

What To Know About China's New AI Regulations

By **Peter Schildkraut and Hazel Zhang** (April 19, 2023)

When it comes to regulation of artificial intelligence, the Western world has focused on the European Union's consideration[1] of the proposed Artificial Intelligence Act, the Biden administration's Blueprint for an AI Bill of Rights,[2] enforcement efforts by multiple U.S. federal agencies, and various U.S. state and local laws.[3]

What the Western press has not noticed as much is that China has steadily increased the ways in which it regulates these fascinating new technologies.

To be sure, China's National People's Congress Standing Committee has not adopted a law comprehensively regulating AI. However, the Personal Information Protection Law, Cybersecurity Law,[4] and Data Security Law[5] each address certain aspects of developing, providing, deploying and using AI systems.

Even without a comprehensive law, national regulators and local governments in China have pressed forward. Building on its Internet Information Service Algorithmic Recommendation Management Provisions[6] from a year ago,[7] the Cyberspace Administration of China has doubled down with its Internet Information Service Deep Synthesis Management Provisions.[8]

In addition, the Shenzhen Special Economic Zone and Shanghai have adopted their own policies: Regulations for the Promotion of the Artificial Intelligence Industry in Shenzhen Special Economic Zone,[9] and Regulations for the Promotion of the Development of the Artificial Intelligence Industry in Shanghai Municipality.[10]

All of these measures are now in force, and companies offering AI-enabled products or services in China should take note.

The Measures Vary in Scope

The Cyberspace Administration of China's administrative provisions only apply to different, but somewhat overlapping, sets of AI applications.

The new Deep Synthesis Management Provisions govern generative AI — algorithms to create text, images, audio, video, virtual scenes or other information.[11]

Last year's Algorithmic Recommendation Management Provisions have a wider reach. They apply to algorithms that create content, make personalized recommendations, rank or select information, search or filter content, dispatch service providers, or otherwise provide information to users.[12]

The Shanghai regulations and Shenzhen regulations apply broadly to AI and have similar definitions of the term.

The Shanghai Regulations define AI as:



Peter Schildkraut



Hazel Zhang

the theories, methods, technologies, and application systems for using computers or computer-controlled machines to simulate, extend, and expand human intelligence, perceive the environments, acquire knowledge, and use knowledge to obtain the best results." [13]

The Shenzhen regulations define AI as:

the use of computers or computer-controlled devices, through the perception of environments, acquisition of knowledge, deductions, or other methods, to simulate, extend, and expand human intelligence. [14]

Both definitions echo the one in China's Artificial Intelligence Standardization White Paper (2018 Edition): [15]

[The] theories, methods, technologies, and application systems for using digital computers or digital computer-controlled machines to simulate, extend, and expand human intelligence, perceive the environments, acquire knowledge, and use knowledge to obtain the best results. [16]

These definitions generally align with how the Organization for Economic Cooperation and Development [17] and G20 [18] commonly define an AI system:

a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives.

They may be even closer to the definition used by the United Nations Educational, Scientific and Cultural Organization: [19]

systems which have the capacity to process data and information in a way that resembles intelligent behaviour, and typically includes aspects of reasoning, learning, perception, prediction, planning or control.

While all these definitions are similar, their multiplicity highlights that there is no single commonly accepted definition of AI either within countries or internationally. On the margins, the distinctions can matter in determining the legal requirements a particular technology must observe.

The Deep Synthesis Management Provisions

Generative AI systems have raised concerns about deception. Students and others may try to pass off AI-created content as their own. Political opponents, domestic or international, may offer convincing audio or visual "recordings" of leaders or candidates saying or doing things that never happened.

Jilted lovers or blackmailers may create realistic-looking, but utterly fake, pornographic videos or images to compromise their targets. Scammers may use AI-created instructions or pleas [20] appearing to come from trusted individuals to separate victims from their money. And so on.

