Chambers
Global Practice Guides

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

Artificial Intelligence 2022
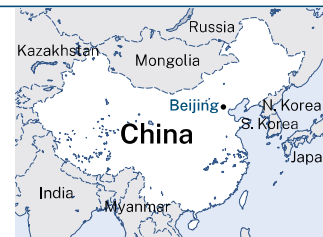
China: Law & Practice and Trends & Developments
Susan Ning and Han Wu
King & Wood Mallesons

CHINA

Law and Practice

Contributed by:
Susan Ning and Han Wu
King & Wood Mallesons see p.15

CONTENTS

1. GENERAL LEGAL FRAMEWORK

1.1 General Legal Background Framework

China has developed a large number of laws and regulations that systematically address AI-related issues, as well as rules regulating particular AI-related subject matters.

At the level of national laws, AI – as a technology that highly relies on the use of internet and data – will be subject to the three basic laws in the information technology field, namely:

- the Cybersecurity Law of the People's Republic of China (CSL);
- the Data Security Law of the People's Republic of China (DSL); and
- the Personal Information Protection Law of the People's Republic of China (PIPL).

They are enacted to guarantee cybersecurity and regulate data (including personal information) processing activities.

Under these basic laws, the State Council, the Cyberspace Administration of China (CAC) and other authorities responsible for cybersecurity and data protection within the scope of their respective duties are tasked to develop and enforce specific regulations. For example, the CAC has issued a number of rules/draft rules concerning internet information services, especially including the use of AI technologies in such fields.

At regional levels, local governments have enacted relevant cybersecurity and data regulations in conjunction with the actual development of their respective regions, with 12 representative provinces and cities such as Shanghai and Shenzhen since 2021.

Apart from general cybersecurity and data protection laws, laws and regulations of other legal sectors also apply to AI if the application of AI touches specific issues regulated in these other legal sectors, including consumer protection law, anti-monopoly law and industrial-specific laws.

2. INDUSTRY USE OF AI AND MACHINE LEARNING

2.1 AI Technology and Applications

AI and machine learning have become the key force in promoting the development of the financial industry, according to a report issued by the China Academy of Information and Communications Technology (CAICT). In the banking industry, AI technology is widely used in biometric identification, credit risk prevention and intelligent customer services (such as chatbots). According to the CAICT, as of September 2021, one of China's state-owned banks had collected and used 40 PB of data assets and implemented more than 1,000 AI applications.

Another noteworthy application of AI technology is automated driving. The investment and financing of the automated driving industry are increasingly active in China. Robotaxis are the top priority. For example, in 2021, Baidu and Pony.ai became the first two domestic enterprises to be allowed to carry out commercial robotaxi services in Beijing. The commercial use of low-speed automatic vehicles is also accelerating. In May 2021, approximately 100 automatic delivery vehicles from JD.com, Meituan, and Neolix were issued with official vehicle codes in Beijing; in September 2021, the automatic express car developed by JD.com was put into trial operation on the roads in Qionghai City to provide delivery services to communities within 3 km.

Since 2020, while bringing havoc to the markets and industries in China, the COVID-19 outbreak has also revealed unprecedented opportunities for the AI industry. To respond to the pandemic control policies in China, the market has seen a high demand for products and services based on AI technology, AI-powered medical research and diagnosis, pandemic control decision-making, a uniform national "Health Code" platform that traces individuals' health status for pandemic control, and internet-based convenience services powered by AI, such as food delivery, online shopping and internet hospitals.

3. EXECUTIVE DEVELOPMENTS

3.1 Policies

At the national level, China has drawn up comprehensive plans for the development and application of AI. In December 2021, the Ministry of Industry and Information Technology (MIIT), along with seven other state ministries released the 14th Five-Year Plan for the Development of Intelligent Manufacturing (the "Plan"), which listed AI as one of the core technologies in China's intelligent manufacturing.

The Plan also emphasises strengthening research on the application of specific AI technologies in certain industries. In the finance sector, for example, the China Banking and Insurance Regulatory Commission (CBIRC) issued the Guiding Opinions on Promoting the High-quality Development of Banking and Insurance Industries, encouraging banking and insurance institutions to make full use of emerging technologies such as AI, big data, cloud computing, blockchain, biometrics and other technologies to improve service quality.

In addition, the Chinese government is also making efforts on establishing a national stand-

ard system for AI technology. In August 2020, the State Standardisation Administration, the CAC, and other state ministries jointly released the Guidance on Establishing the New Generation of National AI Standardisation System (the "AI Standards Guidance"), aiming at setting up a preliminary national AI standardisation system by 2023. The Opinions on Accelerating the Construction of a National Unified Market, issued by the Central Committee of the Communist Party of China and the State Council in 2022, has made it clear that it is necessary to strengthen the standard system in fields including AI.

3.2 National Security

It is a common issue for AI operators that they may collect a large amount of data to feed their AI system. Since China's laws and regulations on data processing have a clear concern for national security, AI companies are also advised to be aware of related legislative requirements.

Critical Information Infrastructure (CII)

The Regulation on Protecting the Security of Critical Information Infrastructure has defined CII as network facilities and information systems in important industries and fields that may seriously endanger national security, the national economy and people's livelihood, and public interest in the event of being damaged or losing functionality. CII Operators (CIIO) are required to take protective measures to ensure the security of the CIIs. Furthermore, the CSL imposes data localisation and security assessment requirements on cross-border transfer of personal information and important data for CIIOs.

Important Data

The DSL have defined important data as data the divulging of which may directly affect national security, public interests, and the legitimate interests of citizens or organisations, and certain rules impose various restrictions on its processing. The DSL contemplates security assessment

and reporting requirements for the processing of important data in general.

