Academic Journal of Management and Social Sciences
ISSN: 2958-4396 | Vol. 9, No. 2, 2024

Risks of Generative Artificial Intelligence and Multi-Tool Governance

Fangfei Hu, Shiyuan Liu *, Xinrui Cheng, Pengyou Guo, Mengqi Yu

Nanjing Audit University, Nanjing, Jiangsu, 211815, China

*** Corresponding author:** Shiyuan Liu (Email: 3486641392@qq.com)

Abstract: While generative AI, represented by ChatGPT, brings a technological revolution and convenience to life, it may raise a series of social and legal risks, mainly including violation of personal privacy and data security issues, infringement of intellectual property rights, generation of misleading and false content, and exacerbation of discrimination and prejudice. However, the traditional AI governance paradigm oriented towards conventional AI may not be adequately adapted to generative AI with generalized potential and based on big models. In order to encourage the innovative development of generative AI technology and regulate the risks, this paper explores the construction of a generative AI governance paradigm that combines legal regulation, technological regulation, and ethical governance of science and technology, and promotes the healthy development of generative AI on the track of safety, order, fairness, and co-governance.

Keywords: Generative Artificial Intelligence; ChatGPT; Risk; Multi-tool Governance.

1. Introduction

A human-computer interaction application called ChatGPT has exploded around the world, setting off a technological race to develop pre-trained large models of generative artificial intelligence. Generative AI is rooted in Artificial Intelligence Generated Content (AIGC), which, as a new type of content production in the Internet 3.0 era, has gone through two stages: expert creation in the Internet 1.0 era and user creation in the Internet 2.0 era. Along with the innovation of content production, enterprises scramble to access the big model, opening up a new business model of 'model as service', forming an industrial ecosystem in which upstream enterprises research and develop the basic model → midstream enterprises in each vertical segment access and fine-tune the basic model to form a professional model → end-users use the service application, which is expected to become the digital infrastructure for promoting the development of the digital economy in the era of Artificial Intelligence. Among them, service applications may be launched by upstream enterprises on the basic model they have developed. Take chatbots as an example, ChatGPT launched by OpenAI, Bard launched by Google, and ERNIE Bot launched by Baidu generate cross-modal content such as text, audio, image, and video according to end-users' requirements with the support of the GPT, LamDA, and ERNIE large-language models, respectively, and more enterprises provide data and algorithm support for the research and development of their service applications by accessing basic models or professional models. For example, Microsoft accessed GPT to release the AI assistant Windows Copilot, which promotes the application of AI in office software.

Generative AI, as a state-of-the-art result formed by the use of AIGC technology, is characterized by massive training data, cross-modality, versatility, emergence, generalization, human-computer interaction, etc., and its operational process can be broadly divided into three phases of data collection, model training, and content generation. On 30 January 2023, a Colombian judge for the first time incorporated ChatGPT's response into a judgement, causing a heated debate in the legal community. Generative AI may generate a series of social and legal risks while promoting production and facilitating life. Currently, the traditional AI governance paradigm represented by the EU, the US and China may present response challenges in different dimensions. Against the above background, this paper combines the industrial, technological characteristics and operation mechanism of generative AI, tries to explore the construction of generative AI governance paradigm on the basis of the traditional AI governance paradigm, and applies the multiple governance tools to regulate the risks, and safeguard the innovation and development of generative AI technology while regulating it.

