GLI GLOBAL LEGAL INSIGHTS

AI, Machine Learning & Big Data

2022

Fourth Edition

Contributing Editor: **Charles Kerrigan**

glg global legal group

Global Legal Insights
AI, Machine Learning & Big Data

2022, Fourth Edition
Contributing Editor: Charles Kerrigan
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS – AI, MACHINE LEARNING & BIG DATA

2022, FOURTH EDITION

Contributing Editor
Charles Kerrigan, CMS Cameron McKenna Nabarro Olswang LLP

Publisher
James Strode

Production Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Charles Kerrigan of CMS Cameron McKenna Nabarro Olswang LLP for all of his assistance.

Published by Global Legal Group Ltd.
59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 207 367 0720 / URL: www.glgroup.co.uk

ISBN 978-1-83918-190-0
ISSN 2632-7120

Printed and bound by TJ Books Limited
Trecerus Industrial Estate, Padstow, Cornwall, PL28 8RW
May 2022

CONTENTS

China

Susan Xuanfeng Ning & Han Wu
King & Wood Mallesons

Introduction

Artificial intelligence ("**AI**") is trending and rapidly reshaping our society. AI is no longer a mere concept but rather an appreciable technology that supports our daily life in a variety of aspects, such as facial recognition in e-payments and smart home application systems based on virtual assistants. 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**"), in 2025, the total size of China's AI market is expected to exceed US$18.4 billion and China will account for about 8.3% of the global total, ranking second among individual countries.[1]

Trends

The Chinese Academy of Science recognises eight key AI technologies that have achieved breakthroughs and 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.[2] Among the industries adopting AI in China, security protection, finance and marketing account for the majority, representing 53.8%, 15.8%, and 11.6% of the total market size of industries adopting AI in 2018, followed by agriculture, client service, retailing, manufacturing, education and others. 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.[3] According to the report released by iResearch Global, the AI industry is maturing, and from the perspective of participant types, AI start-ups make up about 30–45% of the future market, and as the head AI companies are trying to get listed on the Science and Technology Innovation Board or Hong Kong Stocks, their market shares will further increase.[4]

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.[5] Aiming to strengthen the role of AI in supporting and leading economic and social development, the Ministry of Science and Technology released several official Letters, which demonstrate the state-level support for provincial and municipal governments to build their own national new-generation AI

innovation and development pilot zone. In such circumstances, more and more traditional enterprises begin to upgrade their intelligence or increase investment in internal Research and Development ("**R&D**"), which will bring opportunities for the further development of the AI market, and China's AI spending will continue to grow in the next five years. According to IDC's forecast, with the continuous implementation of AI applications, the Chinese market will grow at a compound annual growth rate of 24.4% and is expected to exceed US$18.43 billion in 2025.[6]

Since 2020, while bringing havoc to the markets and industries in China, the COVID-19 outbreak has also revealed unprecedented opportunities for the AI and big data industry. To respond to the necessary yet prevalent pandemic control policies in China, the market has seen a high demand for products and services based on AI and big data technology, such as platforms for remote working and online courses, big data and AI-powered medical research and diagnosis, big data-based 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, internet hospitals, and others. Meanwhile, the application of AI in court trials, including but not limited to the application of computer image recognition, voice recognition, etc., has been one of the highlights of AI developments over the past year.

Due to the unprecedented need for AI in the big data industry and the immense data demand for machine learning, the lawfulness and legitimacy of data has become the key legal issue arising out of the adoption of AI and big data machine learning. For example, the Personal Information Protection Law of the People's Republic of China (the "**PIPL**") provides several legal grounds that an entity shall comply with when collecting personal information. It is also a common issue for AI operators that they might unintentionally breach data protection laws and regulations when purchasing data to feed their AI systems due to the difficulties in ensuring that the data transfer and subsequent processing fall within the scope of the data subjects' consent. On the other hand, the legitimacy, fairness and ethical issues in AI adoption itself have increasingly raised concerns of relevant authorities and industry practices. As a result, regulations and guidelines specifically targeting the legitimate use and ethical risks of AI were made public, such as the Guidelines for the Practice of Cybersecurity Standards – Guidelines for the Prevention of AI Ethical Security Risks issued by the National Information Security Standardization Technical Committee (the "**TC260**"), as well as the regulation Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services promulgated by the Cyberspace Administration of China (the "**CAC**") jointly with other state departments.