Cybersecurity Review
On 28 December 2021, the CAC, together with certain other national departments, promulgated the revised Cybersecurity Review Measures, aiming at ensuring the security of the CII supply chain, cybersecurity and data security and safeguarding national security. The regulation provides that CIIOs that procure internet products and services, and internet platform operators engaging in data processing activities, shall be subject to the cybersecurity review if their activities affect or may affect national security, and that internet platform operators holding more than one million users' personal information shall apply to the Cybersecurity Review Office for a cybersecurity review before listing abroad.

4. LEGISLATIVE DEVELOPMENTS

4.1 Enacted Legislation
Currently, legislations regulating particular AI-related subject matters in China include the following:

Data Protection
The CSL and DSL directly address the national strategy for enhancing cybersecurity and data security. As for personal information protection, there are three overarching statutes setting forth general principles:

• the PIPL, enacted on 1 November 2021;
• the Civil Code, released in May 2020; and
• the CSL, articulating requirements for personal information protection.

The PIPL proposes to extend the legal basis of processing personal information, as compared to the Civil Code and the CSL, in order to adapt to the complexities of economic and social activities. Since 2019, when multiple departments in China jointly issued the Announcement on Special Treatment of Illegal Collection and Use of Personal Information by App, the current trend shows that the enforcement of app personal information protection has continued to be enhanced, especially in the areas of small programs, SDK (software development toolkit) third-party sharing and algorithmic recommendation as the focus of regulation.

Antitrust
Concerning the Antitrust Guidelines for the Platform Economy, concerted conduct may also refer to the conduct whereby undertakings do not explicitly enter into an agreement or decision but are co-ordinated through data, algorithms, platform rules or other means. As such, AI operators shall also comply with the Anti-Monopoly Law, which requires that competitors are prohibited from reaching monopoly agreements of price-fixing, production or sales restrictions, market division, boycott, or other restraining behaviours. Moreover, dominant market players are also prohibited from conducting discriminatory activities against their counterparties by means of algorithm.

Consumer Protection
Business operators providing products/services to consumers by means of algorithms shall be subject to the Law on Protection of Consumer Rights and Interests, which acts as the basic consumer protection legislation. As for e-commerce businesses, they should further comply with the E-commerce Law, in which there are specific rules dealing with personalised recommendations.

Information Content Management
The Provisions on Ecological Governance of Network Information Content issued by the CAC, effective in January 2020, articulate requirements

for content provision models, manual intervention and user-choice mechanisms when network information content providers feed information to users by adopting personalised algorithms.

In December 2021, the CAC issued the Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services (the "CAC Algorithm Recommendation Rules") to provide special management regulations on algorithmic recommendation technology. The CAC Algorithm Recommendation Rules mark the CAC's first attempt to regulate the use of algorithms, in which internet information service providers are required to use algorithms in a way that respects social morality and ethics, and are prohibited from setting up any algorithm model inducing users to become addicted or to over-consume.

For industrial-based regulations, please refer to **9. AI in Industry Sectors**.

4.2 Proposed Legislation

During the past two years, the data protection authorities in China have issued a large number of draft regulations, aiming at providing detailed implementation guidance for national legislations about data processing activities. For example, the draft Regulations for the Administration of Network Data Security, as a supporting regulation of the CSL, DSL and PIPL, clarifies specific issues in the field of data security management and supplements the basic principles in the national legislations. The draft of Measures on Security Assessment of the Cross-border Transfer of Data articulates in greater detail the framework of cross-border data security review.

For AI-related rules, the CAC released the draft Provisions on the Administration of Deep Synthesis of Internet Information Services in February 2022, which provides specific rules for providers of deep synthesis technologies in the context of information content management.

5. AI REGULATORY REGIMES

5.1 Key Regulatory Agencies

In China, the CAC is responsible for the overall planning and co-ordination of cybersecurity, personal information protection and network data security, and has issued a number of regulations concerning the application of AI technology in terms of internet information services. There are also many other departments – such as departments in the industrial sector, telecommunications, transportation, finance, natural resources, health, education, science and technology – and other departments undertake the duty to ensure cybersecurity and data protection (including that related to AI) in their respective industries and fields. Public security authorities and national security authorities also play an important role for network and data security within their respective purviews.

5.2 AI Definitions

The practice guidance issued by the National Information Security Standardisation Technical Committee (TC260) – ie, Practice Guide for Network Security Standards-Guidelines for Prevention of Ethical Security Risks in Artificial Intelligence – has defined AI as the simulation, extension or expansion of human intelligence by using a computer or its controlled equipment, through the methods of perceiving the environment, acquiring knowledge and deducing.

Another draft standard, the Information Security Technology-Security Specification and Assessment Methods for Machine Learning Algorithms, also released by TC260, defines machine learning algorithms as algorithms that solve problems by using a limited and orderly set of rules to gen-

erate classification, to reason, and to predict based on the input data.

5.3 Regulatory Objectives

It is a normal practice for the CAC and other departments to co-operate in rule-making and enforcing the laws. Most of the data protection-related rules are jointly issued by multiple regulatory agencies including the CAC, the MIIT, public security authorities and other related departments. These laws and regulations have played a key role in ensuring network and data security, and the protection of personal information. In particular, the CAC recently promulgated a series of rules or drafts on the application of AI technology, with an aim to promote the positive and good application of algorithms. These laws and regulations also aim to protect the social and public interests and national security involved in the network and data fields from being endangered.