2. Social and Legal Risks of Generative Artificial Intelligence

2.1. Risk of Infringement of Personal Privacy and Data Security

Firstly, generative AI has the risk of violating personal privacy in the data collection phase. OpenAI's dataset is divided into raw dataset and real-time dataset [1]. The company has not publicly explained the source and ownership of the raw dataset, presenting a 'black box' state. The real-time dataset does not strictly implement the principle of 'informed consent' of users, and users will inevitably upload private information when using the platform. As the platform is in a strong position and the users are in a weak position, and the difference between the two positions is too great, the platform only grants the right to collect and use the relevant information based on the user's 'Confirmation of Use Agreement' is unfair. In addition, even if the user agrees to collect the data uploaded by himself, the platform should not collect excessive user information, and sensitive personal information should be protected. The definition of sensitive information is so vague that people in different regions and cultures, and even the same person in different contexts, have different definitions of sensitive data [2] , making it difficult to establish standards for defining sensitive information and making it difficult for platforms to be held accountable for

infringing on sensitive information. Article 13 of the Personal Information Protection Law stipulates that personal information processors should obtain the consent of individuals to process personal information, and generative AI obtaining personal data without the consent of individuals violates the relevant provisions and may infringe on personal privacy.

Secondly, generative AI has a data security risk of leaking data during the model training phase. In 2023, Samsung's semiconductor division allowed engineers to use ChatGPT to check source code, and three employees on three different occasions accidentally leaked sensitive information to ChatGPT, which was used for model training, after which Samsung took emergency measures and limited the capacity of uploading data to ChatGPT. If the leak is a trade secret, there may also be a risk of violating the rights of corporate data, Samsung, Amazon, Goldman Sachs have banned or restricted the use of ChatGPT by their employees at work due to concerns about data security risks. Data leakage may indirectly infringe on personal privacy and trade secrets, or even harm public interests and national security, while affecting the quality of the generated content.

2.2. Risk of Infringement of Intellectual Property Rights

Firstly, the data collection and model training phase.

Article 7 of the Interim Measures for the Administration of Generative Artificial Intelligence Services stipulates that, when performing model training tasks, providers of generative artificial intelligence services (hereinafter referred to as 'providers') must ensure that the source of the training data is lawful and are strictly prohibited from infringing on the rights and interests in intellectual property enjoyed by any third party. The section '5.2 Security Requirements for Corpus Content' of the Technical Specification 'Basic Requirements for Security of Generative Artificial Intelligence Services (TC260-003)' emphases that the Provider should pay special attention to and actively avoid potential risks of intellectual property infringement in the corpus, and avoid adopting materials that may lead to intellectual property disputes. Under the Copyright Law and the Patent Law, providers are obliged to thoroughly investigate and eliminate the risk of copyright and patent infringement in training data. Specifically, unless relying entirely on data resources in the public domain, providers should obtain prior permission from the holder of the corresponding work or patent right before using training data containing information about a specific work or patent to ensure compliance and legality.

Generative AI may be at risk of copyright infringement. At the data collection stage, large-scale reproduction and integration of works that are still under copyright protection may not only touch the legal boundary of the right of reproduction, but may also potentially infringe the right of compilation, as the way in which the data is aggregated involves the creative labour of selecting and arranging the original work. At the model training stage, operations such as weight removal, correcting errors and splitting data into small linguistic units essentially involve the deletion, restructuring and deformation of the content of the work, which may very likely touch on the right of modification and threaten the integrity of the work, and may even improperly exercise the right of adaptation, translation and re-compilation.

Generative AI may be at risk of patent infringement. Technology development activities may involve the unauthorized use of others' patents as research and development aids, raising legal issues of patent infringement. A patent is essentially an exclusive right that gives the patent holder exclusive control over the 'implementation' of the patented product or process. A product patent requires that the product be put into use in its entirety, and a method patent requires that all of the disclosed steps be carried out [3]. Following the principle of patent exhaustion, once a patented product is first sold on the market by lawful means, subsequent use of the product does not, in principle, constitute infringement. However, this principle does not extend to method inventions. The setting of this legal boundary means that generative AI may incur the risk of patent infringement if it uses another person's method patent without obtaining authorization when creating a new invention or performing an invention procedure.

Secondly, the content generation phase.

