Legal 500
Country Comparative Guides 2026

China
Artificial Intelligence

Contributor

Han Kun Law Offices

Kevin Duan

Partner | kevin.duan@hankunlaw.com

Yaqi Li

Associate | yaqi.li@hankunlaw.com

Yufeng Gan

Associate | yufeng.gan@hankunlaw.com

Jiayu Song

Associate | jiayu.song@hankunlaw.com

This country-specific Q&A provides an overview of artificial intelligence laws and regulations applicable in China.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

China: Artificial Intelligence

1. What is the legal definition of "artificial intelligence" in your jurisdiction, if any? If no definition exists, how do regulators or courts typically describe artificial intelligence?

Currently, there is no specialized definition of "artificial intelligence" under Mainland China laws and regulations. Some recommended national standards and guidelines provide their own interpretations, such as "the research and development of the mechanisms and applications related to artificial intelligence systems," and "the use of computers or devices controlled by them to simulate, extend, or expand human intelligence through environmental perception, knowledge acquisition, and deductive reasoning." These interpretations are reflected in the national standard Information Technology – Artificial Intelligence – Terminology (GB/T 41867-2022, 信息技术 人工智能 术语), Section 3.1.2, and the Cybersecurity Standard Practice Guideline – Guidelines for the Prevention of AI Ethical Security Risks (网络安全标准实践指南——人工智能伦理安全风险防范指引), Section 2.1.

Furthermore, a subset of AI, "generative AI technologies," has been defined in the Interim Measures for the Management of Generative Artificial Intelligence Services as "models and related technologies capable of generating text, images, sounds, videos, and other content."

2. Has your country developed a national strategy for artificial intelligence? If yes, what progress has been made in its implementation? Are there plans for updates or revisions?

Yes. China's ambitions in artificial intelligence are outlined in the comprehensive New Generation Artificial Intelligence Development Plan (hereinafter the "Development Plan"), issued by the State Council of the PRC in 2017. The Development Plan details a three-step strategy for propelling China to the forefront of AI innovation, with milestones in 2020 for solidifying China's status as an innovative nation, by 2025 for leading-edge breakthroughs, and by 2030 for achieving top-tier innovation and integration in economic and social spheres. Moreover, the Development Plan specifies the key tasks to achieve these milestones, including but not limited to (i) building open and coordinated AI science and technology innovation systems; (ii) fostering a high-end, highly efficient smart economy; (iii) constructing a safe and convenient intelligent society; (iv) strengthening military-civilian integration in the AI domain; (v) building a safe and efficient intelligent infrastructure system; and, (vi) planning major scientific and technological projects for the new generation of AI.

In addition, the State Council issued the Opinions on Further Implementing the "Artificial Intelligence Plus" Initiative in August 2025, setting out policy measures to accelerate AI adoption across various sectors and strengthen supporting capabilities. The Opinions identify six priority areas for AI application, including scientific and technological innovation, industrial development, consumer services, public welfare, governance capability, and global cooperation. The Opinions also highlight key supporting areas for AI development, including models, data, computing power, applications, open-source ecosystems, talent, policies and regulations, and security.

3. Has your jurisdiction adopted any AI-specific laws, regulations, voluntary standards, or ethical guidelines? If so, please provide a brief overview. If not, which existing laws could be/are applied to artificial intelligence and the use of artificial intelligence, what are the main interpretive challenges, and are there any pending artificial intelligence legislative initiatives?

Yes. China has adopted a series of AI-specific regulations, voluntary standards and ethical guidelines, including but not limited to

Key AI-related regulations:

- *Administrative Provisions on Recommendation Algorithms in Internet-based Information Services ("Algorithm Recommendation Regulations")*, effective since March 1, 2022, focus on technologies underlying recommendation algorithms used in providing Internet services, many of which are AI-related, such as generation and synthesis algorithms and decision-making algorithms.

The regulations aim at creating a transparent and

equitable algorithmic environment. It requires the related AI or Algorithms service providers to be open about the logic driving their algorithms, to provide users with the ability to tailor or decline algorithmic suggestions, to establish processes for detecting and mitigating any inherent biases within their algorithms, and to fill for algorithm recommendation services with public opinion attributes or social mobilization ability, among other requirements.

