Research on Data Risks and Regulations of Generative Artificial Intelligence

Xinxin Li

Hangzhou Normal University, Hangzhou 310000, Zhejiang, China

Abstract: ***With the disruptive development of generative artificial intelligence technology, the industrial structure has been optimized and upgraded, but it has also brought many data security risks in various stages of the application of artificial intelligence technology. There have been academic discussions both domestically and internationally on the regulation of risks related to artificial intelligence, in order to address a series of challenges such as data security and privacy protection caused by generative artificial intelligence. In order to address the above-mentioned risks and challenges, at present, China's governance of generative artificial intelligence should adhere to the principle of parallel risk prevention and research and development, follow basic ethical and moral principles, formulate specialized legal documents, build a unified regulatory system, establish autonomous mechanisms and other means to enrich the preventive and regulatory measures for generative artificial intelligence, in order to better respond to risks and challenges, and promote the coordinated and healthy development of generative artificial intelligence.***

Keywords: Generative artificial intelligence; Risk; Risk regulation.

1. PROBLEM POSING

Generative Artificial Intelligence, represented by ChatGPT, can simulate and generate content similar to that created by humans, such as images, audio, text, etc. The core of these generative artificial intelligence models is the ability to understand data and tasks, which can continuously interact in context based on feedback from human communication during the process of dialogue and communication with people. Some generative artificial intelligence can also complete creative tasks such as video editing. Generative artificial intelligence collects big datasets, and its content generation capabilities will continue to improve. At present, large language models represented by ChatGPT have reached or exceeded human level in text generation tasks such as answering questions, providing suggestions, summarizing, and optimizing text.

Generative artificial intelligence, on the one hand, accelerates its integration with human society with its powerful interactivity and intelligent generativity. On the other hand, there are many drawbacks such as data breaches and the proliferation of false information, which have given rise to many risks and problems. The response of countries to the legal and institutional response to generative artificial intelligence is gradually shifting from the issues of "substitution" and "assistance" to the issue of "risk". In the early stages of generative artificial intelligence, legal researchers focused on exploring whether generative artificial intelligence could replace humans and whether it could perfectly complete the tasks assigned by humans. In the research stage of the "risk" issue, the focus should be on how the law can prevent and regulate risks in the face of the risks arising from generative artificial intelligence, so that artificial intelligence can better promote the development of human society rather than replacing or even threatening humanity. Yuan [1] developed transformer-based techniques for processing medical texts in legal documents, showcasing AI's potential in interdisciplinary document analysis. The e-commerce sector has benefited from Song's [2] work integrating AIGC with human-computer interaction design to enhance content generation quality and efficiency. Industrial IoT systems have seen notable advancements through Wu's [3] development of an intelligent gateway platform utilizing Jenkins cluster management under cloud-edge architecture, highlighting the growing importance of distributed computing in industrial applications. Urban intelligence has been enhanced by Chen [4] through geospatial neural networks that leverage location data for smart city optimization. Computer vision has achieved remarkable breakthroughs with Peng et al. [5] proposing a dual-augmentor framework for domain generalization in 3D human pose estimation. Their subsequent work on 3D vision-language Gaussian splatting [6] further advances the field by enabling more robust scene understanding and object representation.