6. PROPOSED EU ARTIFICIAL INTELLIGENCE LAW

6.1 Jurisdiction Commonalities

The matter is not applicable in the jurisdiction.

6.2 Jurisdiction Conflicts

The matter is not applicable in the jurisdiction.

7. STANDARD-SETTING BODIES

7.1 Standards

The State Standardisation Administration (CSA) is responsible for approving the release of national standards, and TC260 (as mentioned above) is one of the important standard-setting bodies on AI technology. So far, TC260 has issued a series of recommended national standards and prac-

tical guidelines containing provisions regarding the use of AI-related technology. For example, the national standard Information Security Technology – Personal Information Specification-provides rules on automated decision-making similar to the PIPL, which states that controllers adopting automated decision-making that may influence data subjects' interests should conduct security assessments of personal information ex ante and periodically, and should allow data subjects to opt out of such automated decision-making.

The draft standard Information Security Technology – Security Specification and Assessment Methods for Machine Learning Algorithms specifies the security requirements and verification methods of machine learning algorithms in the stages of design and development, verification testing, deployment and operation, maintenance and upgrading, and decommissioning, as well as the implementation of security assessment of machine learning algorithms.

In addition, there are standard-setting bodies to formulate AI-related standards in specific industries. The PBOC, along with the Financial Standardisation Technical Committee of China (TC 180), which is the CSA-authorised institution to engage in national standardisation, plays a leading role in writing AI-related standards in the financial field. The recommended industry standard of Personal Financial Information Protection Technical Specification, which was issued in the name of the PBOC, sets forth requirements for financial institutions to regularly assess the safety of external automated tools (such as algorithm models and software development kits) adopted in the sharing, transferring and entrusting of personal financial information. The PBOC also released the Evaluation Specification of Artificial Intelligence Algorithm in Financial Application in 2021, providing AI algorithm evaluation meth-

ods in terms of security, interpretability, accuracy and performance.

In automated driving, the recent recommended national standard Taxonomy of Driving Automation for Vehicle *s* sets forth six classes of automated driving (from L0 to L5) and sets forth respective technical requirements and the roles of the automated systems at each level. The TC260 released the Security Guidelines for Processing Vehicle Collected Data, which specify the security requirements for automobile manufacturers' data processing activities such as transmission, storage and export of automobile data, and provides data protection implementation specifications for automobile manufacturers to carry out the design, production, sales, use, operation and maintenance of automobiles.

8. GENERAL TECHNOLOGY-DRIVEN AI LEGAL ISSUES

8.1 Algorithmic Bias
From a technical perspective, algorithms may be biased due to a number of reasons. The accuracy of an algorithm may be affected by the data used to train it. Data that lacks representativeness or, in essence, reflects certain inequalities may result in biases of the algorithms. The algorithm may also cause bias due to the cognitive deficits/bias of the R&D personnel. Besides, due to the inability to recognise and filter bias in human activities, algorithms may indiscriminately acquire human ethical preferences during human-computer interaction, increasing the risk of bias in the output results.

For example, the provision of personalised content by digital media has raised serious concerns on the so-called "information cocoon" – a phenomenon where people get more and more limited information selected, based on automatic

analysis of their previous content preferences. Another example is the concern of "big data killing", where different consumers are charged significantly different prices for the same good. According to the China Consumers Association, certain companies use algorithms to make price discriminations over different groups of consumers.

Having been aware of the harm to society and consumers' interests caused by algorithm bias, the Chinese government is trying to regulate the proper application of algorithm both on an industrial-specific basis and on the general data protection side. According to the E-commerce Law, where an e-commerce business operator provides consumers with search results for goods or services based on consumers' preferences or consumption habits, it shall, in parallel, provide consumers with options that are not targeted at their personal characteristics. Similar rules have been set in the PIPL regarding automatic decision-making, where transparency and fairness requirements are explicitly stipulated (see **8.4 Automated Decision-Making**).

The newly issued regulation concerning internet information services, the CAC Algorithm Recommendation Rules, further provide that an algorithm-recommended service provider which sells goods or provides services to consumers shall protect their right to fair transactions, and shall not use algorithms to commit unreasonable differential treatment and other illegal acts in respect of transaction prices and other transaction conditions based on their preferences, transaction practices and other characteristics. "Big data killing" is also under the scrutiny of the Anti-monopoly Law, by which a dominant market player is prohibited from discriminating against its counterparties (including consumers) by means of automatic decision-making programs.

8.2 Facial Recognition and Biometrics

Under the PIPL, facial recognition and biometric information are recognised as sensitive personal information. Separate consent is needed for processing such information and the processing shall be only for specific purposes and with sufficient necessity. Facial information collected by image collection or personal identification equipment in public places shall only be used for maintaining public security, unless separate consent has been obtained.

This gives rise to concerns of intelligent shopping malls and smart retail industries where facial characters and body movement of consumers are processed for purposes beyond security, such as recognising VIP members and identifying consumers' preferences so as to provide personalised recommendations. Under the PIPL, companies must consider the necessity for such commercialised processing and find feasible ways to obtain effective "separate consent".

In the automobile industry, images or videos containing pedestrians are usually collected by cameras installed on cars. This is a typical data source for automobile companies engaging in autonomous driving or providing internet of vehicles services. While training their algorithms and providing relevant services, automobile data processors must consider the mandatory requirements both in the PIPL and the recently issued Several Provisions on the Management of Automobile Data Security (for Trial Implementation), in which videos and images containing facial information are considered as important data. Processors having difficulty obtaining consent for its collection of personal information from outside a vehicle for the purpose of ensuring driving safety shall conduct anonymisation for such information, including deleting the images or videos that can identify the natural person, or conducting partial contour processing of facial information.