Ownership/protection

When discussing AI ownership, we mainly focus on the ownership issues for AI algorithms and data.

AI algorithm ownership

At present, companies in China mainly apply for software copyright and/or a patent to claim the ownership of an AI algorithm and protect it from unlawful infringement.

According to the Regulations on Computers Software Protection (the "**Regulations**") that directly govern and regulate the copyright protections for computer software in China, "computer software" as used in the Regulations refers to computer programs and related documents, and "computer program" refers to a coded instruction sequence that may be executed by devices with information-processing capabilities such as computers, or a

symbolic instruction sequence or symbolic statement sequence that may be automatically converted into a coded instruction sequence to obtain certain expected results; the source program and object program of a computer program shall be deemed as the same work. Therefore, an AI algorithm, which, in essence, is a mathematic method that is developed and achieved through the use of computer programming language, is copyrightable and can be registered. Meanwhile, it is worth noting that software copyright will only be afforded to the expression of the source program: target programs within one computer program, together with source programs, are seen as the same work. In addition, with the same logic of new registration for updated computer software, it is reasonably foreseeable that if an AI algorithm is trained and evolved through machine learning, the updated version is separately copyrightable, and a new registration could be initiated by the relevant right holder as *prima facie* evidence of possessing such copyright.

Companies may go a step further and apply for a patent for their software inventions to protect the design. According to the Patent Law, an applicant for a patent for an invention shall undergo substantive examination, and inventions and utility models that are granted patent rights shall possess the characteristics of novelty, creativity and practicality. Part II, Chapter 9 of the Guidelines for Patent Examination articulates specific examination standards for invention applications relating to computer programs. On 31 December 2019, the State Intellectual Property Office ("**SIPO**") released the Announcement of the Revisions to the Guidelines for Patent Examination (No. 343) to clarify the rules for examining patent applications in new business forms and fields such as AI, and thereby decided to add Section 6 to Chapter 9 on "Provisions on Examination of Invention Applications Relating to Algorithmic Features or Features of Business Rules or Methods" to present the particular examination characters for such invention applications. Specifically, the new Section 6 provides a three-step test to examine the patentability of a claim thereunder, including: (1) inclusion of technical features; (2) the technical solution as a whole; and (3) characteristics of novelty and creativity, illustrated by several examples. With the clear examination guidelines, it is expected that SIPO will embrace an increasing number of patent applications for AI algorithms in the near future and that more companies will consider patent protection as one available option to protect their AI algorithm.

From a practical view, the Supreme People's Court (the "**Supreme Court**") released its Report on the Intellectual Property Trial Work of the People's Courts (the "**Report**") in October 2021, recognising challenges the judicial system is currently facing in new fields including AI protection.[7] The Report pointed out that a large number of new types of disputes emerged in industries including AI, creating difficulties in clarifying complex technical facts and application of laws. Regarding the IP issues involving AI adoption, 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 a legal entity. Although recognised as one of the top 10 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.

Data ownership

Currently, China does not have specific laws that clearly define the ownership of data, while society has reached consensus for the recognition of the data asset – which, by definition, is an economic resource, competition resource or property right in the form of data – and

companies are swarming into the field, eager to make the ultimate use of their data resources. Given that different types of data (personal information, important data, etc.) are subject to specific restrictions on collection, processing, storage and sharing, it is difficult to align on the data ownership in practice. For example, as ownership is the fundamental prerequisite of a trade, there is still a call to draw a clear line between the personal information ("**PI**") subjects and the company for the ownership of personal information, to establish and promote a benign societal data governance.