2. RISKS AND CHALLENGES BROUGHT BY GENERATIVE ARTIFICIAL INTELLIGENCE

2.1 Data Security Risks

Firstly, there are risks associated with generative artificial intelligence in the preparation phase of data collection and annotation [4]. The basic logic of the operation of generative artificial intelligence is that AI users use AI technology to automatically generate personalized content through algorithms such as machine learning and natural language processing. If the training data sources are uneven, there may be bias in the annotated data, and generative artificial intelligence algorithms may learn from human bias, ultimately compromising the accuracy of generative artificial intelligence [5]. For example, 96% of ChatGPT's training dataset comes from English text, which may cause potential ideological bias during instruction processing. In addition, generative artificial intelligence may generate a large amount of false information during operation and use. Generative artificial intelligence can automatically generate personalized content based on users, with lower cost and higher quality. However, driven by market demand, most of the current generative artificial intelligence models are chat based human-computer interaction models, allowing users to send instructions in a convenient form and generate corresponding information in order to expand the user base and achieve maximum profitability. This type of information often takes meeting users' personalized needs as the starting point, with matching priority over accuracy, which may lead to difficulties in distinguishing authenticity. In addition, cases of using generative artificial intelligence to fabricate false information for personal gain also frequently occur.

2.2 Privacy, Security, and Compliance Issues

Generative artificial intelligence can violate personal privacy during the data collection phase. Generative artificial intelligence may collect a large amount of data information in the early stages of training, some of which may even be without the consent of individual users, causing privacy issues. For example, on a wide range of information dissemination platforms, the information published on WeChat official account is a mixture of good and bad, and there will be information formed by the use of generative artificial intelligence. Such information is used without the consent of others, making personal information difficult to be protected, which may cause serious infringement. There is a risk of privacy leakage in the interactive use of generative artificial intelligence [7]. Taking "ERNIE Bot" and "Tongyi Qianwen" as examples, when registering for use at the initial stage, it is required to collect the user's personal information in advance. It is difficult to use the application if the user disagrees. In addition, in the formal use stage, the personal information entered by the user is also inadvertently collected and used, and the above behaviors will not be clearly notified to the user.

3. PRELIMINARY SPECIFICATIONS FOR GENERATIVE ARTIFICIAL INTELLIGENCE

Generative artificial intelligence not only brings new opportunities and development prospects, but also breeds many risks and problems. Relevant departments at home and abroad attach great importance to supervision and have taken a series of measures for this purpose.

3.1 Relevant foreign regulations

In response to the risks and challenges posed by generative artificial intelligence, the European Union has actively responded and made a series of legislative explorations on artificial intelligence. The European Commission released a legislative proposal on the development of uniform rules for artificial intelligence in April 2021. After multiple discussions, the AI Act was finally passed, which set up specialized regulations for generative artificial intelligence, including a ban on facial recognition and new transparency requirements.

The US Department of Commerce focuses on development guidance and emphasizes open management of artificial intelligence, allowing enterprises and markets to take the lead in the development of artificial intelligence. For specific risk control, the US has released the "Artificial Intelligence Bill of Rights Blueprint" and formulated the "Artificial Intelligence Risk Management Framework". In April of the same year, it released a draft of the "Artificial Intelligence Accountability Policy" for soliciting opinions on regulatory issues related to artificial intelligence (such as ChatGPT).

The Canadian federal government first collected opinions on generative artificial intelligence, calling on some stakeholders to provide technical evidence on copyright issues related to generative AI. The Canadian government believes that humans can contribute sufficient skills and judgment in works created with the help of artificial intelligence technology, and thus be considered the authors of such works. It is necessary to further regulate the copyright issues of AI generated works, and further legislation can clarify the priority ownership of AI generated works or AI assisted works by rethinking how to define authors, even without relying on their identity.

3.2 Relevant regulations in China

In recent years, under the requirement of developing new quality productive forces, China has actively conducted research on the rule of law. In the field of artificial intelligence, it is mainly led by programmatic documents, forming a comprehensive governance system from multiple perspectives and aspects. It has a significant voice in the legislation of generative artificial intelligence.

On the one hand, China has successively issued the Guiding Opinions on Strengthening the Comprehensive Governance of Internet Information Service Algorithms, which clarifies that the goal of our algorithm governance is to establish a comprehensive governance pattern of algorithm security with sound governance mechanism, perfect regulatory system, and standardized algorithm ecology; The Opinion on Strengthening Ethical Governance of Science and Technology proposes the requirement of ethics first governance; And documents promoting the development of artificial intelligence applications, such as the "New Generation Artificial Intelligence Development Plan" and the "Guiding Opinions on Accelerating Scene Innovation to Promote High Quality Economic Development through High Level Application of Artificial Intelligence".