Generative AI may be at risk of copyright infringement. Changes between the generated content and the input data of an AI can be categorized into four types: without any modification, modification but not to the extent of adaptation, modification equivalent to the act of adaptation, and modification beyond adaptation [4]. The first three categories correspond to potential infringements of the right of reproduction, the right of modification, and the right of adaptation, respectively, while the last category may fall into the category of 'fair use' due to its essentially innovative or transformative nature, and thus does not constitute infringement. Thus, if the generated content is substantially the same as a pre-existing copyrighted work or does not go beyond adaptation, it may constitute copyright infringement.

Generative AI may be at risk of patent infringement. The core of patent law is to protect inventions and creations that are novel, inventive and practical. If the generated technical solutions are only minor adjustments to the prior art or pure wordplay without bringing substantial technological advances, these patent applications may not meet the basic criteria for patent granting, which may not only lead to an overall decline in patent quality, but also trigger a patent bubble and increase the cost of innovation in the industry. Even if successfully granted, these patents may infringe on existing basic or core patents.

2.3. Risk of Generating Misleading, False Content

Firstly, generative AI may generate misleading information due to the lack of professional knowledge. ChatGPT's generated content mainly comes from databases, and the information in databases is ultimately limited, and the shortcomings are more obvious in some highly specialized fields. For example, the dispute about insurance claims in the financial field - whether the effective time of the insurance contract is when the policyholder pays the premium, or when the policyholder receives the policy, or the 'zero hour of the next day' as stated in the insurance terms. The dispute in China does not have a clear legal provision, in judicial practice, the judge's judgement and reasoning are also different. Reasonable resolution of these disputes requires not only a strong legal foundation but also sufficient thinking, while ChatGPT lacks professional training and the conclusions based on data integration alone are likely to be wrong and misleading to users.

Secondly, generative AI may make false expressions

because of false information in the database. When the database contains false information, generated content containing false expressions may be produced. Even if the data is all true, ChatGPT may generate false information based on the internal text generation model, which is still unavoidable with the current technology path [5]. Users 'use and dissemination of false information based on their trust in the generated content may bring about adverse effects for the national image, public order, and personal reputation. In May 2023, the Pingliang Public Security Bureau's cybersecurity brigade detected the first case in China in which generative AI was used to concoct false news, which aroused widespread concern and adverse effects in the society.

2.4. Risk of Discrimination and Prejudice

Firstly, generative AI may be at risk of sexism. Today's society is still divided over the status of women, and the attitude of algorithm developers towards this issue plays a significant role in generating content. In order to cater to users, ChatGPT usually filters out irrelevant information, and this behavior can inadvertently result in the reinforcement of pre-existing discriminatory tendencies. For example, Google Translate software often translates the Turkish phrase 'he/she is a doctor', which has no explicit gender designation, into the male form and 'he/she is a nurse' into the female form. In addition, sample data stored within generative AI over time is also at risk of gender discrimination.

Secondly, generative AI may risk employment bias. Recruitment company HireVue uses online 'video interviews' or 'game-based challenges' to assess job applicants' qualifications, but many older employees do not play video games, and fewer women than men play games. The company's proprietary algorithm itself fails to recognize that there are differences in preferences between groups, thus discriminating against groups such as older employees and women in employment. In addition, sample data stored within the generative AI over time is also at risk of employment discrimination.

3. Responding to the Challenges of the Traditional AI Governance Paradigm

3.1. The Risk Governance Paradigm Represented by the EU

In 2021, the Council of the European Union put forward a proposal for a regulatory framework of AI in the EU, referred to as the Artificial Intelligence Bill, which proposes to develop a technology-neutral definition of AI systems in EU law and to categorize AI applications with different requirements and obligations based on a 'risk-based pathway' and to develop the corresponding regulatory approach accordingly. The bill classifies the risk level of AI applications into four categories: unacceptable risk, high risk, medium risk and low risk, with applications deemed to carry unacceptable risk being prohibited altogether, such as biometric classification systems based on sensitive features.