Traditionally, lawmakers structure the legal framework for personal information protection based on the leading legislative stance of an absolute protection of the PI subject's privacy rights and personality rights. As such, with reference to China's Cybersecurity Law (the "**CSL**") and its supporting measures, processing of personal information can only be granted upon the PI subject's authorised consent. However, to facilitate the free flow of data exchanges in the new economy, academic experts and lawmakers have commonly accepted the view that personality rights not only have personal interests but also proprietary interests, the latter of which individuals are entitled to transfer under certain circumstances. Therefore, the PI subjects are theoretically entitled to realise their proprietary interests in personal information as long as no infringement of public interests would incur and upon the PI subject's authorised or explicit consent. In view of the PI subject's right to realise proprietary interests and almost exclusive right to control their personal information (i.e. to determine the way of provision, usage and processing), academics regard PI subjects as the owners of their personal information.

Meanwhile, besides personal information itself, companies are concerned over the ownership of anonymised personal information that technically has no connection to and cannot trace back to identify the PI subjects upon erasure of such information's identifiability. Under the current legal structure to protect personal information from illegal provision to third parties under the CSL, the PIPL and Criminal Law and in consideration of the technical effect of anonymisation, as long as anonymised personal information cannot identify the PI subjects, companies may be entitled to some level of ownership to that anonymised personal information to promote data exchanges. However, given the risk that anonymised personal information may be retraced to the PI subjects, some academics hold the view that companies should only be granted restricted ownership of the anonymised personal information upon balancing the interests of the PI subject's privacy rights.

On the other hand, in general, companies may attempt to claim ownership on non-personal information data, and some judicial cases further affirm the competitive rights of platform operators in the user data they hold from the perspective of the Anti-Unfair Competition Law. However, certain types of specific data are under heavy regulation, and companies' claim of ownership to such data may be barred or substantially restricted. Under the Law on Guarding State Secrets, data recognised as state secrets are administered by state secret authorities and thus companies may not assert ownership to such data. In addition, for important data, often defined as data whose divulging may directly affect national security, public interests, and legitimate interests of citizens or organisations, certain rules (either enacted or in draft form) impose various restrictions on its processing. For example, the CSL imposes data localisation and security assessment requirements on cross-border transfer of important data by critical information infrastructure operators, while the Data Security Law contemplates security assessment and reporting requirements for processing of important data in general, and advocates a classified protection scheme for important data. Companies are also advised to be aware of legislative trends, as the definition of and specific requirements for important data are yet to be finalised, which may possibly further limit companies' ownership claims.

At the time of writing, China is in the legislative process of establishing a personal information protection law and it is expected that lawmakers will respond to the outstanding question of data ownership, especially personal information ownership, in the near future.

Antitrust/competition laws

Over the last decade, AI has greatly empowered and reformed the commercial world, especially in online retailing. For example, Walmart dominated the retail industry in the US in early 2003 but was soon surpassed by Amazon a few years later, due to the latter's possession on a massive scale of personal and market data for its AI machine learning and business pattern experiments, and the adoption of an AI algorithm to harvest its data to constantly predict and adjust the pricing for its products. Today, Amazon's success has influenced all e-commerce platforms to adopt a pricing algorithm, yet it also gives rise to competition law risks.

Under the Anti-Monopoly Law of China (the "**AML**"), competitors are prohibited from reaching monopoly agreements of price-fixing, production or sales restrictions, market division, boycott, or other restraining behaviours. Under the Interim Provisions on Prohibiting Monopoly Agreements, a *de facto* concerted action by competitors, absent an explicit agreement or consent, is also prohibited if there are consistent market behaviours by the competitors and a common intention among them. Concerning the Antitrust Guidelines for the Platform Economy (the "**Guidelines**"), concerted conduct may also refer to the conduct whereby undertakings do not explicitly enter into an agreement or decision but are coordinated through data, algorithms, platform rules or other means. A common view is that pricing algorithms are controlled by the competitor and should not become an exemption of anti-monopoly liability. As such, the anti-monopoly culpability varies by the methods of adopting pricing algorithms. If competitors explicitly agreed to adopt the same or similar pricing algorithm and result in similar pricing patterns, such action may be considered a prohibited price-fixing agreement under the AML. If competitors lack explicit consent, but unilaterally and constantly adapt algorithms that predict and align with the pricing of the competitors, there might be a *de facto* connection of will that also constitutes a prohibited concerted action. However, it is worth noting that, in China, there are currently no actual enforcement actions or litigations regarding this issue.

