A Comprehensive Guide to the AIGC Measures Issued by the CAC

Peng Cai

1. INTRODUCTION

With the rapid advancement of artificial intelligence technology, promoting its healthy development and standardization has become more crucial than ever. This is especially true given the trend of artificial intelligence-generated content (**AIGC**) triggered by ChatGPT. As a result, regulatory authorities in major countries are closely monitoring generative AI and enforcing appropriate regulations. In China, the Cyberspace Administration of China (**CAC**) issued the *Measures for the Management of Generative Artificial Intelligence Services (Draft for Comment)* (the "**AIGC Measures**") on April 11, 2023, which aims to provide clearer guidance for China's AI and algorithm-related industries in terms of the current regulatory landscape. This article will provide a comprehensive analysis of the AIGC Measures to enhance readers' understanding of its significance.

2. BASIC APPROACH AND PRINCIPLES OF THE AIGC MEASURES

(1) Bolstering AIGC Development: The Legal Framework and Application Scope of the AIGC Measures

The AIGC Measures is based on three pillar data laws in China, namely the *Cybersecurity Law* (**CSL**), the *Data Security Law* (**DSL**), and the *Personal Information Protection Law* (**PIPL**). These superior laws, combined with the AIGC Measures, the *Internet Information Service Algorithmic Recommendation Management Provisions* (the "**Algorithm Provisions**"), the *Internet Information Service Deep Synthesis Management Provisions* (the "**Deep Synthesis Provisions**"), and the upcoming *Measures for Ethical Review of Science and Technology (Trial)*, form the primary legal foundation and regulatory framework for ensuring compliance in the AIGC industry.

The AIGC Measures defines generative artificial intelligence as technology that creates content

based on algorithms, models, and rules. Its scope regarding AIGC is broader than that of the Deep Synthesis Provisions. AIGC companies targeting the public in the People's Republic of China (**PRC**), regardless of their physical locations, are subject to regulatory supervision. ChatGPT's recent move of shutting down user accounts from the PRC can be considered a precautionary measure to avoid being subject to the laws and regulations of the PRC. The AIGC Measures may also regulate AIGC products that aim at specific targets, which means that even if an AIGC product is not directly targeted at the public, but at specific domestic enterprise users or custom-designed products, it may still be subject to the AIGC Measures.

The AIGC Measures stresses the importance of prioritizing the use of secure and trustworthy software products, tools, computing, and data resources. It is worth noting that using secure and trustworthy network products and services is mandatory under the PRC laws and regulations for critical information infrastructure operators and important data processors. Detailed guidelines or referential standards remain to be introduced to assess the security and trustworthiness of network products and services in the future.

(2) Primary Principles of the AIGC Measures

The AIGC Measures sets out five primary principles: adherence to the core values of socialism, prohibition of algorithmic discrimination, prohibition of unfair competition, prevention of false information, and non-infringement of others' legitimate interests. It is worth emphasizing that certain principles hold significant value and merit highlighting:

(a) Prohibition of algorithmic discrimination. The prohibition of algorithmic discrimination is a key aspect of algorithm compliance under the current E-Commerce Law. The AIGC Measures extends the prohibition of algorithmic discrimination to other aspects such as algorithm design, training data selection, model generation and optimization, and service provision.

(b) Prohibition of unfair competition. The Anti-Unfair Competition Law, Anti-Monopoly Litigation Interpretation, and four supporting anti-monopoly-related regulations regulated the use of data, algorithms, and platform advantages for unfair competition or monopolistic behavior. The AIGC Measures also addresses these issues, reflecting a response to similar compliance issues concerning algorithms.

(c) Prevention of false information. The AIGC Measures demands that content generated by AI must be accurate and truthful, and Service Providers (defined hereunder in first paragraph of Article 3) must take steps to prevent the creation of false information. However, what constitutes "false information" is still unclear. Some AI-generated content, such as synthetic articles, synthetic pictures, and deep fake videos, are not inherently authentic, and requiring such content to be completely accurate may contradict the original purposes for which the relevant technologies were created. Considering that AI technology is still in its early stage, it can be a huge challenge for Service Providers to ensure 100% accuracy of AI-generated content.

(d) Non-infringement of others' legitimate interests. AIGC poses the risk of violating individuals' legitimate rights and interests, such as portrait rights, reputation rights, and rights to privacy. In addition, the demand for data processing that arises from algorithms training often leads companies to use data from the internet, which may entail the infringement of intellectual property, trade secrets or data ownership of others. Correspondingly, the AIGC Measures sets out the principle of non-infringement of privacy and intellectual property.