On the other hand, the Civil Code of the People's Republic of China serves as a general principle; The Data Security Law clarifies the principles of algorithm governance, requiring technology to promote economic and social development, and comply with social ethics and morality; The Personal Information Protection Law requires increased protection of personal information. In addition, the Administrative Provisions on the Recommendation of Algorithms for Internet Information Services jointly issued by other departments focuses on the governance of algorithm discriminatory decisions represented by "big data killing"; The Interim Measures for the Management of Generative Artificial Intelligence Services focus on the standardized development of generative artificial intelligence [11]. It is particularly pointed out that the Interim Measures for the Management of Generative Artificial Intelligence Services are a comprehensive regulation. Through multiple efforts, the legal system of generative artificial intelligence is gradually improving.

3.3 Challenges of Generative Artificial Intelligence Regulations

Although China has issued a series of legal norms in the field of artificial intelligence in recent years, and is relatively leading in the legal norms of generative artificial intelligence, overall, there are still many constraints and shortcomings.

Firstly, the content of generative artificial intelligence legal norms overlaps. In the "Interim Measures", there is no classified and graded management of the legal responsibility for the provision of generative artificial intelligence, resulting in the specific responsibility of AI providers being scattered in different data processing scenarios, such as the "Cybersecurity Law" and the "Personal Information Protection Law". The "Interim Measures" themselves cannot provide precise guidance [12].

Secondly, the Interim Measures do not have specific implementation standards and legal responsibilities for the output of generative artificial intelligence. Although the document specifies certain labeling for images and videos of the process, there is no detailed implementation standard, which makes such labeling easy to avoid in reality and has weak applicability. In addition, the boundaries of rights and responsibilities of legal regulatory entities are blurred [13]. The Interim Measures are jointly issued by multiple departments, which results in each department having regulatory responsibilities. There may be a phenomenon where various departments compete to regulate or evade regulation, and this uncertain governance model is not conducive to the effective control and coordinated promotion of regulatory work in generative artificial intelligence.

Finally, a complete and unified system of responsibility has not been established. Article 9 of the Interim Measures requires providers of generative artificial intelligence to bear the responsibility of network information content producers, which is very different from the traditional binary separation of service providers and content producers in the intelligent industry. Generative artificial intelligence faces risks and hidden dangers such as excessive data collection, illegal collection, and data abuse during the operation stage. Based on the overall operation process of generative artificial intelligence, regulations cannot be separated, and a unified generative artificial intelligence data risk responsibility system needs to be established. Moreover, generative artificial intelligence does not have complete control over the generated content, which will bring new contradictions to the hierarchical management and responsibility governance of generative artificial intelligence.

In summary, the current legal content of generative artificial intelligence in China is incomplete, the responsibilities of regulatory bodies are vague, the regulatory measures are chaotic, and the legal responsibility rules are complex. It is urgent to conduct in-depth research in both theory and practice.

4. THE REGULATORY PATH OF GENERATIVE ARTIFICIAL INTELLIGENCE

At present, the legal norms for generative artificial intelligence in China are relatively comprehensive, but it is still difficult to cope with specific practical problems. We should continue to explore and improve risk prevention paths.

4.1 Improve specialized laws in the field of artificial intelligence

Given the diverse and complex nature of generative artificial intelligence, specialized laws should be established to address the risks associated with it, in order to achieve a systematic layout of legal governance in the field of artificial intelligence [15]. For some reference clauses in the original documents, they should be deleted or modified. For those that are standardized and duplicated in legal texts, they should be minimized. For those that are not clearly defined in legal texts, multiple parties should be clarified to ensure the accurate application of generative artificial intelligence. In addition, when formulating laws, it is necessary to provide a certain explanation of generative artificial intelligence, using easy to understand language to help users understand the basic logic of algorithms, potential risks of algorithms, etc., increase the transparency of generative artificial intelligence, create appeal channels for users under reasonable conditions, enrich the ways for complainants to file complaints, and enable users to timely safeguard their legitimate rights and interests.