- *Administrative Provisions on Deep Synthesis in Internet-based Information Services ("Deep Synthesis Regulations")*, effective since January 10, 2023, are designed to govern internet information service providers (and technology supporters) utilizing advanced deep synthesis technologies, encompassing deepfakes and various AI-generated materials that have the potential to obscure the distinction between actuality and artificial constructs. These regulations are meticulously designed to exert stringent control over content generation, aiming to eliminate user confusion or misidentification and to curb the propagation of illegal and misleading information. The requirements set out include but are not limited to prominent labeling of generated content, the establishment of a comprehensive rumor-refuting mechanism, and the emphasis on the obligation of algorithm filing.
- *Interim Measures for the Management of Generative Artificial Intelligence Services ("Generative AI Measures"),* effective since August 15, 2023, establish rules to regulate those who provide generative AI capabilities to the public within Mainland China. These Measures encompass content safety, prohibition of discrimination, fair competition, and data quality, and connect existing regulatory requirements such as information content supervision, personal information protection, intellectual property, unfair competition, technology ethics, generation content identification, security assessment, and algorithm filing.
- *Measures for the Labeling of AI-Generated Synthetic Content ("AI Content Labeling Measures")*, effective since September 1, 2025, further specify the labeling requirements for AI-generated content. The *AI Content Labeling Measures* introduce differentiated explicit labeling obligations for various types of AI-generated content, and require service providers to embed implicit labels containing prescribed information into the metadata of the AI-generated files. Online content distribution platforms and App stores are also responsible for verifying such labels.
- *Interim Measures for the Administration of Anthropomorphic AI Interactive Services* ("*Anthropomorphic AI Measures*"), effective since July 15, 2026, establish regulatory requirements for providers of anthropomorphic AI interactive services that simulate human personalities, thinking patterns and communication styles through continuous AI-powered emotional interaction. Key requirements include, but are not limited to, clearly informing users that they are interacting with an AI system, strengthening content safety and risk management mechanisms, providing necessary user guidance and intervention mechanisms, conducting security assessments and submitting relevant reports to local cyberspace administration authorities, and implementing enhanced protection measures for minors and elderly users.
- *Measures for Artificial Intelligence Technology Ethics Review and Service (Trial) ("AI Ethics Review Measures")*, effective since March 20, 2026, further refine the ethical review requirements for AI science and technology activities based on the *Technology Ethics Review Measures (Trial)*. The AI Ethics Review Measures establish various procedural requirements tailored to the characteristics of AI-related activities, including application and acceptance procedures, general review procedures, simplified procedures, expert re-review procedures, emergency procedures, and registration and filing requirements. The Measures focus on assessing whether AI science and technology activities comply with key ethical principles, including human well-being, fairness and justice, controllability and trustworthiness, transparency and explainability, accountability and traceability, and privacy protection.

Other recommended guidelines, including but not limited to:

- *Cybersecurity Standard Practice Guideline – Guidelines for the Prevention of AI Ethical Security Risks* released in January 2021, addresses potential ethical and safety risks

associated with artificial intelligence, providing guidelines for the safe conduct of AI-related activities, including R&D, design and manufacturing, deployment and application, etc.
- *The mandatory national standard GB 45438-2025, Cybersecurity Technology—Labeling Method for Content Generated by Artificial Intelligence*, was released in February 2025 and took effect on September 1, 2025. As a supporting standard to the AI Content Labeling Measures, it specifies detailed methods and provides examples for labeling various types of AI-generated content, including explicit labels for AI-generated content and interactive interfaces, as well as implicit labels embedded in the metadata of AI-generated files.
- *Basic Security Requirements for Generative Artificial Intelligence Service ("TC260-003 guidelines")* released on February 29, 2024, specifies the basic security requirements for generative artificial intelligence services. This guideline serves as an important reference in the security assessment process during the LLM launch filing and covers aspects such as training data security, model security, security measures, and criteria for security assessments.
- *The recommended national standard GB/T45654—2025, Cyber Security Technology—Basic Security Requirements for Generative Artificial Intelligence Service ("GB/T45654—2025 standard"),* was released in April 2025 and took effect on November 1, 2025. It further refines the requirements set out in the TC260-003 guidelines and introduces several additional provisions, such as security mechanisms for on-device large models, requirements for refusal to answer inappropriate questions, specifications for the regular updates of test question banks.

Furthermore, it is noteworthy that, according to the 2024 Legislative Work Plan issued by the State Council of the PRC, the *AI Act* is scheduled to be submitted to the Standing Committee of the National People's Congress for review. However, the draft of the AI Act has not yet been published, and the 2025 and 2026 Legislative Work Plans do not include any legislative work related to the AI Act. Therefore, whether a unified AI Act will ultimately be introduced remains uncertain. Howerver, the 2026 State Council Legislative Work Plan now expressly calls for accelerating comprehensive legislation to promote the healthy development of AI and for improving legislation on common AI elements (including data, computing power, algorithms, intellectual property, cybersecurity, and supply-chain security) and key application scenarios.