The Supreme People's Court also provides its judicial view regarding the processing of facial information and clarifies scenarios that may cause civil liabilities, such as:

- failing to comply with laws when conducting facial verification, recognition, or analysis in business premises and public places;
- failing to disclose rules on the processing of facial information or failing to explicitly state the purposes, methods and scope of such processing;
- failing to obtain the separate consent;
- failing to take proper measures for ensuring the security of facial information which results in leaks, distortion or loss of facial information.

Companies failing to perform obligations under the PIPL and related regulations are also faced with administrative penalties and even criminal liabilities (ie, for infringing citizens' personal information).

8.3 Transparency

In China, chatbots are usually deployed by e-commerce platforms or online sellers to provide consulting or after-sale services for consumers. While there has not been a special regulation targeting the compliant use of chatbots or similar technologies, it does not mean that such use avoids the scrutiny of current effective laws. For example, under the regime of consumer protection law, companies using chatbots to address consumers' questions or requests must ensure the rights and interests of consumers are properly protected; where chatbots are enabled to make decisions based on a user's personal information, the PIPL shall apply.

Furthermore, chatbots providing (personalised) content recommendations may also need to comply with the rules issued by the CAC Algorithm Recommendation Rules. Companies shall

pay special attention to the recent CAC Algorithm Recommendation Rules, if their chatbots are equipped with automated content push functions.

Relevant laws have set out transparency requirements on the use of AI-related technology. If such technology involves processing of personal information, processors are required to notify individuals of such processing. There are also transparency requirements for automated decision-making (see **8.4 Automated Decision-Making**). Users of internet information services involving AI technology are also entitled to be informed of the provision of algorithm-recommended services in a conspicuous manner. According to theCAC Algorithm Recommendation Rules, relevant service providers are required to appropriately publish the basic principles, purposes and main mechanics of algorithm-recommended services.

8.4 Automated Decision-Making

There are specific rules for automated decision-making in the PIPL. Firstly, automated decision-making using personal information shall be subject to transparency requirements; processors are required to ensure the fairness and impartiality of the decision, and shall not give unreasonable differential treatment to individuals in terms of trading price or other trading conditions.

Where information feed or commercial marketing to individuals is carried out by means of automated decision-making, options not specific to individuals' characteristics shall be provided simultaneously, or convenient ways to refuse shall be provided to individuals. Individuals whose interests are materially impacted by the decision made by automated means are entitled to request relevant service provider/processor to provide explanations and to refuse to be subjected to decisions solely by automated means.

8.5 Theories of Liability

There have been hot debates on the allocation of liabilities in an AI scenario. In a traditional view, the civil law – including tort law – deals with legal relationships between/among civil subjects such as natural persons, companies or other organisations; thus, it seems difficult to treat AI, which is developed by humans through computer programming, as a liability subject. However, such consensus might be challenged considering the strengthened self-learning and independent decision-making ability of AI technology, both now and in the foreseeable future.

From a tort law perspective, the owner of AI-enabled technology that harms the interest of others should be directly liable. However, the application of AI technology usually involves a number of roles, such as the AI developer, the product/service manufacturer, the seller and even the user. It must be prudent when defining who is the proper "owner" that should be liable.

Secondly, liability is usually established on the fact that the infringer is at fault. This brings difficulty when the decision that harms others' interest is made by AI technology which goes beyond the control of the technology user – a typical example is the driver of a car equipped with an autopilot program. Furthermore, even discussing the liability of the developer or provider of the AI technology, it remains a problem for the plaintiff to prove at a technical level that there is an internal design defect in the AI technology, particularly considering the ability of autonomous deep learning of AI as well as the complexity of the external environment that may interfere with AI's decision-making during the interaction.

Therefore, the attribution of responsibility in an AI scenario shall be conducted with sufficient consideration and proper definition of the duty of care of different subjects, combining with the state-of-art, as well as objective factors that may

affect the computing process of the AI technology.

9. AI IN INDUSTRY SECTORS

9.1 Healthcare

As for AI technologies that act as a medical aid during the process of diagnosis and treatment, the Department of Health (currently named the National Health Commission) has issued technical specifications for robot-assisted cardiac surgery in 2012. Apart from that, in 2021, the State Food and Drug Administration issued the Guiding Principles for the Classification and Definition of Artificial Intelligence Medical Software Products, which clearly defines AI medical software as "independent software that uses AI technology to realise its medical use based on medical device data", and medical device data as "the objective data generated by medical devices for medical purposes and in special cases includes the objective data generated by general equipment for medical purposes".

On the other hand, the adoption of AI technology involving processing of data shall also be subject to the data protection laws. As for information related to patients, apart from personal information protection requirements, companies must pay additional attention to rules in the medical and health sector, whereby the use, sharing of patients' medical record is strictly restricted. The use and transfer of medical data may also trigger legal obligations in bio-security laws and may even raise national security issues.

9.2 Financial Services

The application of AI technology in the financial sector may have a significant impact on the rights and interests of individuals. For example, it is a common practice for financial institutions to evaluate the credit situation of individuals

through automated decision-making. In such case, the rules on automated decision-making in the PIPL shall apply, whereby individuals have the right to refuse the decisions solely by automated means. Financial companies are suggested to make appropriate manual intervention in the decision-making process of AI. In addition, the legality of the data on which the application of AI technology in financial sector is based should be carefully checked. Obtaining information related to personal credit by illegal means may lead to serious liabilities, including even criminal liability.

