the criminal offences of, for example, fund-raising fraud or illegally engaging in fund payment and settlement business.

Law stated - 22 July 2022

OUTSOURCING

Key legal issues

What key legal issues arise when outsourcing services to a provider either inside or outside your jurisdiction?

Agreement

When choosing the provision of services on an outsourced basis, an enterprise shall try to avoid direct personnel management, including signing any written agreement with outsourced employees or paying salaries and social insurance premiums. Instead, the enterprise should sign standardised outsourcing agreements with its outsourced services provider.

Qualification

The outsourced services provider shall possess corresponding qualifications if the outsourcing business involves qualification requirements.

Business secrets

Enterprises shall not assign outsourced employees to core positions that may have access to the business secrets of the enterprise.

Tax

If an outsourced service provider is qualified for the recognition of advanced technology-based service enterprises in terms of employee qualifications, sources and percentages of revenue, it will be entitled to tax incentives.

Law stated - 22 July 2022

Sector-specific issues

Are there any particular digital business services that cannot be outsourced or that are subject to specific regulation?

In general, outsourcing of digital business services is allowed and encouraged. A few particular digital financial services are prohibited from outsourcing, such as the following:

- Risk management of commercial banks accepting loaning applications online. According to the rule, commercial banks must strengthen their responsibilities regarding risk control. Banks shall independently carry out risk management of loans operated through internet platforms, and complete the whole risk management process, which has important impacts on loaning risk assessment and risk control. It is strictly prohibited to outsource the key links of loaning management at any time, including pre-loan, in-loan and post-loan.
- Information technology of banks, asset management companies and insurance institutions, which is related to the financial institution's core competitiveness, shall not be outsourced.

Law stated - 22 July 2022

Contractual terms

Does the law require any particular terms to be included in outsourcing contracts?

It is provided in the Measures for the Risk Supervision of Information Technology Outsourcing of Banking and Insurance Institutions that the following contents in information technology outsourcing contracts or agreements shall be specified (including but not limited to):

- Service scope, service content, service requirements, working time limit and arrangement, responsibility allocation, delivery requirements, relevant restrictions in follow-up cooperation, and agreement on service quality assessment and evaluation.
- Requirements for compliance, internal control and risk management, compliance with laws and regulations and internal management systems of banking and insurance institutions, and notification and implementation mechanism for regulatory policies.
- Service continuity requirements – the service continuity management objectives of service providers shall meet the business continuity objectives requirements of banking and insurance institutions.
- The right of banking and insurance institutions to conduct risk assessment, monitoring, inspection and auditing of service providers, and service providers undertake to accept the supervision and inspection of the outsourcing services of banking and insurance institutions undertaken by the China Banking and Insurance Regulatory Commission.

- Triggering conditions for contract modification or termination, and transitional arrangements for contract modification or termination.
- The ownership of relevant information and intellectual property rights in outsourcing activities, as well as the content and scope that service providers are allowed to use, and the requirements for service providers to use legal software and hardware products.
- Resource guarantee clauses.
- Security confidentiality and consumer rights protection agreements, including but not limited to:

    - prohibiting service providers from using or disclosing the information of banking and insurance institutions beyond the scope permitted by the contract; and
    - service providers shall not transfer or misappropriate the data of banking and insurance institutions in any form, or seek benefits other than those agreed in the outsourcing contract.

- Dispute resolution mechanism, breach of contract and compensation clauses. Cross-border outsourcing should specify the applicable law and jurisdiction for dispute resolution. In principle, Chinese arbitration institutions and Chinese courts should be selected for jurisdiction, and Chinese laws should be applied to resolve disputes.
- Reporting terms, including at least the content and frequency of regular reports, reporting routes, reporting methods and time-limit requirements in case of emergencies.

What is more, the banking and insurance institutions shall expressly require in the contract or agreement that service providers shall not subcontract outsourced services or subcontract them in disguised form. When it comes to subcontracting outsourced services, the contract or agreement shall include the following terms:

- Not to subcontract the main business of outsourcing services.
- The main service provider is generally responsible for the service level and ensures that the subcontracted service providers can strictly abide by the outsourcing contract or agreement.
- The main service provider monitors the subcontracting service providers and fulfils the obligation of notification or report approval for changes of subcontracting service providers.

Law stated - 22 July 2022

Employee rights

What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation? Do the rules apply to all employees in your jurisdiction?

Generally speaking, in the company, the benefits related to salary, annual leave and promotion of outsourced employees might be inferior to regular employees. In terms of the rights of employees (such as severance or consultation) under Chinese employment law, there is no legal distinction between outsourced and regular employees.