Algorithms also give rise to the AML liability of abusing a dominant market position by discriminative pricing. With the rapid development of the platform economy in China, internet giants in industries such as ride-hailing food delivery, film ticketing, and hotel reservations are being accused of price discrimination among the public.[8] Algorithmic price discrimination refers to pricing the same product differently depending on the individual features of each buyer, especially empowered by AI harvesting consumer big data. Article 19 of the Interim Provisions on Prohibiting Abuse of Dominant Market Positions explicitly prohibits business operators with a dominant market position from offering discriminative treatment to counterparties in price, volume, quality, discount, and other conditions without justified reasons. However, this prohibition of price discrimination only applies to operators with dominant market positions under the AML. In addition, the Guidelines also set the "differential pricing based on big data and algorithm" as one example of abuse of the dominant market position against the AML. Endeavouring to prevent discriminative pricing by all e-commerce vendors, Article 18 of the E-Commerce Law of the PRC articulated that when e-commerce operators provide search results of goods or services to consumers, they shall also provide options not targeting cons features. The Ministry of Culture and Tourism

published and implemented the Interim Provisions on the Management of Online Travel Business Services in August 2020, which prohibited price discrimination against travellers by big data and other technical measures.

The application of big data also gives rise to concerns of abusing dominant market positions in data by mega internet platforms. In theory, internet platform behemoths may take advantage of the scale of the platform to attract and collect more user and market data, which is subsequently used to further improve the platform's competitive strength; as such, the platform's dominant position is further strengthened via the network effect. Under the Guidelines, for identification of the dominant market position for the platform, assessment factors include users' multi-habitats, users' switching costs, and difficulty with data access, user habits, etc. Some court decisions have also recognised the competitive value of data to companies. In *Sina v. Maimai* in 2016, the court held that Maimai conducted unfair competition behaviour prohibited by the Anti-Unfair Competition Law of the PRC by collecting user information on Sina's social media platform, Weibo, without Sina's consent. The court reasoned that, in the internet economy, data such as user information had become important corporate assets and the scale of data was a major element of their competitive strength, and data shall thus be afforded legal protection.[9] Article 18 of the AML also articulates that the identification of a dominant market position shall also consider factors of competitive strengths other than market share, such as technological competitiveness. Therefore, it cannot be ruled out that the control of large amounts of valuable data in a particular market may contribute to a leading enterprise being identified as having a dominant market position, and such enterprises shall be particularly cautious in undertaking actions the AML recognises as abusing said dominant position, such as refusal to deal, price discrimination, unreasonable trade restrictions, tying and others. In fact, there are already companies seeking for judicial remedies. In November 2021, a big data company brought a lawsuit against Sina Weibo, the largest microblog platform in China, alleging that Sina Weibo refused to grant a licence for use of its data, abusing its dominant marketplace and thus violating the AML. The company requested Sina Weibo to license its data under reasonable conditions and make compensations. The court has yet to make its decision.

Board of directors/governance

One key issue in relation to introducing AI to companies' governance is the integrity of automated decision-making. 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. Factors that may influence the integrity of automated decision-making include but are not limited to the legality of data collection, quality of data set, accountability of the algorithm, potential bias in AI application, etc.