Apart from these general rules, the People's Bank of China (the PBOC) and other financial regulators jointly issued the Guidance Opinions on Regulating Asset Management Business byFinancial Institutionsin April 2018, which articulate qualification requirements and human intervention obligations for financial institutions providing asset management consulting services based on AI technologies. In addition, the newly promulgated Implementation Measures for Protection of Financial Consumers' Rights and Interests of the People's Bank of China and Financial Data Security Data Lifecycle Security Specificationalso form a differentiated financial data security protection requirement covering the whole data life cycle based on data security grading.

9.3 Autonomous Vehicles

The Several Provisions on the Management of Automobile Data Security (for Trial Implementation),issued by the CAC jointly with other departments, specified the rules for use of automobile data and identified the scope of important data in automotive industry. The MIIT and other ministries jointly issued the Trial Administrative Provisions on Road Tests of Intelligent Connected Vehicles, effective in May 2018, to regulate the qualification, application and procedure requirements of automated driv-

ing road tests and liabilities incurred by road test accidents. At local government level, companies engaging in autonomous driving road tests are required to apply for a professional review for their testing plans and get approvals before implementing a road test. Currently, more than 20 cities have issued their administrative measures for automated driving road test qualifications.

Additionally, road testing of autonomous driving inevitably involves the processing of road and geographic data, which are further subject to the laws regarding surveying and mapping activities.

10. AI AND EMPLOYMENT

10.1 AI in Corporate Employment and Hiring Practices
As businesses turn to automated assessments, digital interviews and data analytics to parse job resumes and screen candidates, the use of AI technology in recruiting has been increasing.

One of the main benefits of AI recruiting is its ability to quickly organise candidate resumes for employers. AI is able to sift through hundreds of resumes, scour candidates for relevant past experience, or other qualities that might be of interest to employers, and ensure the best candidates are screened within minutes. This greatly reduces the time required to review applications.

On the other hand, however, without a broadly representative dataset, it might be difficult for AI systems to discover and evaluate suitable candidates in a fair manner. For example, if the positions in the company have been dominated by male employees for the past years, the historical data on which the AI recruitment system is based may lead to a gender bias, making women who would otherwise be qualified for the job excluded from the candidates list.

As resumes usually constitute personal information, employers using AI technology to process candidates' information shall be subject to the transparency and related requirements under the PIPL, and shall ensure the fairness and rationality of the decision-making process. To best avoid bias, employers are suggested to establish a regular review and correction mechanism for the AI technology used for recruiting and endeavour to mitigate the risk of unfair and unreasonable decision-making. Further, human participation in the entire recruitment process should be guaranteed, so that the interview, evaluation and decision on whether the candidate is qualified shall be mainly processed by humans.

11. INTELLECTUAL PROPERTY

11.1 Applicability of Copyright and Patent Law
When AI-enabled technology/algorithms are expressed in the form of computer software, the software code of the whole set or a certain module can be protected in China under the Regulation on Computers Software Protection. While AI-enabled technology/algorithms are expressed through a technical scheme, it can be protected as a process patent. The latest revision of the Patent Examination Guidelines in 2020 specifically adds provisions for the examination of invention applications that include algorithmic features. In addition, if the development and use of the algorithm is of high confidentiality, such algorithm might be protected as a trade secret or technical know-how.

As for the datasets, it remains unclear in law whether companies or persons could successfully establish ownership over such intangible assets. Recent judicial cases have affirmed the competitive rights of platform operators in the user data they hold from the perspective of the

Anti-Unfair Competition Law, and regulations made by certain local governments have tried to formulate a right/interest system for data that involves individuals and enterprises. However, given that different types of data (personal information, important data, state secrets, etc) are subject to restrictions in different legal regimes, challenges still exist for ownership protection over data, from both a legislative and a practical perspective.

There remains hot debate on whether machines can be the holder of any intellectual property rights. In China, one of the well-known local courts, Shenzhen Nanshan District People's Court, determined in a copyright infringement case in 2020 that articles automatically generated by an AI-written assistant software shall be copyrightable and constitute a work of the legal entity that owns the software. Although recognised as one of the top ten cases in 2020 by People's Court Daily, the court's opinion on whether automatically generated contents are copyrightable still remains controversial, especially considering that an opposite decision has been made by the Beijing Internet Court in another similar case.

12. E-DISCOVERY AND LITIGATION

12.1 E-discovery and Litigation Support Services

In 2017, the State Council issued the New Generation Artificial Intelligence Development Plan and proposed to establish "smart courts" – that is, "to establish a smart court data platform that integrates trials, personnel, data applications, judicial disclosure and dynamic monitoring to promote the application of artificial intelligence in evidence collection, case analysis, and legal document reading and analysis".

In this context, various places have begun to make beneficial explorations of artificial intelligence in judicial practice. At present, the use of speech recognition technology to assist in the recording of court proceedings has become a common practice of many domestic courts. For criminal cases, intelligent assistant case-handling systems have been developed and applied at local level, with an attempt to unify evidence standards, formulate evidence rules, and build evidence models. In civil litigation scenarios, certain local courts have adopted a smart trial platform which allows the parties to participate in trials without being in the court, and even without being present at the same time. The AI assistant judge can act as the host of the trial. As long as the parties are online, the AI assistant will guide the parties to present evidence, cross-examination, etc.

It is foreseeable in the future that AI technology will be used in a wider scope for litigation. Trained with a huge amount of case data, artificial intelligence technology will play a greater role in unifying case trial standards and many other aspects.

