



CHINA

# AI Laws of the World



# Introduction



Artificial intelligence (AI) is rapidly transforming the way we work. As AI technology advances, governments are grappling with how to regulate its development to maximise benefits whilst mitigating risks.

Some jurisdictions have implemented AI-specific laws, whilst others are in the process of drafting regulations, and many rely on existing legal frameworks to address AI-related concerns.

This guide provides an overview of AI laws and proposed regulations across 40+ countries. It highlights key legislative developments, including regulations, proposed bills and guidelines issued by governmental bodies.

As the global landscape of AI regulation evolves at an accelerating pace, our 2025 Q1 snapshot provides an insightful overview of these developments, as well as of the common thematic approaches of lawmakers and AI-focused organisations around the world.

## Global key contacts



**Gareth Stokes**  
Partner  
Global Co-Chair, AI Practice  
[gareth.stokes@dlapiper.com](mailto:gareth.stokes@dlapiper.com)  
[Full bio](#)



**Jeanne Dazier**  
Partner  
Global Co-Chair, AI Practice  
[jeanne.dazier@dlapiper.com](mailto:jeanne.dazier@dlapiper.com)  
[Full bio](#)



**Danny Tobey**  
Partner  
Global Co-Chair AI and  
Data Analytics  
[danny.tobey@us.dlapiper.com](mailto:danny.tobey@us.dlapiper.com)  
[Full bio](#)



## Law / proposed law

There is no single comprehensive AI law in the People's Republic of China (PRC). Instead, rules relating to the use and deployment of AI are found in a number of specific laws, regulations and mandatory national standards that regulate different subcategories of AI technologies and services. These include:

- The [Interim Measures for the Management of Generative Artificial Intelligence Services](#) (**GenAI Measures**), which came into force on 15 August 2023 and are the first piece of generative AI-specific regulation for the PRC, regulating the development and application of generative AI technology. The GenAI Measures apply to the use of generative AI technology to provide services that generate contents (including any texts, images, audios, and videos) to the 'public within the PRC' (which has a very wide interpretation). The GenAI Measures outline service providers' obligations in various areas, including model training, content management, service management and user protection.
- The [Administrative Provisions on Deep Synthesis in Internet-based Information Services](#) (**Deep Synthesis Provisions**) came into force on 10 January 2023 and apply to the provision of internet-based information services using deep synthesis technologies within the PRC. Deep synthesis technology is broadly defined, and includes any technology that employs deep learning, virtual reality, or other algorithms that are synthetic or generative (such as text/Q&A generation, image generation and voice attribute editing). The Deep Synthesis Provisions impose compliance obligations on various players, including providers of deep synthesis services, providers of technical support for deep synthesis services and users of such services. Particularly, there is a requirement for deep synthesis service providers to verify the real identity of users (by way of mobile phone number, ID card number, unified social credit code or national online identity authentication services) before they can release the services to the users.
- The [Administrative Provisions on Recommendation Algorithms in Internet-based Information Services](#) of the Cyberspace Administration of China came into force on 1 March 2022 (**Recommendation Algorithms Provisions**) and apply to any entity that uses recommendation algorithm technologies to provide internet-based information services within PRC. This includes the use of algorithm technologies,

including generation and synthesis technology, personalised pushing technology and ranking and selection technology, etc., to provide users with information. The Recommendation Algorithms Provisions also emphasise the protection of the user. Service providers are required to inform users about the provision of algorithm services, including the principles behind them, their intended purposes and how they operate.

- The Measures for the Labeling of Artificial Intelligence Generated and Synthesized Content (AIGC Labelling Measures) took effect on 1 September. The AIGC Labelling Measures apply to online information service providers that offer AI generative and synthetic services. Such providers are required to add different types of explicit and /or implicit labels to AI-generated content based on contexts, and to restrict the dissemination of non-labelled content via their service platforms either by user terms or by implementing technical measures.
- The mandatory national standard the Cybersecurity Technology—Labelling Method for Content Generated by Artificial Intelligence (AIGC Labelling Standard) took effect on 1 September 2025. The AIGC Labelling Standard implements the AIGC Labelling Measures and sets out detailed standards, specifications, and operational procedures for labelling AI-generated content.
- The Provisional Measures on the Administration of Human-like Interactive Artificial Intelligence Services (Draft for Public Comments) were released on 27 December 2025 to solicit public comment till 25 January 2026. The draft applies to AI services that present simulated human personality traits, thinking patterns and communication styles, and interact with users emotionally through text, images, audio, video or other means. It has a particular focus on addressing psychological risks by requiring providers to warn users against excessive use and to intervene when users show signs of addiction.
- The Amendment to the Cybersecurity Law took effect on 1 January 2026. A general clause on AI is introduced, stating that the government will improve ethical norms for AI while strengthening AI risk monitoring and assessment and safety oversight — potentially paving the way for further AI regulations.