4.2 Establish a unified generative artificial intelligence risk responsibility system

Using classification methods to reasonably define the responsible parties is an effective strategy for managing risks during the operation phase of generative artificial intelligence. At this stage, multiple stakeholders are involved, including service providers, technical researchers, data providers, and system operators. By classifying management and clarifying their respective responsibilities, the management effectiveness of generative artificial intelligence data risks can be improved. Specifically, service providers are primarily responsible for the provision of products; Technical R&D personnel are responsible for data abuse and algorithm bias; If data providers infringe upon the legitimate rights and interests of others during data collection, they shall also bear liability for infringement; If the system operator causes data leakage or other problems due to improper operation, they should also bear corresponding responsibilities. At the same time, while promoting the development of generative artificial intelligence technology, ensuring proper control of data risks and accurately distinguishing different responsible parties is crucial for holding accountable the risk responsibility of generative artificial intelligence [16].

4.3 Establishing a risk supervision mechanism for generative artificial intelligence data

At present, there is a problem of multi head management in the regulation of artificial intelligence, and there is a lack of coordination among governance institutions. Decentralized governance not only hinders the achievement of governance goals, but also hinders the efficient allocation of governance resources. Conflicts often arise between regulatory authorities, causing regulatory work to stagnate. In the current situation where multiple departments are working together to formulate regulations, it is possible to strengthen the supervision among departments through the reasonable allocation of power. Led by the Cyberspace Administration of China, ensure its ability to maintain a coordinated position in the field of artificial intelligence and provide unified guidance to various departments. Other departments have different responsibilities in different governance processes to avoid overlapping and intersecting responsibilities of "no one managing" or "managing together". A normalized and standardized linkage mechanism should be established to regulate and promote the development of technology on the right track, and to solve the problem of multi headed management.

5. CONCLUSION

The vigorous development of generative AI technology is a new quality productivity of China's digital economy and a sharp tool to promote the transformation and upgrading of traditional industries. However, behind the rapid development of AI big data such as ChatGPT and ERNIE Bot, many data risks also follow. The current legal norms in the field of artificial intelligence have shortcomings in terms of regulatory subjects and content. To further promote the development of generative artificial intelligence, it is necessary to improve regulations in the field of artificial intelligence, establish a coordinated and unified regulatory mechanism, and divide responsibility subjects at different stages to alleviate the negative impact of generative artificial intelligence and achieve a balance between the development of new quality technologies and public data security.

REFERENCES

[1] Yuan, J. (2024, December). Efficient techniques for processing medical texts in legal documents using transformer architecture. In 2024 4th International Conference on Artificial Intelligence, Robotics, and Communication (ICAIRC) (pp. 990-993). IEEE.

[2] Song, X. (2024). Leveraging aigc and human-computer interaction design to enhance efficiency and quality in e-commerce content generation.

[3] Wu, W. (2025). Construction and optimization of intelligent gateway software management platform based on jenkins cluster management under cloud edge integration architecture in industrial internet of things. Preprints, January.

[4] Chen, J. (2025). Geospatial Neural Networks: Enhancing Smart City through Location Intelligence.

[5] Peng, Q., Zheng, C., & Chen, C. (2024). A Dual-Augmentor Framework for Domain Generalization in 3D Human Pose Estimation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 2240-2249).

[6] Peng, Q., Planche, B., Gao, Z., Zheng, M., Choudhuri, A., Chen, T., ... & Wu, Z. (2024). 3d vision-language gaussian splatting. arXiv preprint arXiv:2410.07577.