The four-tier AI risk taxonomy targets decision-based AI that handles specific tasks in specific application scenarios for precise and differentiated regulation, whereas generative AI with versatility potential is used as digital infrastructure in a wide variety of application scenarios, which may be at different risk levels, or may even cover all risk levels. In addition, the application scenarios of generative AI with emergent and excellent generalization capabilities may continue to expand along with technological innovations. As a result, the risk governance paradigm that intends to assess a particular generative AI as a certain risk level and accurately regulate it accordingly may suffer from a governance vacuum and a conversion lag, and face the risk of failure. However, one year after the birth of ChatGPT, the EU Parliament passed the Artificial Intelligence Act on 13 March 2024, which still continues the four-level risk classification, so whether the risk governance paradigm is effective for generative AI has yet to be proved in practice.

3.2. The Applied Governance Paradigm Represented by the United States

Compared with the EU, the U.S. federal level has not yet introduced a unified and comprehensive artificial intelligence legislation, but selected key application scenarios were in the form of separate laws and regulations to implement targeted governance, which currently exists mainly in the field of autonomous driving, algorithmic recommendation, face recognition, deep synthesis and other applications [6].

Firstly, from the horizontal level of generative AI application scenarios, there is a challenge to cope with the application governance paradigm of precisely regulating special application scenarios. The versatility of generative AI drives its application scenarios from personalization to universality, while the emergent and excellent generalization capabilities of generative AI make its application scenarios change dynamically. Therefore, the governance paradigm of separate legislation for various application scenarios is difficult to comprehensively cover various industries and fields that apply generative AI [7].

Secondly, from the vertical level of the generative AI industry, there are challenges in dealing with the application governance paradigm that only regulates application scenarios. The industry of generative AI can be divided into three levels, namely, 'basic model, professional model, and service application.' [8] The basic model located in the upstream of the industry acts as the 'engine', model developers from various industries fine-tuning the basic model according to the characteristics and needs of the industry to form the professional model located in the middle of the industry, and the service applications designed on the basis of the professional model and located in the downstream of the industry play the roles of both technology and content producers, providing intelligent and personalized services directly to end users. Therefore, in the generative AI industry, the design problems and defects of the basic model will be transmitted to the professional model and service applications, and the regulation of the application scenarios, i.e. specific service applications, can only solve the problems of the application scenarios, but can hardly be radiated to the basic model and professional model, and cannot alleviate the systematic risks of the generative AI industry fundamentally.

3.3. The Subject Governance Paradigm Represented by our Country

Algorithms in the 'black box' are opaque and difficult to understand, and may challenge the human right to information and autonomous decision-making, threaten the privacy and freedom of individuals, and generate discrimination and bias [9]. In order to regulate AI service providers that use technology and information asymmetry to

form an advantageous position that harms the legitimate rights and interests of users, China has adopted the subject governance paradigm of service provider responsibility, and the Administrative Provisions on Algorithmic Recommendation of Internet Information Services, which came into force on March 1, 2022, clarified the subject responsibility of algorithmic safety of algorithmic recommendation service providers, the Administrative Provisions on Depth Synthesis of Internet Information Services, which came into force on 10 January 2023, clarified the subject responsibility of information security of depth synthesis service providers, and together with the Network Security Law, the Data Security Law, the Personal Information Protection Law and other laws, constructed the main framework of AI governance in China.