Under the Company Law of China, directors, supervisors and senior management personnel are required to comply with the provisions of laws and administrative regulations and the articles of association of the company, and bear fiduciary duties and duties of diligence. Therefore, when a board of directors introduces AI to facilitate its daily operations and decision-making, it certainly needs to fulfil such duties and bear the corresponding consequences thereof. And, 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 oversee the internal use of AI.

Boards of directors are advised to conduct due diligence before introducing a specific AI technology to assist in their decision-making process. They may need to understand detailed information about the operation principle, working purpose, basic algorithm logic and operation of such technics. During the application of AI and big data, boards of directors are expected to have a duty of care. They may first need to ensure that the data used to feed and train the AI system are accurate, and meanwhile conduct regular review of the results output by AI to avoid deviation in the calculation process. Moreover, boards of directors should also prevent AI from causing significant damage to the company, where various means need to be adopted to ensure that the AI system is used safely and smoothly, and it is advised to have the AI maintained by professionals on a regular basis to ensure that the company does not suffer significant losses due to computing errors.

Regulations/government intervention

In recent years, China has developed numerous laws and regulations that systematically address AI, as well as rules regulating particular AI-related subject matters, such as the following:

- **Big data**: The *Data Security Law* released in July 2021 directly addresses the national strategy for developing big data and enhancing data security. The *Regulations for the Administration of Network Data Security (Draft for comments)*, as a supporting regulation, clarifies specific issues in the field of data security management, and refines and supplements the basic principles and systems in the higher law. *Measures on Security Assessment of the Cross-border Transfer of Data (Draft for comments)* on the regulation of data exit security assessment issues, which carries out the concept of comprehensive and strict regulation more thoroughly, also further presupposes the corresponding compliance obligations for the enterprises involved in data exit. The TC260 has issued a series of recommended national standards regarding big data services and systems, including the *Information Security Technology – Big Data Security Management*, *Information Security technology – Guideline for identification of critical data (Draft for comments)*, and others, and also regarding big data security in specific sectors, such as the *Information Security Technology – Guide for Health Data Security*. Since 2021, governments have enacted relevant data regulations in conjunction with the actual development of their respective regions, with 12 representative provinces and cities such as Shanghai and Shenzhen.
- **Personal information protection and automated decision-making**: There are three overarching statutes setting forth general principles of personal information protection: the *PIPL* enacted on 1 November 2021, the *Civil Code* released in May 2020, along with 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. The recommended national standard *PI Specification* issued by the TC260 articulates that when personal information controllers adopt automated decision-making systems that may influence PI subjects' interests (such as automated decisions empowered by AI and big data analysis), they should conduct security assessments of personal information beforehand and periodically, and should ensure the accessibility for PI subjects to complain against such automated decision-making, followed by a

manual review of the complaints. 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.

- **Consumer protection**: Please refer to the *Guidelines*, *E-Commerce Law* and *Interim Provisions on the Management of Online Travel Business Services (Draft for comments)* regarding prohibition against pricing discrimination in the "Antitrust/competition laws" section above.
- **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 push information by adopting personalised algorithms.
- **AI application**: In December 2021, the *Regulations on the Administration of Algorithmic Recommendation of Internet Information Services* (the "**Algorithmic Recommendation Regulations**") were released to provide special management regulations on algorithmic recommendation technology. Based on internet information services, these Regulations put 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. The TC260 issued the *Specification for Security Assessment of Machine Learning Algorithms (Draft for comments)* in August 2021, which provides several provisions for ethical and institutional measures, filling some gaps in national standards in the field of facial recognition and biometric information limited only to technical measures.
- **Automated driving**: The Ministry of Industry and Information Technology (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 driving road tests and liabilities incurred by road test accidents. In addition, more than 20 cities have issued their administrative measures for automated driving road test qualifications. On the other hand, the recent draft recommended national standard of *Draft Taxonomy of Driving Automation for Vehicles*, published by the MIIT on 9 March 2020, sets forth six classes of automated driving (from L0 to L5) and contemplates respective technical requirements and the roles of the automated systems at each level. In October 2021, the *Automotive Data Security Management Provisions (for Trial Implementation)* came into force, which are the first data-specific regulations in the automotive field and focus on regulating important automotive data and sensitive personal information. The TC260 released the *Safety Guide for Car Collection Data Processing*, which refines the technical requirements in the form of an industrial guide, after which the *Safety Requirements for Car Collection Data (Draft for comments)* also formally seeks comments, dividing car data into four types of data: out-of-vehicle data; cockpit data; operational data; location track data; and remote platform storage of no more than 14 days, etc.
- **Finance**: The People's Bank of China (the "**PBOC**") and other financial regulators jointly issued the *Guidance Opinions on Regulating Asset Management Business by*