13. ADVISING DIRECTORS

13.1 Advising Corporate Boards of Directors

Regarding the scenario of companies' governance, automated decision-making may more directly and frequently affect shareholders' vested interests and the operation of the business as a whole. It needs to be established whether automated decisions are attributed as decisions by the board of directors or shareholders' meeting. In general, as the automated decision-making scheme is introduced to the company mainly by decisions of the board, there is consensus that such decision shall be considered as a decision of the board or the shareholders' meeting.

Therefore, if there is any adverse impact on shareholders or the whole business operation, the board or the shareholders' meeting shall be responsible.

To mitigate relevant risks, from a technical perspective, ensuring the traceability of automated decision-making results would be a top priority. From a managerial perspective, companies are advised to assess potential risks in business before implementing the automated decision-making system, limit the applicable scope of such system if a material adverse impact would incur, and set up a manual review mechanism to check and ensure the accountability of final decisions. Furthermore, to neutralise potential bias that may be inserted in or evolved through the algorithm, it is also advisable for companies to set up an AI ethics committee to overview the internal use of AI.

14. OTHER

14.1 Hot Topics and Trends on the Horizon

The ethical issue of AI technology has always been a major concern and is hotly discussed in many countries. In September 2021, the National New Generation Artificial Intelligence Governance Professional Committee issued the New Generation Artificial Intelligence Ethics Code, proposing that, when providing AI-enabled products and services, operators should fully respect and help vulnerable and other special groups, and provide corresponding alternatives as needed.

It is also necessary to ensure that humans have full autonomy in decision-making, and that AI shall be always under human control. Under the State Council's New Generation AI Development Plan, the state government intends to initially establish a legal, ethical and policy system of AI regulation by 2025. It is foreseeable that the government will engage more in AI governance, and specific regulations, such as institutional rules on AI ethics, will gradually become clearer.

King & Wood Mallesons is an international law firm headquartered in Asia that advises Chinese and overseas clients on a full range of domestic and cross-border transactions, providing comprehensive legal services. The firm has over 2,000 lawyers around the world, with an extensive global network of 27 international offices spanning Singapore, Japan, the USA, Australia, the UK, Germany, Spain, Italy and other key cities in Europe as well as presences in the Middle East. With a large legal talent pool equipped with local in-depth and legal practice, it provides legal services in multiple languages. King & Wood Mallesons, with its strong foundation and ever-progressive practice capacity, has been a leader in the industry. It has received more than 300 international and regional awards from internationally authoritative legal rating agencies, businesses and legal media, including Acritas, The Financial Times, ALB, Chambers Asia-Pacific Awards, Euromoney, Legal Business and The Lawyer.

AUTHORS

Susan Ning is a senior partner and the head of King & Wood Mallesons' commercial and regulatory group. She is a pioneer of cybersecurity and data compliance practice. Her many published articles include "New Trends of the US Personal Data Protection – Key Points of the New FCC Rules" and "A Brief Analysis on the Impact of Data on Competition in the Big Data Era". Susan's practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, and compliance of cross-border data transmissions. She has assisted companies in dealing with network security and data compliance issues in the IT, transportation, online payments, consumer goods and finance sectors.

Han Wu is a partner at King & Wood Mallesons. He excels in providing cybersecurity and data compliance advice to multinational companies' branches in China. Han also has expertise in establishing network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the EU (GDPR), the USA and other jurisdictions. In the areas of cybersecurity and data compliance, he provides legal services such as assisting clients: to establish a cybersecurity compliance system; in self-investigation on cybersecurity and data protection; to conduct internal training on cybersecurity and data compliance; in due diligence in data transactions; to design plans for cross-border data transfers; and in network security investigations and cybersecurity incidents.

King & Wood Mallesons

18th Floor
East Tower
World Financial Center
No 1 Dongsanhuan Zhonglu
Chaoyang District
Beijing 100020
P R China

Tel: +86 10 5878 5749
Fax: +86 10 5878 5599
Email: wuhan@cn.kwm.com
Web: www.kwm.com

KING&WOOD
MALLESONS
金杜律师事务所

Trends and Developments

Contributed by:
Susan Ning and Han Wu
King & Wood Mallesons see p.21

Introduction

Artificial intelligence (AI) has become one of the most revolutionary technologies in human history. As summarised by the State Council in its New Generation AI Development Plan, after more than 60 years of evolution – especially driven by new theories and technologies such as mobile internet, big data, supercomputing, sensor networks and brain science, as well as the strong demand for economic and social development – AI has been developing rapidly.

AI industries in China benefit from various market advantages, such as gigantic amounts of data available for machine learning, diverse and huge demand for market applications, and strong policy support. The Chinese government also actively embraces AI technology and recognises it as a key focus of future economic development. As estimated by the International Data Corporation (IDC), by 2025, the total size of China's AI market is expected to exceed USD18.4 billion and China will account for approximately 8.3% of the global total, ranking second among individual countries.

Application and Development of AI Industry

The Chinese Academy of Science recognises eight key AI technologies that have achieved breakthroughs and has identified specific areas of application, including:

- computer vision;
- natural language processing;
- trans-media analysis and reasoning;
- intelligent adaptive learning (which provides each student with a personalised education that suits their character);
- collective intelligence;

- automated unmanned systems;
- intelligent chips; and
- brain-computer interfaces.

Among the industries adopting AI in China, the computer user vision market remains one of the biggest contributors, and machine learning, where intelligent decision-making plays a major role, will be consolidated and achieve growth as the importance of data as a model production factor increases. In addition to the AI technology track, the training and reasoning demand of AI chips that serve as underlying computing power support contributes a lot to the increasing size of the AI industry.