3. OBLIGATIONS OF SERVICE PROVIDERS

Article 5 of the AIGC Measures defines Service Providers as individuals and organizations that use AIGC products to provide services such as chat, text, image, and sound generation. This also includes entities that provide programmable API interfaces to support others in generating related content, but excludes AIGC end-users. It is noteworthy that Service Providers are deemed as *de facto* personal information processors under the AIGC Measures, where Service

Providers shall, per the PIPL, determine the purpose and method of processing personal information independently or jointly with their users when providing AIGC services. However, this is not always the case. When Service Providers only provide API interfaces, they may neither determine the purposes nor the methods. Therefore, in this case, Service Providers are more of " entrusted parties" rather than "personal information processors". Regardless, the main body of the AIGC Measures focuses on the extensive obligations of Service Providers, which will be introduced and analyzed as follows:

(1) Obligations of Security Assessment and Algorithm Filing

The AIGC Measures requires that Service Providers conduct security assessments in accordance with the *Provisions on the Security Assessment of Internet Information Services with Public Opinion Properties or Social Mobilization Capacity* (the "**Security Assessment Provisions**") and fulfill algorithm filing obligations in accordance with the *Internet Information Service Algorithmic Recommendation Management Provisions* (the "**Algorithm Management Provisions**"). While the Security Assessment Provisions and Algorithm Management Provisions limit the scope of such assessments and filings to internet information services that feature public opinions or social mobilization, regulatory authorities actually determine whether certain services fall within the scope based on the potential rather than actual effects. Therefore, generative AIGC product providers are advised to complete the security assessment and algorithm filings since most AIGC products may affect public opinions or mobilize the society. It remains unclear whether downstream Service Providers must repeat the filings if upstream Service Providers have already filed.

(2) Obligations to Ensure the Legality of the Source of Training Data

The AIGC Measures requires Service Providers to ensure the legality of training data from various aspects, including complying with laws and regulations, not infringing intellectual property rights, obtaining a legal basis for processing personal information, ensuring authenticity, accuracy, objectivity, and diversity, and meeting other regulatory requirements. Given that the issue of the source data's legality is a risk inherent to algorithmic training, the

AIGC Measures' requirements for Service Providers to ensure such legality may indicate enhanced regulatory oversight over data sources in the future. Furthermore, ensuring objectivity and diversity of data is crucial to preventing algorithmic discrimination and information silos. However, it remains unclear whether the AIGC Measures applies authenticity and accuracy requirements solely to source data or to artificially created products (data) as well.

(3) Obligations of Including Annotations and Marks

The AIGC Measures imposes two distinct obligations: the obligation of including annotations in Article 8 and the obligation of including marks in Article 16. Article 8 requires Service Providers to accurately and consistently annotate training data to assist in the learning and training of algorithms. To achieve this, the AIGC Measures requires Service Providers to establish clear, specific, and operable annotation rules and provide training for annotators. It is essential to note that accurate annotation is crucial to meeting the accuracy requirement for trained algorithm models as stipulated in Article 4 of the AIGC Measures. Article 16 requires Service Providers to comply with the obligations of making marks as outlined in the Deep Synthesis Provisions. Requirements for two types of marks are laid out in the Deep Synthesis Provisions: traceability marks and significant marks. Traceability marks apply to all generated content, while significant marks are only required where the content may confuse or mislead the public. In terms of the obligation of including marks, the AIGC Measures goes further beyond the Deep Synthesis Provisions, mandating that the AIGC Service Providers must apply significant marks, regardless of the possibility of causing confusion or misleading.

(4) Obligations to Verify the Real Identity of End-Users.

The AIGC Measures requires Service Providers to authenticate the identity information of end-users in accordance with the CSL. "Real-name authentication on the backend and voluntary participation on the frontend" has become a standard requirement for nearly all online services. Based on the similar requirements for real-name authentications under the Deep Synthesis Provisions, the AIGC Measures may require Service Providers to collect the following

information for real-name authentication: mobile phone numbers, identity card numbers, unified social credit codes, and so forth.

(5) Obligations to Prevent Excessive Reliance or Addiction

Article 10 of the AIGC Measures requires Service Providers to take steps to prevent users from becoming overly reliant on or addicted to generated content. To safeguard users' rights, the AIGC Measures requires that Service Providers clarify and disclose the users, occasions and purposes their services are intended for. However, compliance obligations, user protection, and ethical standards may differ across various business scenarios and necessitate further refinement. Service Providers can implement measures like pop-up reminders or limits on frequency and duration of use to avert addiction. Regular evaluation of the algorithm mechanisms, models, data, and application results is essential to ensuring ethical compliance. The AIGC industry may in the future introduce regulatory campaigns such as "Minor Protection" campaigns to prevent addiction.

(6) Obligations to Limit the Use of Personal Information

The AIGC Measures requires Service Providers to safeguard users' input information and usage records, not to retain any illegal input information that may reveal their identity, not to create user profiles based on input information or usage, and not to disclose user input information to third parties. However, in contrast to superior laws such as the PIPL and E-commerce Law, the AIGC Measures does not impose additional obligations on Service Providers as personal information processors. Having said that, Service Providers should still obtain separate consent or other legal basis for special personal information processing activities such as user profiling in accordance with the PIPL.