Law stated - 22 July 2022

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rules and restrictions

Are there any rules, restrictions or other relevant considerations when seeking to develop or use artificial intelligence, machine learning, automated decision making or profiling? Are any particular notices of such use required? Are impact assessments recommended or required?

In 2017, the State Council of China issued the New Generation Artificial Intelligence Development Plan (the Plan), providing administrative guidance for artificial intelligence (AI) from the perspective of industrial policy promotion, support and development. Following the Plan, the National New Generation Artificial Intelligence Governance Professional Committee was established, which has issued the Governance Principles for New Generation Artificial Intelligence – Developing Responsible Artificial Intelligence (2019) and the Ethics Norms for New Generation Artificial Intelligence (2021).

On the basis of the above rules, the following requirements are imposed for use of AI:

- The AI developers shall:
  - strengthen self-discipline in all aspects of technology research and development;
  - improve data integrity, timeliness, consistency, standardisation and accuracy;
  - improve transparency and reliability in algorithm design, implementation and application; and
  - avoid possible data and algorithm biases in data collection.
- The AI suppliers shall:
  - abide by rules on market access and competition, and avoid infringement of intellectual property (IP) rights;
  - strengthen the quality monitoring and use evaluation;
  - inform users of the functions and limitations of AI products and services, and protect users' right to know and consent; and
  - respond to and process user feedback in a timely manner, and formulate emergency mechanisms and loss compensation plans or measures.
- The AI users shall:
  - use in good faith;
  - avoid improper use and abuse of AI products and services, and avoid unintentional damage to the legitimate rights and interests of others;
  - not use AI products and services that do not comply with laws, regulations, ethics and standards, and prohibit the use of AI products and services to engage in illegal activities;
  - provide timely and proactive feedback on issues such as technical security loopholes, policy and regulation vacuums, and regulatory lag found in use; and
  - improve usability to ensure safety and efficient use of AI products and services.

In accordance with the Ethics Norms, suppliers are recommended to conduct quality monitoring and use evaluation of AI products and services to avoid undue harm. However, the supervision mechanisms of AI are under development, and regulatory requirements may be further tightened in the near future.

Law stated - 22 July 2022

IP rights

Are there any rules concerning intellectual property and artificial intelligence or machine learning? Can the training data sets and other data associated with artificial intelligence or machine learning be adequately protected by intellectual property rights? Are there particular laws, rules or guidance concerning the ownership of intellectual property created by artificial intelligence or

machine learning systems?

Currently, there are no specific rules concerning IP and AI or machine learning. Therefore, such issues are still under general regulation of IP laws, such as the Copyright Law, Trademark Law and Patent Law.

In practice, the protection by IP rights for AI or machine learning remains controversial.

Under the Patent Law

Article 25 of the Patent Law stipulates that 'scientific discoveries, rules and methods of intellectual activities, etc shall not be granted patent rights'. In the field of AI, the innovation of algorithms is the core of every invention and creation at the technical level. Whether pure algorithms belong to 'the rules and methods of intellectual activities' and whether they can be patented is controversial. The Announcement stipulates that if a claim contains technical features in addition to algorithmic features or features of business rules and methods, then the claim, as a whole, is not rules and methods for mental activities, and shall not be excluded from patentability. Whether the provision will further help AI be protected under the Patent Law is unclear.

Under the Copyright Law

Products generated by AI without human participation, based on current laws, cannot be regarded as works protected by the Copyright Law.

Under the Anti-Unfair Competition Law

Commercial secrets refer to technical information, business information and other commercial information that is not known to the public, has commercial value and has been kept secret by the obligee. Therefore, as the core of AI enterprises, algorithms also have great commercial value, and enterprises usually take strict confidentiality measures to keep the algorithms secret. The Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Cases of Infringement of Trade Secrets also clarifies that the people's courts can protect algorithms as trade secrets. Therefore, AI might be protected in this way.

China has no special laws or regulations on the ownership of IP created by AI or machine learning systems. However, in a judgment rendered in 2020, Nanshan Primary People's Court, Shenzhen, Guangdong recognised that the works generated by Dreamwriter, an AI robot developed by Tecent, constituted works protected by the Copyright Law, and Tecent, as a legal entity, owned such copyrights. This precedent became one of the 'Top 10 Cases in 2020' certified by the Supreme People's Court, which indicates its value as guidance concerning such ownership.

Law stated - 22 July 2022

TAXATION

Online sales

Is the sale of digital products or online services subject to taxation in your jurisdiction? If so, on what basis?

In general, tax is imposed whenever a transaction takes place, regardless of it being online or offline. However, in Chinese tax law practice, virtual product transactions between individuals or between individuals and companies are

exempt from value added tax (VAT) if they do not reach the tax threshold. For individuals who cannot provide evidence of the original value of their property, the competent tax authorities shall approve the original value of their property.