Compared with traditional AI, generative AI has the industrialization characteristics of 'basic model-professional model-service application' and the interactive characteristics of human-machine dialogue, which makes its risks come from multiple subjects in the process from model development to user use. The traditional AI subject governance paradigm, which only targets service providers, may have limitations in responding to these risks. The Interim Measures for the Administration of Generative Artificial Intelligence Services (hereinafter referred to as the 'Measures'), which came into force on 15 August 2023, continue the subject governance approach by stipulating that generative AI service providers (hereinafter referred to as 'Providers') shall assume the responsibility of network information content producers, and where personal information is involved, they shall assume the responsibility of personal information processors. Although Article 4 sets out the obligations of users, for example, paragraph 4 states that 'they shall not infringe upon others' rights to portrait, reputation, honour, privacy and personal information.' And the second paragraph of Article 14 imposes technical regulations on users, 'If a provider finds that a user has used a generative AI service to engage in unlawful activities, it shall take measures such as warning, restricting the function, suspending or terminating the provision of services to the user, keep the relevant records, and report them to the competent authorities concerned.' All reflect the Measures' progressive significance in conforming to a certain extent to the subject diversification characteristics of generative AI, but still list the provider as the only legally responsible subject. Providers are the 'engine' driving the development of the generative AI industry, and if they bear too much responsibility, it may not be conducive to improving their research and development enthusiasm, and is not conducive to the effective management of systemic risks of generative AI.

4. A Generative AI Governance Paradigm with Multiple Governance Tools

Generative AI has strong technical expertise and ethical subversion, and the iteration cycle of the technology will become shorter and shorter, so the rigid governance based on legal norms cannot significantly improve the effectiveness of governance. For the governance paradigm of generative AI, we should adhere to the concept of inclusive and prudent governance, establish the principle of people-oriented governance, make up for the limitations of the traditional AI governance paradigm, make comprehensive use of diversified governance tools such as law, technology, ethics, etc., innovate the regulatory system with law, crack the professional problems with technology, and make up for the insufficiency of hard law with soft law.

4.1. Statutory Regulation

Firstly, based on the industrial characteristics of generative AI, a new path of legal regulation that combines vertical layered governance and multiple subject governance is explored.

Vertical layered governance. In the industry pattern of 'basic model - professional model - service application', the basic model is the prerequisite for the generation of professional model and service application, and even some basic models have the functions of supplying both data elements and information content, which can directly launch service application to the end-users to generate content. Therefore, basic model governance is the core of the governance of the generative AI industry, and a set of professional and effective basic model governance models should be designed to clarify the legal obligations and responsibilities of basic model service providers, and provide targeted governance for higher-risk application scenarios at the same time, so as to fundamentally mitigate the systemic risks of the generative AI industry.

Multi-subjects' governance. From the perspective of the generative AI industry as a whole, the behavior of providers plays a decisive role in the generation of risk, and while they are subject to legal regulation, the illegal and criminal behavior of some users should also be taken seriously enough and be incorporated into the framework of legal regulation. There is a case in which a user named 'Walkerspider' induced ChatGPT to 'break out of jail': the user asked ChatGPT to play the role of DAN and told it that DAN could do anything without any rule constraints, thus forcing ChatGPT to give an answer that violates the OpenAI guidelines [10]. When a provider fails to block user-generated harmful content in a timely manner, and the dissemination of that content harms the state and public interests and disrupts public order, the provider and the user can be held jointly liable and share the risk. In addition, subdividing the responsibility of the provider, according to the characteristics of the industrial level in which it is located for the provider of the basic model, professional model to set up regulation rules separately. Constructing a diversified and precise generative AI subjects' responsibility matrix, reasonably allocating responsibilities, improving the quality and efficiency of governance, and seeking an optimal solution to the contradiction between legal regulation and technological progress.

Secondly, for the risks arising from the operation of generative AI, taking the example of coping with the risk of intellectual property infringement, it provides suggestions for the improvement of the existing legal regulation.

In the face of the real needs of the development of artificial intelligence in the context of the big data era, the traditional 'authorization before use' is particularly inefficient and costly in dealing with massive amounts of data, which undoubtedly constitutes a major obstacle to the progress of generative artificial intelligence technology. In view of this, some academics and policymakers have argued for the inclusion of data ingestion in the legal scope of 'fair use'. The principle of 'fair use' permits the use of protected works without prior authorization or payment from the copyright owner in certain limited circumstances, such as for personal study, research or

enjoyment. Extending this principle to the field of AI means that generative AI can access and utilize a wide range of data resources more freely, significantly reducing training costs and improving training efficiency, as well as effectively avoiding the risk of copyright infringement. For example, the EU Digital Single Market Copyright Directive further opens up copyright exceptions for data mining activities for scientific research and cultural heritage purposes, allowing research institutes and cultural heritage protection units to conduct text and data mining without direct authorization from the copyright holder under certain conditions. Therefore, rationalizing the data collection and model training activities of generative AI as 'fair use' and drawing on advanced international legislative practices similar to the EU Copyright Directive can improve the operational efficiency of generative AI technology and facilitate technological innovation while safeguarding the rights and interests of the original authors.