4. Are there legal requirements for artificial intelligence transparency, explainability, or audits? Are there obligations to disclose the use of artificial intelligence to customers/clients?

Yes. China has established certain requirements relating to AI transparency, explainability, and audits through algorithm-related regulations.

- For transparency, providers of algorithm recommendation services are required to inform users of the use of algorithm recommendation technologies in a prominent manner and disclose relevant information, including the basic principles, intended purposes, and main operating mechanisms of their algorithms (Article 16 of the *Algorithm Recommendation Regulations*). In addition, generative AI service providers are required to implement content labeling requirements for AI-generated content (Article 17 of the *Deep Synthesis Regulations*; Article 12 of the *Generative AI Measures*), and providers of anthropomorphic AI interactive services are also required to inform users that they are interacting with an AI system rather than a human being (Article 18 of the *Anthropomorphic AI Measures*).
- For explainability, Chinese regulations encourage algorithm recommendation service providers to improve the transparency and explainability of algorithmic rules, including rules relating to retrieval, ranking, selection, recommendation, and display, etc. (Article 12 of the *Algorithm Recommendation Regulations*). Furthermore, where algorithmic decisions have a material impact on users' rights and interests, algorithm recommendation service providers are required to provide explanations and assume corresponding responsibilities in accordance with applicable laws (Article 17 of the *Algorithm Recommendation Regulations*).
- For audits, algorithm recommendation service providers are required to periodically review, evaluate, and verify their algorithm mechanisms, models, data, and application results, and ensure that their algorithms do not

involve inducement of user addiction, excessive consumption, or other practices violating applicable laws, regulations, or ethical standards (Article 8 of the *Algorithm Recommendation Regulations*). In addition, providers of anthropomorphic AI interactive services, as well as providers of algorithm recommendation services, deep synthesis services, and generative AI services that possess public opinion attributes or social mobilization ability, are required to conduct security assessments and submit relevant reports to the cyberspace authorities as part of applicable regulatory filing or registration requirements.

5. Are there legal requirements or best practice expectations for human oversight and human-in-the-loop in artificial intelligence systems?

Yes. China algorithm-related regulations require AI service providers to establish human oversight mechanisms in specific scenarios, particularly where AI systems may affect users' rights and interests or generate public-facing content.

First, AI service providers are required in certain scenarios to implement human review and intervention mechanisms. Algorithm recommendation service providers are required to establish mechanisms for human intervention and user choice, particularly in key scenarios such as homepage displays, trending searches, rankings, and pop-up notifications. Deep synthesis service providers are also required to review user input data and generated content through technical or manual means.

Second, AI service providers are also expected to establish human escalation and correction mechanisms. For example, algorithm recommendation service providers, deep synthesis service providers, and generative AI service providers are required to establish accessible complaint and reporting channels, specify handling procedures and response timelines, and process complaints and reports in a timely manner.

Furthermore, AI service providers and other regulated entities (such as algorithm recommendation service providers, deep synthesis service providers, and technical support providers for deep synthesis services) are required to strengthen algorithm governance, including conducting regular reviews, evaluations, and verification of algorithm mechanisms, models, data, and application results. Certain AI services are also subject to security assessment requirements, as summarized in the response to Question 4. These requirements may involve human review and assessment of algorithm performance, safety risks, and compliance issues.

6. Are there specific legal or regulatory requirements addressing algorithmic bias, discrimination, or fairness in AI systems (including gender bias)?

Yes. China's current regulations governing algorithms and artificial intelligence contain requirements addressing algorithmic bias, discrimination and fairness. Specifically:

Article 4 of the *Interim Measures for the Administration of Generative Artificial Intelligence Services* expressly requires providers of generative AI services to take effective measures throughout algorithm design, training data selection, model generation and optimization, and service provision to prevent discrimination based on ethnicity, belief, nationality, region, gender, age, occupation, health and other factors. Article 21 of the *Provisions on the Administration of Algorithmic Recommendations in Internet Information Services* requires algorithmic recommendation service providers that sell goods or provide services to consumers to protect consumers' right to fair transactions and prohibits the use of algorithms to impose unreasonable differential treatment in transaction prices or other transaction terms based on consumers' preferences, transaction habits or other characteristics. In addition, Article 24 of the *Personal Information Protection Law* requires that automated decision-making involving personal information be transparent and that its outcomes be fair and impartial. Where an automated decision has a significant impact on an individual's rights and interests, the individual has the right to request an explanation and to refuse decisions made solely through automated decision-making.

