GLI GLOBAL LEGAL INSIGHTS

AI, Machine Learning & Big Data

2021

Third Edition

Contributing Editors: **Matt Berkowitz & Emma Maconick**

glg global legal group

Global Legal Insights
AI, Machine Learning & Big Data

2021, Third Edition
Contributing Editors: Matt Berkowitz & Emma Maconick
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS – AI, MACHINE LEARNING & BIG DATA

2021, THIRD EDITION

Contributing Editors
Matt Berkowitz & Emma Maconick, Shearman & Sterling LLP

Head of Production
Suzie Levy

Senior Editor
Sam Friend

Production Editor
Jane Simmons

Publisher
James Strode

Chief Media Officer
Fraser Allan

We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Matt Berkowitz & Emma Maconick of Shearman & Sterling LLP for all of their 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 978-1-83918-116-0
ISSN 2632-7120

Printed and bound by TJ Books Limited
Trecerus Industrial Estate, Padstow, Cornwall, PL28 8RW
May 2021

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 of market application, 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, the market size of AI in China could reach USD62.7 billion by the end of 2021, with a compound annual growth rate of 30.4% from 2019 to 2024.[1]

Trends

The Chinese Academy of Science recognises eight key AI technologies that have achieved major 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 own 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.[3] According to the Ministry of Industry and Information Technology ("**MIIT**"), the revenue of platform operational technical service based on cloud computing and big data technologies reached RMB2.2 trillion for the year of 2019, including revenue of typical cloud service and big data service amounting to RMB32.84 billion.[4]

The Chinese government recognises AI as an important component of national strategy and plans to establish an AI regulatory system in the near future. The State Council has included AI in the Report on the Work of the Government from 2017 to 2019 consecutively and intelligent manufacturing in 2020 and 2021, and has also promulgated a number of national strategic policies such as the *New-generation AI Development Plan* and the *Three-year Plan for New-generation AI Industry Development (2018–2020)* to set forth specific goals in technology achievement and the regulatory regime of AI in three eras from 2018 to 2030.

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. As a result, the telecommunication industry witnessed immense development in 2020, reaching a revenue of RMB802.7 billion for the first seven months in 2020, with emerging technologies such as big data, cloud computing, and data centres being the biggest contributors to the growth, according to the MIIT.[5] In addition, the financial industry, particularly intelligent risk control, has become the frontier of AI and big data application in recent years.

Due to the unprecedented need for AI and big data industry and the immense data demand for machine learning, the lawfulness and legitimacy of data sources has become the key legal issue arising out of the adoption of AI and big data machine learning. For example, under the *Cybersecurity Law of the PRC* ("***CSL***"), network operators (such as service providers adopting AI) may only collect and process personal information within the scope of the personal information subject's ("**PI subject**") consent, save for a few exceptions contemplated by laws and regulations. The immense demand for data to feed AI's machine learning becomes a motivation for some enterprises to illegally collect and use data on internet platforms. In particular, big data technologies in the financial industry have been taking the lead in the development of a digital economy in China, and the public security bureau of China has investigated and suspended the operation of a number of social credit information services that illegally collected citizens' credit information without consent and used it to build up marketable profiles of individuals or to feed the machine learning of AI models. On the other hand, 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.

Ownership/protection

When talking about AI ownership, we mainly focus on the ownership issues for AI algorithm 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 the Protection of Computer Software* ("***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 files, and "computer program" refers to coded command sequences that computers or other similar devices with information-processing ability could execute in order to achieve a required result, or symbolic command sequences or symbolic statement sequences that can be automatically transformed into coded command sequences. 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 original software copyright certificate holder shall consider initiating a new registration for the updated version, if it is materially changed in functionality and performance.

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.

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 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 *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 owner 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* 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*.[6] 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 *Draft 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 is yet to finalise, which may possibly further limit companies' ownership claims.