For transactions between companies in China, the seller company shall pay tax in accordance with Chinese tax law. As for cross-border virtual products between companies, China's current practice is that the foreign companies that provide virtual product services must set up a standing body in China or cooperate with a domestic entity in China. The authorities will impose VAT on the standing body or cooperative entity. There will also be a tax imposed on for-profit businesses from China.

Law stated - 22 July 2022

Server placement

What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers, a platform or a metaverse within your jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

If the servers installed overseas by a domestic company are used solely for offshore websites, such servers will not be subject to taxes in China. Nevertheless, if such servers are installed abroad and still engaged in network business related to China or the offshore companies send professionals to provide technical services in China the domestic company receiving services shall withhold the taxes and surcharges.

If an offshore company placed servers in China and receives revenue from China through such servers, that portion of the revenue related to China is subject to taxes.

Where there are special agreements on tax collection of cross-border income in tax treaties or agreements signed between China and an overseas country or region, the domestic company may opt to apply the preferential tax rate in the tax treaties or agreements.

Law stated - 22 July 2022

Electronic invoicing

Do the rules in your jurisdiction regulate the format or use of e-invoicing, either generally or for a specific market segment? Is there a requirement to provide copies of e-invoices to a tax authority or other agency?

E-invoicing has been generally implemented in China. In 2015, China started to implement e-invoicing for VAT regular invoices, and in 2020 started to implement e-invoicing for VAT special invoices.

China implements a uniform format for e-invoicing. As of 2019, the national standard Electronic Invoice Based Information Specification came into effect, stipulating the uniform format and required information for e-invoices.

The State Administration of Taxation has built a nationwide unified e-invoice service platform. Issuance of e-invoices are synced on the platform, and thus there is no need to submit copies of e-invoices to the State Administration of Taxation.

Law stated - 22 July 2022

DISPUTE RESOLUTION

Venues

Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

China has established three internet courts in Beijing, Hangzhou and Guangzhou. These courts specialise in internet-related cases online, all of which are located in the most booming and prosperous areas of China's internet industry. These internet courts are skilled in hearing disputes arising from contractual disputes over online shopping or services and underrate financial loans, as well as online copyright disputes and internet-related public interest litigation, among others. Most of the evidence in the cases heard by internet courts is in the form of electronic data and is stored on the Internet.

Law stated - 22 July 2022

ADR

What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

For online or digital disputes, alternative dispute resolution (ADR) is a very common practice in China. E-commerce platforms such as Alibaba and JD.com have set up their own ADR platforms and most consumers are accustomed to solving online shopping contractual disputes through such platforms.

For example, on Alibaba, when a consumer is dissatisfied with goods or services online, the consumer usually submits evidence and negotiates with the supplier first. After the consumer submits the dispute, the two parties have three to 30 days to negotiate without the involvement of the e-commerce platform itself. If the supplier provides a different proposal, the consumer could request Alibaba's assistance by clicking the 'escalate dispute' button or may continue to negotiate with the seller.

In general, the ADR platforms of businesses are more inclined to protect the interests of consumers.

However, some consumers will directly seek the help of the official ADR platform, which is the 12315 platform. The 12315 platform is a hotline that is directly affiliated with the State Administration for Market Regulation (SAMR). In addition, at a local level, many SAMR offices have also established their own separate complaint channels in the form of the hotline or social media accounts.

Law stated - 22 July 2022

UPDATE AND TRENDS

Key trends and developments

Are there any emerging trends or hot topics in the regulation of digital content and services, digital transformation and doing business online in your jurisdiction? Is there any pending legislation that is likely to have consequences for digital transformation and doing business online?

The Personal Information Protection Law (PIPL) came into effect on 1 November 2021, which along with the Cybersecurity Law and the Data Security Law establishes an extensive legal framework of cybersecurity and personal information protection in China.

Following the establishment of the legal framework, Security Assessment Measures for Outbound Data Transfers has been released and will come into effect on 1 September 2022, stipulating the security assessment procedures and requirements of data export or outbound transfer.

Law stated - 22 July 2022

Jurisdictions

Belgium	Astrea
Chile	Magliona Abogados
China	Buren NV
Cyprus	Antoniou McCollum & Co LLC
France	UGGC Avocats
Germany	SKW Schwarz
Gibraltar	Hassans
Hungary	VJT & Partners
India	AZB & Partners
Israel	AYR - Amar Reiter Jeanne Shochatovitch & Co
Italy	ICT Legal Consulting
Japan	Anderson Mōri & Tomotsune
Malaysia	Raja, Darryl & Loh
South Korea	Barun Law LLC
Turkey	Boden Law