From an academic view, the AI Index 2022 Annual Report released by Stanford University shows that, despite rising geopolitical tensions, the USA and China had the greatest number of cross-country collaborations in AI publications from 2010 to 2021, increasing five times since 2010. The report further pointed out that, in 2021, China continued to lead the world in the number of AI journals, conference and repository publications.

The Chinese government recognises AI as an important component of national strategy and plans to establish an AI regulatory system shortly. AI is one of the seven key areas of digital industrialisation in the 14th Five-Year Plan, and intelligent transformation will also be the focus of state-owned enterprises in the next three years.

Since 2020, the COVID-19 outbreak has greatly changed the way people live and work; simultaneously, it has also brought great opportunities for the application of AI technology. In terms of pandemic prevention and control, AI has played

an important role in monitoring and analysis, personnel and material management and control, medical treatment, drug research and development, logistics support, and resumption of work and production.

Regulation Updates Regarding AI

Currently, the regulation over AI is usually combined with specific sectors where AI technology is applied or is closely related. For example, the E-Commerce Law requires operators of e-commerce to provide the consumer with options not targeting their identifiable traits when providing the results of a search for commodities or services for a consumer based on their hobbies, consumption habits, or any other traits thereof. There are similar requirements in the Personal Information Protection Law (PIPL) regarding automated decision-making by use of personal information. There are also rules in the automated driving, medical and financial sectors. For the relevant laws and regulations, please refer to the Artificial Intelligence 2022 China Law & Practice.

The year 2021 has been called "the first year of algorithm governance in China". In August 2021, the Cyberspace Administration of China (CAC) issued a public consultation on the Regulations on the Administration of Algorithm Recommendations for Internet Information Services (Draft for Public Comments), which re-stated that users should be provided with options that do not target their personal characteristics or be provided with convenient ways to close them. Subsequently, the CAC and nine other ministries and commissions issued the Guidance on Strengthening the Comprehensive Governance of Internet Information Service Algorithms ("Guidance on Governance of Algorithms"), announcing that China would establish a comprehensive algorithm governance system within three years.

The year 2022 began with the release of the Regulations on the Administration of Algorithm

Recommendations for Internet Information Services ("CAC Algorithm Recommendation Rules"), which came into effect in March. Based on internet information services, the regulation puts forward specific and detailed requirements for algorithm recommendation services from the perspective of algorithm fairness and information content management, and clarified the scope of "algorithm recommendation technology", the regulatory principles and rules of algorithm recommendation services, as well as specific classification, filing, security assessment and other regulatory means.

Law Enforcement and Judicial Practices Regarding AI

The abuse of algorithms has received increasing attention from the regulators of different sectors. Based on the Guidance on Governance of Algorithms, the CAC initiated a special action of Clear Algorithm Abuse Governance, and conducted algorithm inspections on more than 300 internet companies across the country, including news media, e-commerce platforms, and video websites. With the coming into force of the Regulations on the CAC Algorithm Recommendation Rules, the CAC continued its enforcement in 2022 and has started the annual special action for algorithm governance, together with other relevant authorities.

This annual action aims to deeply investigate and rectify the algorithm security problems of internet enterprise platforms, evaluate the algorithm security capabilities, with a special focus on examining large-scale websites, platforms and products with strong public opinion attributes or social mobilisation capabilities.

Enforcement activities in other legal fields reflects the multi-dimensional regulation over the application of algorithms. From an antitrust view, the abuse of algorithm by a dominant market player

Contributed by: Susan Ning and Han Wu, **King & Wood Mallesons**

may cause serious consequences, damaging the interests of consumers and market competition.

On 8 October 2021, the State Administration for Market Regulation (SAMR) announced an administrative penalty decision against Meituan, which was found to have abused its dominant market position within the Chinese online food delivery service market. According to SAMR's investigation, Meituan forced its merchants into exclusive co-operation agreements by charging differential rates and slowing down their approvals to list on the app. Meituan also required its merchants to "pick-one-from-two" among Meituan and other rival platforms by charging exclusive co-operation deposits, adopting algorithms, data and other technical means, as well as various punitive measures. All of the above acts constitute an abuse of a dominant market position under Article 17 of the Anti-Monopoly Law (AML), as they have forced, "without justifiable reasons", their trading counterparts to make transactions exclusively with themselves.

Meituan is not the only internet platform behemoth to be imposed with a fine as a result of its "pick-one-from-two" activities via manipulation of algorithms and data. In December 2020, SAMR issued administrative penalties against Alibaba, which was fined CNY18,228 billion for abusing its dominant position in the domestic online retail platform service market. This was the highest penalty amount in China's anti-monopoly enforcement history.

In terms of court decisions, in April 2021, the first case related to face recognition technology ushered in the final verdict. The plaintiff was dissatisfied with a wildlife park's change to the way of entering the park for annual card users, from fingerprint recognition to face recognition, and he brought the park to court on the grounds of infringement of privacy and breach of service contract. The court of second instance decided that the wildlife park's unilateral change in the way annual card users enter the park constitutes a breach of contract, and its intention was to use the customers' photos to expand the scope of information processing goes beyond the purpose for data collection stated previously, indicating that there is a possibility and danger of infringing on the personal interests of the plaintiff. Furthermore, as the park had ceased to use fingerprint gates, the court finally ordered the wildlife park to delete the plaintiff's facial character information as well as his fingerprint recognition information.

This case reflects the judicial protection of personal information in the AI application scenario, which has paid sufficient attention to the principle of "lawful, proper and necessary" for enterprises to process personal information by means of AI technology.