4.2. Technology Regulation

British jurist Roger Brownsword's Law 3.0 theory argues that 'ex ante technological solutions are more effective than ex post efforts to detect and correct breaches of contractual terms and conditions.' [11] Emphasizing the importance of using technology to regulate technology.

In order to avoid the risk of infringement of personal privacy, trade secrets and intellectual property rights that may be violated by training data, synthetic data can be created by methods such as Generative Adversarial Networks and Variational auto-encoder. Synthetic data is a kind of non-artificially created data that mimics real-world data and is able to display the same information as the original data without revealing personal or sensitive information. Taking medical research as an example, synthetic data maintains the same biological characteristics and percentage of genetic markers as the original data, but the patient's name, age, and so on are false [12]. Therefore, strengthening the application of synthetic data in generative AI pre-training can avoid the risk of infringement from the source.

With regard to the risk that the output may contain harmful content such as misleading, false, bias and discrimination, technical means can be used to achieve the dual regulatory effect of risk prevention and consequence management. Firstly, generative AI should be 'AI aligned', so that its goals and behaviors follow human values and ethics, and harmful outputs and abusive behaviors of the models can be prevented as much as possible. Specific techniques include Reinforcement Learning with Human Feedback, Adversarial Testing and content filtering tools. Secondly, the use of generated content detection and identification technology to accurately identify and quickly alert harmful content, blocking its continued generation and dissemination; smooth user feedback channels, giving play to the advantage of the user's first discovery of harmful content, and helping to eliminate harmful content.

4.3. Ethical Governance of Science and Technology

Compared with legislative adjustments with a lag, ethical governance of science and technology restrains providers through agile industry standards, corporate autonomy and other forms to avoid technology from falling into disorder at the beginning of innovation. Foreign countries have explored the use of science and technology ethics to prevent the risks of AI technology earlier, and the European Union proposed 'kindness', 'non-harm', 'autonomy', 'justice' in the 'Ethical Guidelines for Trustworthy AI' released as early as 2019. The EU has proposed five ethical principles and seven key requirements for science and technology, namely 'kindness', 'non-harm', 'autonomy', 'justice' and 'interpretability' in its 'Ethical Guidelines for Trustworthy AI' released as early as 2019, and has guided AI developers and deployers to put the principles into practice through assessment lists, so as to enhance the operability of the principles and requirements. The National Artificial Intelligence Initiative Act of 2020 enacted by the United States indicates that its digital science and technology ethics regulation focuses on the triple model of government legislation and standards-led regulation, pluralistic and participatory regulation by social organizations such as industry associations and research institutes, and embedded autonomy where science and technology ethics are embedded in corporate governance [13]. China's 'New Generation of Artificial Intelligence Ethics Code' released in September 2021 proposes to 'enhance human well-being', 'promote fairness and justice', 'protect privacy and security', 'ensure controllability and trustworthiness', "Strengthening responsibility", and "Enhancing ethical literacy", while proposing eighteen specific ethical requirements for specific activities such as AI management, research and development, supply, and use. The Measures for Ethical Review of Science and Technology (for Trial Implementation) issued in September 2023 clarifies the principles of science and technology ethics established by the Opinions on Strengthening Ethical Governance of Science and Technology, and adopts a governance model combining review, management, government review, supervision. The research and development activities of generative AI have been included in the list of review, but the current review criteria for it are relatively general, and there is a lack of operational evaluation criteria and systematic evaluation procedures.