7. What legal frameworks apply to AI-related harm and defective artificial intelligence systems? Who can be held liable (developer, deployer, victim of the damage, others), how is liability allocated, and what burden of proof applies to victims?

Legal framework

China currently does not have specific legislation establishing a liability framework for defective artificial

intelligence systems or AI-related harm. Instead, liability arising from AI-related harm is generally determined under existing legal frameworks, including *the Civil Code, the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law ("PIPL"), the Product Quality Law, and the Criminal Law*.

From a civil liability perspective, AI-related harm may involve infringement of personal information, privacy, portrait, reputation, intellectual property rights, or other legitimate rights and interests. In cases related to AI voice and image copyright infringement, courts typically apply the principle of fault liability, obligating AI service providers to bear tort liability for any damages incurred within the scope of their fault (e.g., (2024) Yue 0192 Min Chu No. 113). When determining whether an AI service provider is at fault, the court will consider not only whether it has committed direct tort, but also whether it has fulfilled its duty of care and adopted appropriate preventive measures (e.g., (2024) Zhe 01 Min Zhong No. 10332).

Notably, Article 69 of the PIPL establishes fault-presumption liability in instances where a personal information handler infringes upon rights or interests through the processing of personal information. This requirement mandates that personal information handlers must assume liability for damages and other related tort liabilities unless they can prove that they were not at fault.

AI-related activities may also trigger criminal liability where the relevant conduct constitutes a crime under the Criminal Law. For example, using AI technology to fabricate or disseminate false information that disrupts social order may constitute the crime of fabricating or intentionally disseminating false information under Article 291(A) of the Criminal Law; using AI technology for bullying, intimidation, or threats may constitute the crime of picking quarrels and provoking trouble under Article 293; and using AI technologies such as deepfakes to illegally obtain personal information may constitute the crime of infringing citizens' personal information under Article 253 (A).

Potentially liable parties and allocation of liability

In the absence of explicit regulations on defective AI systems, the responsibility for harm caused by an AI system is determined based on the principles of general civil tort law and the specific circumstances of each case.

According to the *Civil Code*, the party responsible for damage is determined based on the fault that caused the harm. This fault can be attributed to the developer, the deployer, and the user. If multiple parties contribute to the damage, they are held individually liable for their respective share. In cases where determining individual responsibility is impossible, joint and several liability may be imposed. The victim's fault or events, such as force majeure, may partially or completely absolve the party responsible for the damage.

For instance, under the specific autonomous cars regulations, if an intelligent connected vehicle operating in autonomous driving mode causes damage in a traffic accident, and the responsibility is determined to be with the intelligent connected vehicle, the entity conducting the testing and application of the intelligent connected vehicle model shall bear the corresponding compensation liability according to law. If the car manufacturers, autonomous driving system development units, infrastructure and equipment providers, safety officers, and other relevant entities are at fault for the occurrence of the traffic accident, in that case, the entity may legally seek compensation from them. If a crime is committed, the responsible individuals shall be held criminally liable according to the law. (Implementation Guidelines for Pilot Implementation of Intelligent Connected Vehicle Access and Road Traffic (Trial), Article 19; Regulations on the Management of Intelligent-Connected Vehicles in Shenzhen Special Economic Zone, Article 53-54; Measures for the Testing and Application Management of Intelligent-Connected Vehicles in Shanghai, Article 43)

Burden of proof

Under current laws, there is no specific provisions regarding the burden of proof in cases involving AI-related damages, so general rules will apply. According to Article 67 of the Civil Procedure Law, parties are responsible for providing evidence to support their claims, and therefore the party seeking compensation bears the burden of proof. However, it is worth noting that there are instances of burdenshift. For example, under Article 69 of the PIPL, if processing personal information infringes on personal information rights and causes damage, and the personal information handler cannot prove they are not at fault, they shall bear liability for damages and other tort liabilities. In such cases, if the personal information handler cannot demonstrate that it was not at fault for the damage, it is presumed that the defendant was at fault in causing the damage, and it should bear the corresponding liability for compensation.

Furthermore, there are ongoing debates within the academic and practical communities regarding the liability for defective AI systems. Some argue that product liability under the Product Quality Law should apply, indicating that AI product developers should be held

liable for damages caused by defects in their products, regardless of fault, unless they can demonstrate a legal exemption such as the defect being undetectable with current scientific and technical knowledge. Others believe that the aforementioned approach may lead to an unlimited expansion of liability, potentially hindering technological innovation. As an alternative, they propose adopting a fault-based liability principle, holding AI system developers accountable for tort damages to others' civil rights only within the scope of their fault, with fault-presumption or strict liability applied only in exceptional circumstances as specified by law.