Focus on AI Governance: Ethical Norms

In AI governance, legal constraints and flexible ethical norms usually go hand-in-hand. Compared with laws and regulations, ethics codes reflect more of a general direction and universal guidance. In China, the National Professional Committee on the Governance of New Generation Artificial Intelligence released the Code of Ethics for New Generation Artificial Intelligence on 25 September 2021, proposing six basic ethical requirements:

• promoting human welfare;
• promoting fairness and justice;
• protecting privacy and security;
• ensuring controllability and trustworthiness;
• strengthening responsibility; and
• enhancing ethical literacy.

The Code thereby aims to integrate ethics into the whole life cycle of artificial intelligence and provide ethical guidelines for natural persons, legal persons and other related institutions engaged in AI-related activities.

Contributed by: Susan Ning and Han Wu, ***King & Wood Mallesons***

Recently, in March 2022, China's State Council issued the Opinions on Strengthening Ethical Governance of Science and Technology, proposing that during the 14th Five-Year Plan period, the government will focus on strengthening the study of legislation on the ethics of science and technology in the fields of life sciences, medicine and artificial intelligence, and timely promote the elevation of important ethical norms of science and technology into national laws and regulations.

Official institutions are endeavouring to establish ethical standards for algorithms. The China Academy of Information and Communications Technology issued the White Paper on AI Governance ("CAICT White Paper"), which lays out ethical standards for using AI, such as that algorithms should protect individual rights. The CAICT White Paper proposed that AI should treat all users equally and in a non-discriminatory fashion and that all processes involved in AI design should also be non-discriminatory. AI must be trained using unbiased data sets representing different population groups, which entails considering potentially vulnerable persons and groups, such as workers, persons with disabilities, children and others at risk of exclusion.

Enterprises, on the other hand, are the protagonists in implementing ethical codes. In recent years, the establishment of ethics-related departments has become an important manifestation of corporate self-regulation. At the 2019 National Congress, Baidu proposed to accelerate AI ethics research and encouraged companies to implement AI ethical principles in product design and business operations. At the 2020 World AI Conference, Megvii proposed three principles for companies to uphold when practising AI governance:

- no absence – deep involvement in it;
- no confrontation – the development of technology, the application of business and the

formulation of rules should be complementary; and
- action speaks louder than words – every step of AI governance should be reflected in daily work.

It is foreseeable that more and more technology companies will follow the fast-paced flow of policies and regulations to establish a more complete system and mechanism for the ethical review of AI technology.

AI technology is still in the early stages of industrial application, and many deep-seated ethical issues and their implications have not yet been fully revealed. Therefore, the Chinese authorities are closely tracking the frontiers of technology and widely incorporating the opinions and suggestions of experts and scholars from different disciplines and fields, as well as enterprises and consumers, in order to make scientific and dynamic adjustments to ethical regulations.

Conclusion

At present in China, legislation and law enforcement in many fields have touched on the legal issues arising from the current application of AI technology, including data protection, consumer rights protection and anti-monopoly issues. It is foreseeable that the cross-use of various AI technologies and the updating and iteration of such technologies will inevitably lead to more complicated legal issues.

General questions such as whether AI can qualify as a "human" in a legal sense, as well as specific issues such as whether the "creation" of AI can be protected – and how to assign responsibilities for AI infringing upon the rights and interests of others – will be discussed in depth with the wider and deeper penetration of AI in different industries. On the other hand, ethical and moral requirements will also constitute an important tool for constraint over AI technology.

Contributed by: Susan Ning and Han Wu, **King & Wood Mallesons**

King & Wood Mallesons is an international law firm headquartered in Asia that advises Chinese and overseas clients on a full range of domestic and cross-border transactions, providing comprehensive legal services. The firm has over 2,000 lawyers around the world, with an extensive global network of 27 international offices spanning Singapore, Japan, the USA, Australia, the UK, Germany, Spain, Italy and other key cities in Europe as well as presences in the Middle East. With a large legal talent pool equipped with local in-depth and legal practice, it provides legal services in multiple languages. King & Wood Mallesons, with its strong foundation and ever-progressive practice capacity, has been a leader in the industry. It has received more than 300 international and regional awards from internationally authoritative legal rating agencies, businesses and legal media, including Acritas, The Financial Times, ALB, Chambers Asia-Pacific Awards, Euromoney, Legal Business and The Lawyer.

AUTHORS

Susan Ning is a senior partner and the head of King & Wood Mallesons' commercial and regulatory group. She is a pioneer of cybersecurity and data compliance practice. Her many published articles include "New Trends of the US Personal Data Protection – Key Points of the New FCC Rules" and "A Brief Analysis on the Impact of Data on Competition in the Big Data Era". Susan's practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, and compliance of cross-border data transmissions. She has assisted companies in dealing with network security and data compliance issues in the IT, transportation, online payments, consumer goods and finance sectors.

Han Wu is a partner at King & Wood Mallesons. He excels in providing cybersecurity and data compliance advice to multinational companies' branches in China. Han also has expertise in establishing network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the EU (GDPR), the USA and other jurisdictions. In the areas of cybersecurity and data compliance, he provides legal services such as assisting clients: to establish a cybersecurity compliance system; in self-investigation on cybersecurity and data protection; to conduct internal training on cybersecurity and data compliance; in due diligence in data transactions; to design plans for cross-border data transfers; and in network security investigations and cybersecurity incidents.

King & Wood Mallesons

18th Floor
East Tower
World Financial Center
No 1 Dongsanhuan Zhonglu
Chaoyang District
Beijing 100020
P R China

Tel: +86 10 5878 5749
Fax: +86 10 5878 5599
Email: wuhan@cn.kwm.com
Web: www.kwm.com

Chambers
Global Practice Guides

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com

practiceguides.chambers.com