As of today, 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 the PRC* ("***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. With reference to the *Antitrust*

Guidelines for the Platform Economy ("***Guidelines***"), concerted conduct may also refer to the conduct whereby undertakings do not explicitly enter into an agreement or decision, but are actually 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 adopt algorithms that predict and align with the pricing of the competitors, there might be a *de facto* connection of will which 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 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.[7] 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 for abuse of 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 consumers' personal 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.

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 the purpose of identification of the dominant market position for the platform, assessment factors include users' multi-habitats, users' switching cost, difficulty for 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 in 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 thus data shall be afforded legal protection.[8] 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 *AML* recognises as abusing said dominant position, such as refusal to deal, price discrimination, unreasonable trade restrictions, tying, and others.

Board of directors/governance

One key issue in relation to introducing AI to companies' governance is the integrity of automated decision-making. 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.

From a national regulatory perspective, at the current stage, national standard-makers are trying to restrict the use of information systems' automated decision-making from a personal information protection perspective, which we understand may impact the automated decision regulations within companies' governance as well. Under the national standard *Information Security Technology – Personal Information Security Specification* ("***PI Specification***"), when decisions are made based on automated decisions by information systems and may significantly influence the PI subject's rights and interests (such as personal credit, loan limits, or interview screening based on user profiling), the PI subject shall be provided with methods to appeal.

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.

Regulations/government intervention

While few laws or regulations systematically address AI in China, there are rules regulating particular AI-related subject matters, such as the following:

- **Big data**: The *Draft Data Security Law* released in July 2020 directly addresses the national strategy in developing big data and enhancing data security. The National Information Security Standardisation Technical Committee ("**TC260**") has issued a series of recommended national standards regarding big data services and systems, including the *Information Security Technology – Big Data Security Management Guide*, *Information Security Technology – Big Data Security Management Guide*, and others, and also regarding big data security in specific sectors, such as the *Information Security Technology – Guide for Health Data Security*. The National Health Commission of the

PRC also issued the *Trial Provisions on Managing the Standards, Security and Service of National Healthcare Big Data* in July 2018 to set forth general system security requirements and big data protection measures such as storing data within the PRC.

- **Personal information protection and automated decision-making**: There are two overarching statutes setting forth general principles of personal information protection: the *Civil Code* released in May 2020 articulating general requirements for processing of personal information, along with the *CSL* articulating requirements for personal information protection for network operators. 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. The *Draft Personal Information Protection Law* released in October 2020 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, such as the Chinese government's administration of the "Health Code" adopting big data.
- **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 Cybersecurity Administration of China, effective since 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.
- **Automated driving**: The MIIT and other ministries jointly issued the *Trial Administrative Provisions on Road Tests of Intelligent Connected Vehicles*, effective since 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 own 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.
- **Finance**: The People's Bank of China ("**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 or entrusting of personal financial information.

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,[9] which further demonstrates the government's determination in AI regulation. In October 2019, the Big Data Security Standard Special Taskforce of 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.[10] In addition, in August 2020, the State Standardisation Administration, the China Administration of Cyberspace and three other State ministries jointly released the *Guidance on Establishing the New Generation of National AI Standardisation System* ("***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.

Algorithmic exploitation

The mass application of AI and big data gives rise to a serious concern of algorithmic exploitation in business models that build upon big data and algorithms. 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.[11] 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.

In essence, algorithmic exploitation is an exploitative abuse of data dominance, similar to algorithmic price discrimination as discussed in the "Antitrust/competition laws" section

above. Because most data directly links 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 operate 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.

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 ("**CAICT White Paper**"), which lays out ethical standards for using AI, such as that algorithms should protect individual rights. Currently, there is no labour law guidance or regulation related to algorithmic exploitation, making this uncharted legal territory. As the internet behemoths' unethical use of algorithms has become a hotly discussed issue in recent years, we expect that regulators may turn their attention to algorithmic exploitation in the near future.