8. What cybersecurity obligations apply to AI systems?

AI systems should comply with the cybersecurity requirements under the *Cybersecurity Law*, the *Personal Information Protection Law*, the *Regulations on Network Data Security Management*, and other applicable laws and regulations.

- **Network and system security.** Operators of AI systems generally qualify as network operators under the *Cybersecurity Law* and should implement the Multi-Level Protection Scheme for cybersecurity, establish internal security policies and operating procedures, designate responsible personnel, adopt technical measures to prevent cyberattacks, intrusions and malicious programs, monitor network operations, and retain relevant network logs for at least six months. They should also implement measures such as data classification, backup and encryption. Where a network product or service contains vulnerabilities or other security risks, the operator should promptly remediate them, notify users and report to the competent authorities as legally required. In the event of a cybersecurity incident, the operator should immediately activate its emergency response plan and take remedial measures.
- **Data and personal information security.** When processing training data, user inputs, interaction records or other network data, AI systems should establish data security management policies and adopt measures such as encryption, backup, access controls and security authentication. In the event of data leakage, tampering or loss, the operator should take immediate remedial action and, depending on the circumstances, notify the competent authorities, affected individuals or other interested parties.
- **Important data and critical information infrastructure.** Where an AI system processes important data or is used by a critical information infrastructure operator, stricter requirements may apply. These may include appointing dedicated data security personnel and establishing a dedicated management body, conducting periodic risk assessments, submitting annual important data risk assessment reports, and complying with data localization and cross-border data transfer security requirements.

9. Is the use of artificial intelligence insured and/or insurable in your jurisdiction, including with cyber policies? Are there market trends, or limitations?

Yes. AI-related risks can be insured in China, although the market for AI-specific insurance products is still at an early stage of development.

For example, insurers have started to explore insurance products specifically addressing risks arising from AI applications. Certain insurers in China have introduced insurance products covering liabilities arising from AI-generated content, such as intellectual property infringement or other third-party claims caused by AI-generated outputs. In addition, insurance mechanisms have also been explored for AI infrastructure-related risks, such as performance guarantee insurance for computing power services, which may provide compensation where the actual computing performance delivered by a service provider fails to meet agreed standards.

The AI insurance market in China is expected to continue developing as AI adoption increases. Regulatory authorities in certain regions, such as Shanghai, Zhejiang, and Shenzhen, have encouraged insurance institutions to develop insurance products tailored to AI-related risks and establish risk compensation mechanisms for AI products and services. Nevertheless, AI insurance remains subject to certain limitations, including difficulties in assessing and quantifying AI-related risks due to limited historical claims data, uncertainties regarding liability allocation among AI developers, providers and users, and the lack of standardized coverage for certain emerging AI risks.

10. Can artificial intelligence be named as an

inventor in a patent application filed in your jurisdiction? If not, what is the current legal position?

In China, artificial intelligence (AI) cannot be named as an inventor in a patent application. This stems from two main reasons:

- Firstly, China's legal framework classifies patent-related rights as a form of civil right, which can only be held by natural persons or legal entities (such as corporations, associations, etc.). Consequently, an inventor enjoys certain rights, such as the right to be named on the patent, which AI cannot possess. This stance is supported by the China National Intellectual Property Administration (CNIPA) in its decision on Patent ZL20198006158.0, which addressed Dr. Stephen Thaler's attempt to list the AI system DABUS as the inventor. Dr. Thaler has made similar attempts in multiple jurisdictions worldwide, seeking to have AI recognized as an inventor.
- Secondly, Chinese patent legislation stipulates that an inventor must be a natural person. According to the documents issued by the China National Intellectual Property Administration (CNIPA), including the Guidelines for Patent Applications Related to Artificial Intelligence (Trial) and Section 4.1.2 of Part I, Chapter 1 of the Patent Examination Guidelines, only natural persons can be listed as inventors. Legal entities, collectives, or AI systems are not eligible.

11. Do images or works generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to, and under what conditions?

In addressing this issue, China's legislative and judicial spheres have made preliminary explorations and engaged in discussions, but clear rules have yet to be established. More cases and rules are needed to make things clearer.