During the 2025 National People’s Congress, several delegates proposed the drafting of a specific AI law to address emerging risks, encourage innovation and establish a more consistent AI governance system. In particular, the possibility of classifying AI services into different risk categories and regulating them accordingly has been discussed.

## Regulatory guidance / voluntary codes

In addition to enacting laws specifically pertaining to AI-related technologies, the PRC also regulates AI through the implementation of recommended national standards and regulatory guidance:

- Basic Security Requirements for Generative Artificial Intelligence Service (GB/T 45654-2025): sets out requirements regarding training data security, model security, and technical measures that AI services providers should implement during their operation. It also provides guidance on how to conduct administrative filings with the Chinese authorities, which may be necessary for providing AI services to external users.

- Security Specification for Generative Artificial Intelligence Pre-Training and Fine-Tuning Data (GB/T 45652-2025) (**AI Data Standard**): sets out the security and data privacy requirements for pre-training and fine-tuning data in the context of generative AI.
- Generative Artificial Intelligence Data Annotation Security Specification (GB/T 45674-2025): sets out specific rules and procedures on data annotation.
- Basic Security Requirements for Generative Artificial Intelligence Service (TC260-003/2004): a set of technical standards for generative AI. It provides guidelines for generative AI service providers in relation to training data, algorithms and content generated by AI and require service providers to implement assessments and measures to mitigate risks associated with generative AI.

## Appointed supervisory authority

While a single national supervisory body with specific authority for AI has not yet been appointed in PRC, the development of AI-related regulations is undertaken collaboratively by various governmental authorities (including the Cyberspace Administration of China/CAC, the Ministry of Education, the Ministry of Science and Technology, the Ministry of Industry and Information Technology /MIIT, the Ministry of Public Security/MPS and the National Radio and Television Administration).

In addition, National Technical Committee 260 on Cybersecurity of SAC ("TC260") plays a pivotal role in organising and executing technical standardisation efforts related to domestic information security matters, and formulates technical standards across an array of domains, including network security technology, security mechanisms, security services, security management and security assessments.

## Definitions

The PRC does not yet have an omnibus AI regulation – instead, the PRC has adopted a sector driven approach. That said, there are relevant definitions under specific laws and regulations.

Under the GenAI Measures:

- "Generative AI technology" refers to "*models and related technologies that have the ability to generate texts, images, audios, videos or other content.*"
- "Generative AI service provider" refers to "*any organisation or individual that uses generative AI technology to provide generative AI services (including providing such services through providing programming interfaces or other means).*"
- "Generative AI service user" refers to "*any organisation or individual who uses generative AI services to generate content.*"

Under the Deep Synthesis Provisions:

- "Deep synthesis technology" refers to "*any technology that employs deep learning, virtual reality or any other generative or synthetic algorithm to generate texts, images, audio, video, virtual scenes or other network information.*"

- "Deep Synthesis services provider" refers to *"any organisation or individual who provides deep synthesis services."*
- "Providers of technical support for deep synthesis services" refers to *"any organisation or individual who provides technical support for deep synthesis services."*
- "User of deep synthesis services" refers to *"any organisation or individual who uses deep synthesis services to generate, reproduce, release or distribute information."*
- "Training data" refers to *"labelled or benchmark datasets used for training machine learning models."*

Under the Recommendation Algorithms Provisions:

- "Application of recommendation algorithm technologies" refers to *"using algorithm technologies such as generation and synthesis technology, personalised pushing technology, ranking and selection technology, retrieval and filtering technology, and dispatching and decision-making technology to provide users with information."*