The Deep Synthesis Management Provisions address these concerns. Among other requirements:

- Fake news is prohibited;[21]
- Providers must verify the real identity information of their users;[22]
- Providers must monitor for illegal or negative information;[23]
- Providers must have convenient portals for user appeals, public complaints, and reports and published processes, including time limits, for resolution;[24]
- App stores and other distribution platforms must review deep synthesis services for safety and address legal violations with warnings, suspensions, or blocking or removal from their platforms;[25]
- Services that enable "editing of biometric information such as faces or voices" must prompt users of those features to notify and obtain consent from their subjects;[26]
- Security assessments are required for services that generate or edit biometric information or "special items, scenarios, or other non-biometric information that might involve national security, the nation's image, national interests, and the societal public interest";[27]
- Generated content must have a technical, but nonobtrusive, indication that it is generated, and users must be able to add prominent labels;[28]
- Noticeable marks indicating the content has been generated must be placed conspicuously on:
 - Text simulated as coming from natural persons;
 - Generated speech;
 - Generated "images or video of virtual persons such as face generation, face swapping, face manipulation, gesture manipulation, or editing services that significantly change personal identification characteristics";

- Simulated immersive realistic scenes; and
- Other services that have functions that generate or significantly alter information content";[29]
- Providers "shall comply with laws and regulations, respect social mores and ethics, and adhere to the correct political direction, public opinion orientation, and values trends, to promote progress and improvement in deep synthesis services;"[30] and
- Providers of services "that have public opinion properties or the capacity for social mobilization" have enhanced filing obligations.[31]

The Shanghai and Shenzhen Regulations

The Shanghai regulations and Shenzhen regulations provide frameworks for the tiered governance of AI while leaving many of the details to be fleshed out later by the municipal governments.

Prior nonbinding guidance from central government technical committees such as the Cybersecurity Standard Practice Guidance - AI Ethical Security Risk Prevention Guidelines, Ethical Norms for New Generation Artificial Intelligence,[32] and the Opinion on Strengthening the Ethics and Governance in Science and Technology[33] are likely to inform how the municipal governments fill in these details.

Consistent with OECD and G20 principles, both frameworks adopt a risk-based approach, with more extensive scrutiny of high-risk AI products and services than of those presenting less risk. However, it remains to be seen what categories of products and services will be classified as high-risk.

It appears that high-risk products and services will have to undergo compliance reviews before being placed into the market. Medium- and low-risk products and services instead will require a premarket disclosure coupled with monitoring of the AI system's performance in the market.

In addition, both regulations contemplate some additional flexibility for medium- and low-risk products and services.

Shanghai's provides for some sort of pilot program[34] while Shenzhen will allow early use of low-risk systems for which the state and local standards have not been developed, provided they meet advanced international standards and do not raise concerns for national security, public interest, and the personal safety of citizens.[35] Details of the pilot program and early-use process await further development.

Under both the Shanghai regulations and Shenzhen regulations, parties must follow relevant laws, regulations, and ethical requirements. Moreover, they must not provide products and services that:

- Endanger national security or social public interest;

- Infringe upon personal privacy or rights and interests of personal information;
- Discriminate against users on the basis of race, gender, ethnicity, and religious beliefs, and other factors;
- Use deep synthesis technology to engage in prohibited acts; or
- Use algorithmic technologies to carry out price discrimination or consumer fraud, or other acts that infringe upon the rights and interests of consumers.[36]

The Shenzhen regulations also prohibit parties from providing products and services that endanger physical and mental health and other acts in violation of ethical security norms.[37]

Somewhat similarly, the Shanghai regulations prevent parties from providing products and services that endanger the personal or property safety of users and other acts that violate public order and good morals.[38]

Shanghai will explore the establishment of a negative checklist to prohibit or restrict certain types of AI research, applications and other activities.[39]

Measures on the Administration of Generative Artificial Intelligence Services

Additionally, on April 11, the Cyberspace Administration of China released draft Measures on the Administration of Generative Artificial Intelligence Services.[40] Public comments on the draft are being accepted through May 10, 2023.