Financial Institutions in April 2018, which articulate qualification requirements and human intervention obligations for financial institutions providing asset management consulting services based on AI technologies. The recommended industry standard of *Personal Financial Information Protection Technical Specification* issued by the PBOC also 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. 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 Specification* also form a differentiated financial data security protection requirement covering the whole process of data lifecycle based on data security grading, and build a financial data security management framework with this as the core, and provide reference for third-party security assessment agencies and other units to carry out data security inspection and assessment.

China has also formed a specific plan for establishing a comprehensive legal regime of AI. 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. In October 2019, the China National Information Technology Standardisation Committee announced its plan to establish the AI Technology Sub-committee to engage in the promulgation of national standards regarding AI technology, risk management, products, application and others, which further demonstrates the government's determination in AI regulation. In October 2019, the Big Data Security Standard Special Taskforce of the TC260 released the White Paper of AI Security Standardisation to propose an AI security standard system covering topics of foundational standards, data and algorithm models, technology and systems, management and service, assessments, and products and application. In addition, in August 2020, the State Standardisation Administration, the CAC and three 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, covering national and industrial standards in eight fields, namely: (1) foundational and generic standards; (2) fundamental technologies and products; (3) basic software and hardware platforms; (4) critical general technological standards; (5) technological standards for critical areas; (6) product and service standards; (7) industry application standards; and (8) security and ethical standards.

Civil liability

The algorithm optimisation and the application of AI in several circumstances give rise to hot discussions regarding the allocation of civil liability. In the area of autonomous driving, for instance, the disputes in ownership of the AI, as well as the self-improving of the algorithm, may cause complex situations that require the legislators and academics to explore further solutions. Compared with traditional traffic accidents, the subjects involved in autonomous driving include autonomous vehicle manufacturers, autonomous driving service providers, car sellers, vehicle users and vehicle drivers. In the autonomous driving mode, due to the diversification of subjects involved in tort, the causation between the tortious conduct and the consequences of damage are more ambiguous, and the traditional principle of liability for motor vehicle traffic accidents is hereby challenged. In this case, when an accident happens and causes casualties or property damage, how to determine the responsibility between the human driver and the autonomous driving system (or, in other words, the ultimate responsible person for the autonomous driving system) becomes a problem.

In China, the Road Traffic Safety Law (the "**RTSL**") was promulgated in 2003 and amended in 2007, 2011, and 2021, respectively. The latest revision entered into force on 29 April 2021. On 24 March 2021, one month before the latest official version was ratified, the Ministry of Public Security released the Draft on the Amending of the Road Traffic Safety Law, to clarify the rules for allocating civil liabilities in new forms of traffic incidents involving autonomous driving, and thereby decided to add Article 155, in which, for the first time, the relevant requirements for road testing and passage of vehicles with autonomous driving functions, as well as the allocation of responsibility for violations of laws and accidents, are clarified at the legal level. However, Article 155 is not officially promulgated by the latest revision of the RTSL.

The algorithms of autonomous driving vehicles are constantly optimised; meanwhile, problematic issues including unclear responsibility allocation, moral controversy dilemma, and risk of algorithm bias also rise accordingly. Automated driving vehicles rely on human-computer interaction under the system learning function, which could not be accounted as the proper subjects of accountability, while the degree of algorithm involvement affects responsibility distribution.