Under the AI Data Standard:

- "Pre-training" refers to *"the training process in which a generative AI model acquires general knowledge using large-scale datasets."*
- "Fine-tuning" refers to *"the training process in which a generative AI model, based on pre-training, acquires context-specific service capabilities using data from specific sources."*

## Prohibited activities

Under the GenAI Measures, any organisation or individual is prohibited from:

- using generative AI services to generate any illegal content including content that endanger national security, national sovereignty or the socialist system, etc., or content that propagates terrorism, ethnic hatred, or any violent or obscene content, or false or harmful information; and
- exploiting advantages in terms of algorithms, data, platforms (from an intellectual property perspective) to carry out monopoly or unfair competition practices.

Under the Deep Synthesis Provisions, any organisation or individual is prohibited from:

- using deep synthesis services to engage in illegal activities including those that endanger national security and public interests, disrupt economic and social order, and infringe upon the legitimate rights and interests of others, etc.;
- using deep synthesis services to produce or distribute fake news; and
- using technical means to delete, alter or conceal labels added to information generated or edited using deep synthesis services.

Under the Recommendation Algorithms Provisions, service providers are prohibited from:

- using recommendation algorithm-based services to engage in illegal activities including those that endanger national security and public interests, disrupt economic and social order, and infringe upon the legitimate rights and interests of others, etc.;
- using recommendation algorithm-based services to disseminate information prohibited by laws and administrative regulations (and there is also a positive obligation for service providers to prevent the dissemination of bad information);
- setting up algorithm models that lead users into addiction or excessive consumption, or that are illegal or against ethics and morals;
- create or produce false or misleading news content or share news from sources outside the parameters set by the government;
- use algorithms to create fake accounts, engage in illegal account trading, manipulate user accounts, or generate false likes, comments or shares;
- use algorithms to block information, make excessive recommendations, manipulate rankings in search results, control trends, or otherwise disrupt information presentation in a way that influences public opinion online or evade supervisory or regulatory oversight; and
- engage in monopolistic or unfair competitive practices by using algorithms to place unreasonable restrictions on other internet information service providers or disrupt their lawful operations.

## High-risk AI

The PRC has not yet established a formal categorisation of AI technologies based on their associated risk levels. Nevertheless, specific laws and regulations provide requirements for certain use cases and services with certain capabilities. For example:

- Each of the three pieces of regulation referred to above require providers of services with public opinion attributes or social mobilisation capabilities to perform record-filing procedures and conduct security assessments in accordance with laws.
- Under the Deep Synthesis Provisions, the generated or edited information of certain deep synthesis services that may cause confusion among the public must be labelled with regard to its deep synthesis status prominently, including:
  - smart dialogue or similar services that simulate a human to generate or edit texts;
  - speech generation services (e.g. voice synthesis or voice imitation services);
  - services that generate images or videos of people (e.g. face generation, face swapping, face manipulation or posture manipulation);
  - immersive simulated scene generation, editing or other services;
  - any other editing services that significantly alter personal identification characteristics; and
  - any other services that generate or significantly altering information content.

The same labelling obligations are also reiterated in the GenAI Measures.

## Controls on generative AI

The main regulatory requirements are set out in the 'Law/proposed law' section.

In particular, if an AI service provider intends to provide AI services to external users located in China, it may need to pass certain security assessments conducted by the Chinese authorities and complete the required filings with the Chinese authorities.

Under the AI Security Standard, as well as the standards mentioned in the “Regulatory Guidance / Voluntary Code” section, AI service providers are required to ensure the security of their services, focusing mainly on the following aspects:

- Training data security: service providers are responsible for ensuring the security of training data through effective data sources due diligence, content moderation, privacy protection and annotation process management.
- Model security: service providers should take effective measures to ensure the security of AI model throughout the entire lifecycle of the model. This includes secure model training, output control, ongoing monitoring and evaluation, updates and upgrades, and the protection of the model's operating environment.
- Operation security: service providers should implement comprehensive safeguards concerning the provision of services, the transparency of service operations, the collection of input data, the mechanisms for handling complaints and reports and the business continuity planning.

## Enforcement / fines

The relevant regulatory authorities have the power to impose penalties for violation of the certain provisions of the abovementioned provisions and measures based on the wider applicable laws and regulations of the PRC.