(7) Obligations to Prohibit the Generation of Discriminatory Content

The AIGC Measures requires Service Providers to prevent generating discriminatory content based on a user's race, national origin, gender, and other factors. Under this obligation, Service Providers shall take measures such as preventing discrimination in algorithm design, training

data selection, model generation and optimization, and service provision. Service Providers must also monitor their products to ensure that they do not generate discriminatory content. Violations of these obligations can lead to accountability under the AIGC Measures. However, a complete prohibition on generating content with any hint of discriminatory nature could limit the ability to depict antagonists in the generated novels and scripts, potentially compromising the free application and convenience of AIGC services.

(8) Obligations to Properly Handle User Complaints and Infringing Content

Article 13 of the AIGC Measures incorporates rules from the PIPL regarding individuals' exercise of their rights and explicitly requires Service Providers to establish a mechanism for receiving and handling user complaints and timely dealing with requests to correct, delete, or block their personal information. The second half of Article 13 also requires Service Providers to prevent ongoing harm when generated content infringes upon the rights or interests of others, such as rights of privacy, image, reputation, or trade secrets, or stop other unlawful circumstances from occurring. It is essential to note that Service Providers should take necessary measures to stop infringing or unlawful content during the generation phase and promptly delete, block, or disconnect links, or even terminate services if necessary. Therefore, Service Providers must bear a higher duty of care and implement a monitoring and auditing mechanism during the content generation phase to the extent that it is reasonable and technically feasible.

(9) Obligation to Ensure the Stability of the Service

The AIGC Measures requires Service Providers to ensure the stability of the lifecycle of their generative AI services, where "lifecycle" refers to the period of existence of such services. However, per our observation, only a limited number of AIGC products in the current market are capable of providing "stable services". Further clarification by regulatory authorities is necessary to interpret this requirement, as ambiguity may give rise to lawsuits between users and Service Providers in the future.

(10) Obligations to Optimize the Algorithm Model

The AIGC Measures requires that Service Providers prevent the generation of inappropriate content by implementing content filtering measures, including removing sensitive words and other unsuitable content. In response to user reports and observations to prevent the re-generation of unsuitable content, Service Providers shall also optimize and train algorithm models within three months after discovering inappropriate content or receiving users' compliant. The obligation concerning algorithm training and optimization aims to enhance content control by supplementing content filtering and other measures. However, Service Providers are now obligated under the AIGC Measure to address the "weak links" of artificial intelligence within three months, which is undoubtedly a high standard of obligation for AIGC Service Providers both technically and practically. Relying on user reports as the trigger for algorithm optimization and re-training may impose significant cost burdens for Service Providers.

(11) Obligations to Disclose and Educate

The AIGC Measures requires Service Providers to disclose necessary information, including the source of pre-training and optimization training data, according to the requirements of the CAC and other competent authorities. Service Providers must also educate users to understand and use the generated content rationally.

This obligation mandates administrative authorities to proactively intervene in the technical development of companies based on their information disclosure obligations. It represents a shift from previous passive regulatory approaches, as the CAC and other competent authorities have the administrative power to obtain more information about the development of artificial intelligence systems from Service Providers. However, boundary between protecting a company's trade secrets and fulfilling information disclosure obligations remains to be clarified.

Regarding the obligation to educate users, Service Providers may incorporate relevant educational content into platform rules, privacy policies, or promotional pamphlets.

(12) Obligations to Uphold Social Morality

The AIGC Measures prohibits using AIGC products for illegal or unethical activities such as online hype, malicious posting and commenting, spamming, writing malicious software, and improper business marketing, and emphasizes Service Providers' obligation to monitor such behavior actively. However, there may be challenges in accurately identifying illegal or unethical behavior and balancing user privacy with regulatory needs. These issues require collective efforts from all stakeholders to address.

4. PENALTIES AND EFFECTIVE DATE

The AIGC Measures imposes penalties based on the CSL, DSL, and PIPL and provides the CAC and other competent authorities with discretionary power to impose penalties in the absence of clear provisions in superior laws. Severe violations may result in suspension or termination of AIGC services licenses and even criminal charges. These penalties carry a strong deterrent effect. The AIGC Measures is set to take effect in 2023, and its official issuance is expected to happen soon given the industry's current state.

5. CONCLUSION

The AIGC Measures provides new guidance for developing algorithm-related industries in China. However, some details need to be clarified by lawmakers. The AIGC Measures imposes high compliance obligations on AIGC Service Providers, raising the question of how to balance regulation with industry development. It's recommended that AI companies provide practical recommendations and feedbacks for lawmakers during the public comments period to promote the effective implementation of the AIGC Measures.