- From a legislative standpoint, the Copyright-related Law is open to interpretation, defining a “work” as any original creation in the fields of literature, art, or science that can take a physical form. It must be a product of “intellectual activity”, but the law doesn't explicitly say AI-generated images can't be copyrighted.
- From a judicial standpoint, some local courts in China have already issued effective judgments regarding the copyrightability of AI-generated content. The courts generally recognize that AI-generated images may be eligible for copyright protection if they reflect the user's original intellectual input. In such cases, copyright is typically attributed to the user of the AI. However, there is currently inconsistency among courts in how they determine what constitutes “original intellectual input."
- In cases (2023) Jing 0491 Min Chu No. 11279 and (2024) Su 0581 Min Chu No. 6697, the courts held that the user's selection and refinement of prompts, along with the process of choosing from among multiple output images generated by the AI, demonstrated original intellectual input. Therefore, the resulting images could be protected by copyright.
- By contrast, in (2025) Su 05 Min Zhong No.4840, the court took a stricter approach. It found that the user had failed to provide original creation records proving specific expressive choices regarding layout, composition, lines, and colours. The court further noted that general prompts are more akin to abstract ideas rather than copyrightable expressions, and that only when the user makes concrete choices on such expressive elements can the resulting work be eligible for protection.

12. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations, or guidelines, been introduced regarding AI-driven hiring, performance assessment, or employee monitoring?

With the development of generative artificial intelligence and algorithm technology, artificial intelligence systems have become common knowledge-based tools. The main issues to consider when using artificial intelligence systems in the workplace include:

- Content compliance requirements. Employees are not allowed to violate legal and regulatory requirements when using AI systems and are not allowed to create, copy, publish, or

disseminate content prohibited by laws and regulations (such as content suspected of insult, defamation, discrimination, or other inappropriate content).
- Personal information protection. If the AI system processes personal data, the employee should comply with the requirements of the Personal Information Protection Law and other relevant laws and regulations. For example, processing activities should have a legitimate basis.
- Protection of trade secrets. The data uploaded to third-party AI system providers may not be confidential or secure. Employees should carefully input any confidential information when using AI systems, including but not limited to: 1) trade secrets; 2) technical secrets, and any other information, data, or documents subject to any confidentiality clause.
- Accuracy and reliability. Given the principles, characteristics, and current technological stage of AI systems, they may generate incorrect or misleading information, which may include unauthorized information, data, or third-party intellectual property, as well as reflect biases in training data. Employees should fulfill their duty of careful attention, conduct necessary reviews on the quality, accuracy, authenticity, and completeness of their generated content, and be responsible for any work results generated using AI systems.

13. What are the main privacy/data protection issues arising from artificial intelligence development and use (including training data)? Have data protection authorities issued guidelines or rulings on artificial intelligence, and what are the key takeaways?

In China, privacy issues arising from the use of artificial intelligence are mainly including, but not limited to

- Unauthorized collection of personal information. This risk may arise notably in AI applications that require substantial data inputs. The inadequacy of current data trading and circulation mechanisms exacerbates this risk, giving rise to illicit practices such as unauthorized data transactions on the dark web and the collection of personal information without obtaining the necessary consent.
- Using personal information for training without consent. AI service providers frequently collect user input data to continually enhance AI algorithm models through training and fine-tuning processes. However, when individuals are not adequately informed or fail to provide valid consent, there exists a risk of infringing upon the privacy rights as well as the personal information rights and interests of personal information subjects. Chinese laws and guidelines related to GenAI address these concerns with specific requirements. Specifically, the use of personal information for AI algorithm training should only proceed with consent or other legal bases. Furthermore, AI service providers are encouraged to provide accessible options for users, such as user-friendly features or voice control commands, to opt out of having their input information used for training purposes.
- Illegal cross-border transfer of personal information. This risk may arise when the AI service provider is based overseas or the AI product is deployed on overseas systems or servers, thereby potentially involving the cross-border transfer of personal information. Under Chinese law, personal information handlers should adhere to Article 38 of the PIPL when transferring personal information overseas, which includes applying for data export security assessment, concluding standard contracts for the export of personal information, or passing personal information protection certification. Furthermore, as stipulated by Article 39 and Article 55 of the PIPL, it is necessary to inform personal information subjects about the cross-border transfer of their personal information, obtain their valid and separate consent, and conduct a personal information protection impact assessment (PIPIA). In addition, various regions in China have issued negative lists for cross-border data transfer from pilot free trade zones. The Negative List for Data Export Administration in the China (Beijing) Pilot Free Trade Zone (2025 Edition) (*中国（北京）自由贸易试验区、国家服务业扩大开放综合示范区数据出境管理清单（负面清单）（2025版）*) specifically covers "AI training data" and classifies high-value sensitive data collected or generated during research and development that is relevant to industry competitiveness as important data, including data used in model training, algorithm development, product testing, and other related scenarios. China has

also established a mechanism for the mutual recognition and application of such negative lists across pilot free trade zones, under which a negative list issued by one pilot free trade zone for a particular sector may be referred to and applied by other pilot free trade zones.