This said, the PRC authorities have broad powers in addition to fines which may have an impact on business activities and reputational risks, including the issuance of warnings, suspension of services or business licences, blocking and blacklisting.

## User transparency

The GenAI Measures require service providers to employ effective measures to increase the transparency in generative AI services and to improve the accuracy and reliability of generated content, based on the types and characteristics of the services.

The Deep Synthesis Provisions require deep synthesis services providers to develop and disclose their management rules and platform conventions.

The Recommendation Algorithms Provisions specify that to comply businesses must formulate and disclose the relevant principles, purposes and key operation mechanisms for recommendation algorithm-based services. Users have the right to opt out of the algorithm recommendation services or request the service provider to provide services not targeting their personal characteristics. Service providers must provide users with a convenient option to switch off the algorithmic recommendation

services. If users choose to switch off algorithmic recommendation services, the algorithmic recommendation service provider must immediately cease providing the services.

Under the AIGC Labelling Measures, AI-generated content shall be marked with explicit labels and/or implicit labels, depending on the functionality of the underlying AI services and how the AI-generated content can be used:

- "Explicit labels" refer to *"visible indicators—such as text, audio, or graphics—added to the AI-generated content or interactive interface, which can be clearly perceived by users."*
- "Implicit labels" refer to *"technical markers embedded in the data of AI-generated content files, which are not easily perceived by users."*

Implicit labels should be embedded in the metadata of generated content files. Explicit labels should be added to AI-generated dialogue simulating natural human interaction, synthetic voices significantly altering personal characteristics, human face images generated or altered by AI, and immersive scenes, as well as other high-risk use cases.

## Fairness / unlawful bias

The GenAI Measures require that measures be taken to prevent discrimination on the basis of race, ethnicity, beliefs, nationality, region, gender, age, occupation, etc. in the process of algorithm design, training data selection, model generation and optimisation and provision of services. Further, the lawful rights and interests of others (including rights to likeness, reputation, honour, personal privacy and personal information) must also be respected.

Under the Recommendation Algorithms Provisions, service providers have a responsibility to safeguard specific protected groups, including minors and the elderly, by providing appropriate services that are in line with such groups' characteristics. Where a recommendation algorithm-based service is deployed in an employee work dispatching use case, they must also ensure workers' rights to compensation, rest and leave. Consumers' right to fair trading must also be protected where a service is deployed to provide goods or services to consumers.

## Human oversight

The Recommendation Algorithms Provisions specify that to comply, businesses must (amongst other things) establish and improve relevant management systems and technical measures (including for algorithm mechanism review) and employ professional staff and technical support that is appropriate to the scale of the algorithm recommendation service.

## Key contacts



**Lauren Hurcombe**  
Partner  
Global Co-Chair of  
Technology & Sourcing  
Group  
DLA Piper  
[lauren.hurcombe@dlapiper.com](mailto:lauren.hurcombe@dlapiper.com)  
[View bio](#)



**Carolyn Bigg**  
Partner  
Global Co-Chair Data,  
Privacy and Cybersecurity  
Group  
DLA Piper  
[carolyn.bigg@dlapiper.com](mailto:carolyn.bigg@dlapiper.com)  
[View bio](#)



**Amanda Ge**  
Of Counsel  
DLA Piper  
[amanda.ge@dlapiper.com](mailto:amanda.ge@dlapiper.com)  
[View bio](#)

## For more information

---

To learn more about DLA Piper, visit [dlapiper.com](https://dlapiper.com) or contact:



### Gareth Stokes

Partner

Global Co-Chair, AI Practice

[gareth.stokes@dlapiper.com](mailto:gareth.stokes@dlapiper.com)

[Full bio](#)



### Jeanne Dautier

Partner

Global Co-Chair, AI Practice

[jeanne.dautier@dlapiper.com](mailto:jeanne.dautier@dlapiper.com)

[Full bio](#)



### Danny Tobey

Partner

Global Co-Chair AI and Data Analytics

[danny.tobey@us.dlapiper.com](mailto:danny.tobey@us.dlapiper.com)

[Full bio](#)

## About us

---

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

[dlapiper.com](https://dlapiper.com)