Besides, the uncontrollable defects of the producers of the AI system include, through the autonomous deep learning of AI, and the interaction with the surrounding environment, defects based on the independent judgment of the AI system. Due to the highly unpredictable nature of such flaws, placing the blame on the producers will greatly dampen the R&D incentives of major AI companies. Therefore, perhaps instead of discussing how to attribute responsibility, it is better to establish a complete set of producer-risk-transfer systems, such as a compulsory liability insurance system for autonomous vehicles, which requires autonomous driving companies to ensure their products balance industrial development and victims' remedial relief.

Discrimination and bias

The mass application of AI and big data indeed gives rise to concerns of bias generated out of algorithmic computing process. Ele.me and Meituan, two leading food delivery companies in China, faced criticism over their labour conditions after a widely read article in September 2020 exposed how the apps' algorithms create a dangerous work environment, pressuring riders to their working limits by setting up strict delivery deadlines and threatening deductions from their commission for failure.

As the algorithm's self-learning capability is fuelled by the tremendous amount of data generated each moment, food delivery companies can constantly optimise their algorithm, allegedly reducing the average delivery time by 10 minutes in just three years by 2019.[10] According to Ele.me, its system incessantly calculates the optimal solutions for food delivery orders, capable of determining the most suitable rider to receive the order according to rider's route, location, and direction, and identifying and instructing the optimal delivery routes for 10,000 riders within one second if each rider carries five connected orders and 10 task points. However, the algorithm failed to consider the effects of the weather, road conditions, and traffic lights on delivery time, resulting in sometimes impossible delivery times for riders to meet. As a result, riders almost always need to ride the wrong way and run through red lights, drastically increasing the chance of traffic accidents and getting injured.

Food delivery companies' policies also contribute to creating unsafe working conditions. For example, in Meituan, when a rider's late delivery rate reaches 3%, it is not just the rider that would receive deductions from her commission; rather, everyone working

in the same distribution centre would also be financially adversely affected. Under this evaluation system, being late does not just mean a loss in income but also a loss in working relationships with colleagues, hence putting riders into a constant state of anxiety about meeting the delivery deadline.

Another hot topic related to algorithmic discrimination is "Big data killing", which refers to the phenomenon where a product's price, when seen by returning customers, is set much higher than new customers for the same goods or services. According to the China Consumers Association, certain companies use algorithms to make price discriminations over different groups of consumers. For example, different prices are set for VIP members and ordinary users, where VIP members will see a higher price compared to other users, based on the analysis of their consumption habits and purchasing capabilities. Some companies adopt complicated promotion rules and algorithms to implement price confusion settings to attract certain consumers who have difficulty in calculating real prices.[11]

Similar to algorithmic price discrimination as discussed in the "Antitrust/competition laws" section above, irrational algorithmic exploitation causing discrimination and bias is, in essence, an exploitative abuse of data dominance. Because most data directly link to consumers' personal information as well as the information asymmetry between counterparties and companies, companies with data dominance can easily infringe the rights of counterparties, including their workers and consumers. Traditionally, exploitative abuse operates in the realm of pricing; however, in the digital economy, exploitative abuse often operates in the aspects of algorithm design, privacy clauses, and data integration, which are difficult for consumers to identify, so the operators can carry out exploitative abuse in a covert way. Furthermore, the newly issued Algorithmic Recommendation Regulations explicitly stipulate that companies providing workers with job-scheduling services shall protect the legitimate rights and interests of the workers such as labour remuneration, rest and vacation, and establish and improve relevant algorithms for platform order distribution, composition and payment of remuneration, working hours, rewards and punishments, etc.

To address this predicament, many institutions have made efforts to establish ethical standards for algorithms. For example, the China Academy of Information and Communications Technology issued the White Paper on AI Governance (the "**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.