14. How is data scraping regulated in your jurisdiction from an IP, privacy and competition perspective? Are there recent precedents addressing the legality of data scraping for training of artificial intelligence systems?

From IP, privacy, and competition perspectives data scraping is currently not completely prohibited.

- The court will comprehensively judge the nature of the scraped data, the legality of the scraping methods, the competitive relationship between the scraping party and the scraped party, the impact on the scraped website, and the purpose of using the scraped data to determine whether the data scraping behavior constitutes infringement ; In addition, if the scraped data is protected by intellectual property rights, unauthorized use may constitute intellectual property infringement under the law (especially in the unauthorized disclosure of relevant data or the use of data for profit purposes).
- In practice, the courts determine the legality of data scraping, mainly by comprehensively examining the following points:
- Is there a competitive relationship in business between the scraper and the scraped party?
- Whether the scraped data is public data, whether it involves personal information, copyright data, and other specially protected data, and whether it may constitute the data rights of the scraped party.
- The legality of scraping methods. Generally speaking, taking technical measures to bypass access restrictions on scraped websites is considered illegal access, such as cracking payment restrictions, verification codes, IP access restrictions, etc.
- Whether data scraping is allowed in the ROBOTS Protocol, user agreement, etc. of the crawled website.
- The scale of the data scraped and whether it has caused improper impact or additional operational burden on the scraped website?
- Does the use of scraping data cause an improper impact on data development and utilization, or cause harm to consumer interests?

15. To what extent is the prohibition of data scraping in the terms of use of a website enforceable?

For the terms of use regarding restrictions on data scraping set by websites, judicial practice follows the principle of reasonableness in determining their effectiveness and does not unconditionally recognize them. In some cases, courts believe that, given that the plaintiff has made a legal statement through the website prohibiting the unauthorized use of web scraping software to obtain and use the data in question, even if the data in question has been made public, it is not open data that can be obtained and used arbitrarily. Therefore, other entities should not indiscriminately scrape and use the data in question and should use it within the necessary limits in accordance with the principles of kindness and good faith. From this, it can be seen that even though the legal statements on relevant websites prohibit any scraper from accessing data, existing precedents still recognize access to publicly available data within reasonable limits.

16. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence? What are its powers and enforcement tools?

At present, China does not have a single unified regulatory body overseeing the application and execution of artificial intelligence. Instead, a coalition of regulatory authorities takes part in supervising different facets of AI utilization, which notably comprises the following:

- The Cyberspace Administration of China (CAC), is pivotal in formulating and enforcing internet-related regulations, including those impacting AI.
- The Ministry of Industry and Information Technology (MIIT), driving the integration of AI within industrial development and technological innovation.
- The Ministry of Science and Technology (MST), is instrumental in fostering AI research and development, as well as guiding the ethical and sustainable growth of AI technologies.
- The Ministry of Public Security (MPS), ensures the security aspects of AI applications and

safeguards against their misuse in criminal activities.
- The National Development and Reform Commission (NDRC), plays a macroeconomic role, including the strategic planning and policy-making that influence AI's role in economic development.
- This multi-faceted approach ensures a comprehensive regulatory framework that addresses the diverse and evolving nature of AI technologies.

17. How widespread is the adoption of artificial intelligence in businesses in your jurisdiction, and which sectors are leading?

In China, AI technology is extensively applied across various industries, significantly empowering sectors such as finance, healthcare, education, industrial manufacturing, and law.