If adopted as drafted, the Generative AI Measures would overlap substantially with the Algorithmic Recommendation Management Provisions and the Deep Synthesis Management Provisions. But they would fill some gaps as well. For instance, the Generative AI Measures:

- Seem to extend to offline as well as online generative AI technology while the two earlier provisions apply only to internet information services;
- Would mandate steps to prevent algorithmic discrimination based on various characteristics and prohibit discriminatory content generation; and

- Would clarify how certain privacy and intellectual property protections apply to generative AI, e.g., training data must not contain (1) content infringing on IP rights or (2) personal information without the subject's consent, or it shall comply with other situations provided by laws and administrative regulations; and
- Would require security assessment declarations to be submitted to the State Internet Information Services before services enabled by generative AI are offered publicly.

Although the Generative AI Measures' final form remains to be seen, the Cyberspace Administration of China's proposal of them reinforces the Chinese government's determination to move swiftly toward comprehensive regulation of AI.

Conclusions

China has moved ahead of the EU, the U.S. and other jurisdictions in regulating AI.

Companies offering AI-enabled products and services in China need to consider carefully whether their products and services comply with these new requirements. And they should stay tuned for further developments in this fast-moving field.

Peter Schildkraut is senior counsel and co-leader of the technology, media and telecommunications industry team at Arnold & Porter.

Hazel Zhang is a former associate at the firm.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] <https://www.arnoldporter.com/en/perspectives/advisories/2023/01/europe-ai-act-moves-forward>.

[2] <https://www.arnoldporter.com/en/perspectives/advisories/2022/10/the-blueprint-for-an-ai-bill-of-rights>.

[3] <https://www.arnoldporter.com/-/media/files/perspectives/publications/2022/10/preparing-your-ai-regulatory-compliance-program-fo.pdf?rev=dcd16a421aaf4801bb464242d5751295>.

[4] <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>.

[5] <https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/>.

[6] <https://digichina.stanford.edu/work/translation-internet-information-service->

algorithmic-recommendation-management-provisions-effective-march-1-2022/.

[7] <https://www.arnoldporter.com/en/perspectives/publications/2022/03/have-your-websites-online-services-unlawful>.

[8] <https://www.chinalawtranslate.com/en/deep-synthesis/>. Original Chinese here.

[9] <https://cset.georgetown.edu/publication/regulations-for-the-promotion-of-the-artificial-intelligence-industry-in-shenzhen-special-economic-zone/>. Original Chinese here.

[10] <https://cset.georgetown.edu/publication/regulations-for-the-promotion-of-the-development-of-the-artificial-intelligence-industry-in-shanghai-municipality/>. Original Chinese here.

[11] See Article 23 of the Deep Synthesis Management Provisions.

[12] See Article 2 of the Algorithmic Recommendation Management Provisions.

[13] See Article 2 of the Shanghai Regulations.

[14] See Article 2 of the Shenzhen Regulations.

[15] <https://cset.georgetown.edu/publication/artificial-intelligence-standardization-white-paper/>. Original Chinese here.

[16] See Section 2.1.2 of the Artificial Intelligence Standardization White Paper (2018 Edition).

[17] <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

[18] <https://www.mofa.go.jp/files/000486596.pdf>.

[19] <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.

[20] https://www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/?utm_campaign=wp_the_technology_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_technology202.

[21] Article 6.

[22] Article 9.

[23] Article 10.

[24] Article 12.

[25] Article 13.

[26] Article 14.

[27] Article 15.

[28] Article 16.

[29] Article 17.

[30] Article 4.

[31] Article 19.

[32] <https://www.tc260.org.cn/upload/2021-01-05/1609818449720076535.pdf>. Original Chinese here.

[33] <https://ai-ethics-and-governance.institute/2022/03/22/china-released-opinion-on-strengthening-the-ethics-and-governance-in-science-and-technology/>. Original Chinese here.

[34] Article 65.

[35] Article 44.

[36] Article 72 of the Shenzhen Regulations and Article 67 of the Shanghai Regulations.

[37] Article 72.

[38] Article 67.

[39] See Article 9 of the Shanghai Regulations.

[40] <https://www.google.com/url?q=https://www.chinalawtranslate.com/en/gen-ai-draft/&sa=D&source=docs&ust=1681927083151543&usg=AOvVaw3Bi5EKMomxiYPuLFxZBfF5>. Original Chinese here.