With regard to the governance of science and technology ethics of generative AI in China, we can learn from the experience of the EU and the United States, and based on the existing principles and norms, give full play to the dynamic role of empowered industry associations and other social organizations, formulate a review list and improve the review mechanism for each stage of generative AI, such as data collection, model training, and content generation, and follow the technological innovations to make timely and dynamic adjustments. At the same time, the Science and Technology Ethics Committee under the supervision of the industry association evaluates the AI activities of the unit in accordance with the evaluation standards and evaluation procedures, and finally the industry association integrates the evaluation results of each stage to arrive at the ethical compliance of the AI activities of a certain unit, puts forward suggestions for improvement or requests for rectification, and reports to the relevant departments about the units that are seriously not in compliance with the ethical principles and norms, and handled in accordance with the Measures for the Review of Ethics in Science and Technology (Trial Implementation). Explore a new path of science and technology ethical governance that combines government regulation and industry autonomy, and realize agile governance of generative AI technology risks with soft law first.

5. Conclusion

Generative artificial intelligence has already formed a distinctive industrial form, with distinctive technological characteristics and operational mechanisms. ‘Science and technology are the first productive forces’, and reducing the social and legal risks brought by science and technology without discouraging scientific and technological innovation is the scientific way to govern generative AI. In this paper, legal regulation, technological regulation and scientific and technological ethical governance are jointly incorporated into the governance framework of generative AI, exploring a new path of legal regulation that combines vertical layered governance and multi-subjects governance, and giving full play to the technological expertise of regulating technology with technology, and scientific and technological ethical governance through a combination of governmental regulation and industry autonomy, reducing the lagging disadvantages of legal regulation, constructing a governance model for generative AI.

References

[1] Guo Yu Jie,Ding Guo Feng.Data security risk and response of ChatGPT generative AI[J]. Big Data Times,2023, (07):24-31.

[2] Li Sen. The governance path of generative artificial intelligence data security under the risk prevention perspective - taking GPT class model as an example[J]. Journal of Tibet University for Nationalities (Philosophy and Social Science Edition),2023,44(06):139-145.

[3] Chen Mingtao. Analysis of patent infringement liability under the conditions of cloud computing technology[J]. Intellectual Property Rights, 2017(3):50-59.

[4] Wei Yuanshan. Copyright law responses to generative AI training data: is a fair use rule really needed? [J/OL]. Library and Intelligence Knowledge,2024.

[5] Wu Zongxian,Xiao Yanqiu. Application, risk and legal response of generative artificial intelligence--taking ChatGPT as a perspective[J]. Journal of Tianjin Normal University (Social Science Edition),2024,(03):12-20.

[6] Liu Dian. An overview of the legislative process and main contents of the EU Artificial Intelligence Bill.

[7] Zhang Linghan,Yu Lin. From traditional governance to agile governance: governance paradigm innovation for generative artificial intelligence[J]. E-government, 2023, (09):2-13.

[8] Zhang Linghan. Legal Positioning and Layered Governance of Generative Artificial Intelligence[J]. Modern Law,2023, 45 (04):126-141.

[9] Ding Xiaodong. On the legal regulation of algorithms[J]. Chinese Social Science,2020(12):138-159+203.

[10] Anirudh VK.This could be the End of Bing Chat, https:// analyticsindiamag.com. this-could-be-the-end of-bing-chat/, accessed 28 May 2024.

[11] Roger Brownsword. Law 3.0: rules, regulation and technology [M]. Mao Haidong, Translation. Beijing: Peking University Press,2023: 42+119-125.

[12] See AWS official website, https://aws.amazon.com/cn/what-is/synthetic-data/, accessed on 4 September 2024.

[13] Xiao Hongjun,Yang Zhen. Ethical Regulation of Digital Technology: Progress in the U.S. and Lessons from China[J]. Research on Financial Issues, 2023, (06):73-86.