From a compliance standpoint, companies should be aware of algorithmic exploitation and prepare for adjustments should regulators decide to tap into this uncharted territory. From an ethical perspective, companies might want to ensure their use of algorithms does not amount to algorithmic exploitation in order to avoid unnecessary business risks and promote corporate social responsibility, especially for companies that operate around algorithms.

Algorithmic discrimination

Almost all policy and ethical discourses on AI consider non-discrimination or non-bias as a central principle for AI design. Likewise, 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.

While China does not have a comprehensive anti-discrimination legal system, the issue has been addressed by specific laws and State Council regulations concerning various fields or disadvantaged groups, such as labour law, education law, and advertising law. For example, Article 9 of the *Advertising Law of the PRC* specifies that an advertisement shall be prohibited from, *inter alia*, containing any ethnically, racially, religiously, or sexually discriminatory content. For algorithm discrimination, unless its application falls into the specific regulations of these sectors, there is no anti-discrimination regulatory risk aside from ethical considerations.

However, legislators and academics have been bravely exploring the solutions to restrict the floodgate of algorithmic discrimination. The accountability and explainability of AI and big data algorithms are becoming the central issues of future AI regulations and ethical standards. A number of major market participants have made proposals in algorithmic regulations, such as Tencent publishing the *Advice on Strengthening the Construction of Technological Ethics and Implementing the Idea of Technologies for Good* in March 2019, and Megvii Technology publishing the *AI Application Standards* in September 2019. The year 2020 also witnessed substantial State efforts in setting forth future directions in AI regulations, such as the *Advice on Collaborating in Implementing AI Governance Principles* released by the Working Group of the Expert Committee of the Shanghai

National New Generation AI Innovative Development Pilot Zone in July 2020, and the *AI Standards Guidance* released by five ministries in August 2020. In March 2021, the Guangzhou Municipal Administration for Market Regulation held a seminar regarding big data discrimination, in which 10 major internet platform companies signed the *Commitment Letter of Platform Companies Maintaining Fair Market Competition Order* to warrant that, among other commitments, they would not exploit their advantage in data to conduct price discrimination.[12] In sum, a continuous and long-term campaign against algorithmic discrimination is well expected in China.

* * *

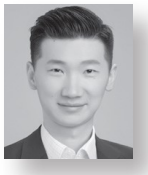
Endnotes

1. International Data Corporation and Inspur, 2020–2021 China Artificial Intelligence Computing Power Development Evaluation Report, December 2020.
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, 2019 China Artificial Intelligence Industry Research Report.
4. China Academy of Information and Communications Technology, the Big Data White Paper, December 2020.
5. *Id*.
6. *Beijing Weimeng Chunagke Network Technology Co., Ltd. v. Beijing Taoyou Tianxia Technology Co., Ltd.*, (2016) Jing 73 Civil Final No. 588, 30 December 2016.
7. 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.
8. *Supra* endnote 6.
9. National Standardisation Technical Committee, Notice on the Proposal of Establishing the AI Technical Sub-Committee of the National Information Security Standardisation Technical Committee, 21 October 2019, original Chinese version available at http://org.sacinfo.org.cn:8088/tcrm/recruit-index/notice/2401.do?menuItem=1.
10. Big Data Security Standard Special Taskforce of the National Information Security Standardisation Technical Committee, Artificial Intelligence Standardisation White Paper, 2019.
11. Renwu, Food Delivery Riders Stuck in the System, 8 September 2020, original Chinese version available at https://mp.weixin.qq.com/s/Mes1RqIOdp48CMw4pXTwXw.
12. Guangzhou Municipal Administration for Market Regulation, Guangzhou Municipal Administration for Market Regulation Held Seminar on "Big Data Discrimination" by Platforms and Administrative Guidance Conference on Regulating Fair Market Competition Order, original Chinese version available at http://scjgj.gz.gov.cn/zwdt/gzdt/content/post_7206705.html.

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