- Within enterprises, AI technologies optimize production processes, predict maintenance requirements, and automate production lines, thereby effectively improving productivity and operational efficiency. Beyond internal applications, AI is also seamlessly integrated into a variety of electronic devices, household appliances, and industrial equipment, significantly enhancing the intelligence and functionality of these products and services.
- Specifically regarding publicly offered generative and synthetic algorithm services, there are currently more than 1,500 generative AI services registered with the Cyberspace Administration of China (CAC). Additionally, nearly eight thousand deep synthetic service algorithms have successfully passed the algorithm filing process. These technologies serve a diverse range of industries and are integrated into various applications, such as intelligent customer service, image generation, speech recognition, and digital humans.
- Notably, the government supports AI with policies such as the Ministry of Science and Technology's 2022 initiative to develop demonstration projects in smart farming, ports, mines, homes, education, driving, healthcare, legal systems, and supply chains. Cities like Shanghai are also promoting AI across various sectors to innovate and enhance urban services. In January 2026, the Ministry of Industry and Information Technology and seven other government departments further issued the *Implementation Opinions on the Special Initiative for "AI + Manufacturing"* (《"人工智能+制造"专项行动实施意见》), aiming to promote the large-scale and in-depth application of AI technologies across key manufacturing industries. Moreover, as announced in May 2025, China's Ministry of Industry and IT promotes "AI + Industry," funding 11 national AI innovation zones and 400+ specialized "little giant" firms.

18. How is artificial intelligence used in the legal sector, by lawyers and/or in-house counsels? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns?

AI is being used by lawyers and in-house counsels for various legal tasks. The main application scenario of AI in the Chinese legal industry is to provide intelligent contract review, legal consultation, legal document generation, legal knowledge retrieval, and legal text reading functions to lawyers and in-house counsels.

However, legal professionals should pay attention to the accuracy and reliability of AI-generated content, as well as the confidentiality of customer information during the research process of legal issues, in order to use AI to assist legal work safely and effectively.

19. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

Key Challenges:

- Data Privacy: AI's use in legal tasks carries risks like client data leaks. Lawyers must focus on safeguarding data, steering clear of entering sensitive client or firm information into AI systems.
- Technical Learning: AI is changing how lawyers work, necessitating substantial effort to learn AI tools for tasks like contract review and case retrieval.
- Diminished Service Demand: AI tools may automate routine legal tasks, possibly decreasing the demand for certain traditional legal services.
- Reduced Industry Barriers: AI could make the legal industry more transparent, potentially affecting lawyers' fees as clients become more informed.

- Fact Verification: AI's capacity to create convincing falsehoods complicates fact-checking, requiring lawyers to use advanced tools to verify information authenticity.

Key Opportunities:

- Improve Efficiency: AI tools can accelerate legal work, reducing time spent on legal research and allowing junior lawyers to quickly acquire professional knowledge.
- Reduce Repetitive Work: AI can streamline repetitive tasks like document comparison, enhancing accuracy and freeing lawyers to focus on more substantive work.
- New Legal Demands: AI's rise in new technologies creates fresh legal challenges and research directions, increasing demand for legal expertise.
- Enhance Client Accessibility: AI can lower legal service costs, making them more accessible to a wider client base.
- Improve Service Quality: AI enhances the precision of legal services, such as contract review and document proofreading, and helps lawyers understand new sectors, leading to more comprehensive and high-quality legal advice.

20. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months? Are there any ongoing initiatives that could reshape AI governance?

According to the 2026 Legislative Work Plan issued by the State Council of the PRC, while a unified AI Act may not be released in 2026, China still plans to advance legislative efforts aimed at promoting the healthy development of AI. The legislative efforts are expected to focus on establishing a comprehensive AI governance framework and improving rules concerning key AI-related elements, including data, computing power, algorithms, intellectual property rights, cybersecurity, and supply chain security, as well as key application scenarios.

As suggested in previous speeches by legislative officials, China's current approach to AI governance will explore an inclusive, cautious, and phased legislative strategy, including:

- Prioritizing the flexible application of existing legal rules, including the use of statutory or judicial interpretation to address prominent legal issues arising from AI development, such as the training of LLMs and the fair use of copyrighted materials;
- Allowing pilot legislation in specific AI application scenarios, enabling local governments to explore within the scope of their legislative powers, or through demonstration projects organized by relevant national authorities;
- Adopting a “small, fast, and targeted” legislative approach in areas requiring urgent legal regulation, including by amending existing laws to address emerging needs.

What's more, China is actively establishing additional AI-related standards aimed at guiding domestic AI enterprises and providing a framework for regulatory compliance. Currently, several standards are in the drafting, public consultation, or approval stages, including but not limited to:

- Technical requirements for retrieval-augmented generation (RAG);
- Technical specifications for embodied large models and robots;
- Standards for AI agents and agent platforms;
- Standards related to Model-as-a-Service (MaaS);
- Standards for trustworthy datasets.

Contributors

Kevin Duan
Partner
kevin.duan@hankunlaw.com

Yaqi Li
Associate
yaqi.li@hankunlaw.com

Yufeng Gan
Associate
yufeng.gan@hankunlaw.com

Jiayu Song
Associate
jiayu.song@hankunlaw.com