As "Big data killing" usually harms the interests of consumers, both the Consumer Protection Law and the E-Commerce Law explicitly require business operators to respect and equally protect the legitimate rights and interests of consumers; the E-Commerce Law further stipulates that 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, which additionally requires personal information processors to ensure the transparency of the decision-making and the fairness and impartiality of the results, and shall not impose unreasonable discriminatory treatment on individuals in respect of the transaction price and transaction conditions.

Legislators and academics have been bravely exploring the solutions to restrict the floodgate of algorithmic discrimination. The Algorithmic Recommendation Regulations 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 over-consumed. The Regulations intend to help companies set up an internal control over the utilisation of algorithms, and meanwhile set out principle rules to protect the rights of typical individual groups who are more likely to be harmed or discriminated by algorithms, such as minors, the elderly, labourers, and consumers.

* * *

Endnotes

1. International Data Corporation, IDC Worldwide Artificial Intelligence Spending Guide, March 2022.
2. Key Laboratory of Big Data Mining and Knowledge Management of the Chinese Academy of Science, 2019 White Paper of Artificial Intelligence Development.
3. iResearch, 2021 China's Artificial Intelligence Industry Report, February 2022.
4. *Id*.
5. National People's Congress, the 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and Outline of the Vision for 2035, March 2021.
6. International Data Corporation, IDC Worldwide Artificial Intelligence Spending Guide, March 2022.
7. Supreme People's Court, the Supreme People's Court on the Intellectual Property Trial Work of the People's Courts, October 2021.
8. Beijing Youth Daily, Beijing Consumer Association Announces the Investigation Result of "Taking Advantage of Existing Customers via Big Data", 28 March 2019, original Chinese version available at http://epaper.ynet.com/html/2019-03/28/content_323364.htm?div=-1.
9. *Supra* endnote 6.
10. Renwu, Food Delivery Riders Stuck in the System, 8 September 2020, original Chinese version available at https://mp.weixin.qq.com/s/Mes1RqIOdp48CMw4pXTwXw.
11. China Consumers Association: How does "big data kill" affect consumer rights and interests?, original Chinese version available at http://www.xinhuanet.com/2021-01/08/c_1126962189.htm.

Susan Xuanfeng Ning
Tel: +86 10 5878 5010 / Email: susan.ning@cn.kwm.com

Susan Ning is a senior partner and the head of the Regulatory Group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the *Journal of Cyber Affairs*. Her publications include *Big Data: Success Comes Down to Solid Compliance*, and *No "Data", No "Internet of Vehicles"*, etc.

Susan's practice areas cover self-assessment of network security, responding to network security checks, data compliance training, etc. Susan has assisted companies in sectors such as IT, transportation, finance, etc. in dealing with network security and data compliance issues.

Han Wu
Tel: +86 10 5878 5749 / Email: wuhan@cn.kwm.com

Han Wu is a partner of the Commercial and Regulatory Group. He excels in providing cybersecurity and data compliance advice to multinationals' Chinese branches and in establishing network security and data compliance systems for Chinese enterprises operating abroad.

In the areas of cybersecurity and data compliance, Han provides legal services including assisting clients in establishing a cybersecurity compliance system, self-investigation on cybersecurity, network security investigations, cybersecurity incidents, data fusion and identification of data assets, etc.

Han has provided legal services on cybersecurity and data compliance to companies in multi-industries. The projects he has participated in encompass industries of financial payment, consumer electronics, internet advertising and personal care, etc. Han is the only lawyer from a Chinese law firm featured in 40 Under 40 Data Lawyers by *Global Data Review* in 2018.

King & Wood Mallesons

18th Floor, East Tower, World Financial Center 1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020, P. R. China
Tel: +86 10 5878 5588 / URL: www.kwm.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

Banking Regulation
Blockchain & Cryptocurrency
Bribery & Corruption
Cartels
Corporate Tax
Employment & Labour Law
Energy
Fintech
Fund Finance
Initial Public Offerings
International Arbitration
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Pricing & Reimbursement

GLI GLOBAL LEGAL INSIGHTS