Promotion on the Legal Framework and Its Practice for the Normative Development of Generative AI in China – Focused on the Relevant Clauses of China's Interim Measures for the Administration of Generative AI Services

Bing Chen *

Posted Date: 14 February 2025

doi: 10.20944/preprints202502.1075.v1

Keywords: generative AI; risk; extraterritorial rule of law; rule of law; practice architecture

Article

Promotion on the Legal Framework and Its Practice for the Normative Development of Generative AI in China—Focused on the Relevant Clauses of China's Interim Measures for the Administration of Generative AI Services

Bing Chen

Center of Competition Law, Nankai University School of Law, Tianjin 300350, China; bing.chen@nankai.edu.cn

Abstract: Nowadays, generative AI technologies and services have entered a stage of explosive growth worldwide. While generative AI brings technological progress and productivity enhancement to the economy, it also raises various risks regarding legal, the ethics of science and technology, and social governance. For the development of AI, the EU adopts a strict regulatory attitude based on the rule of law. It constructs AI norms by unifying the regulations and coordinating regulatory agencies. The United States, on the other hand, adopts a principled and advocacy regulatory strategy. It clarifies the compliance requirements for enterprises with concerns about their autonomy. While the UK only claims the principles that are not mandatory, which is a compromise regulatory approach. Based on the practical needs of China's participation in the international AI competition and comparison among foreign experience, the rule of law of generative AI should rest on the interactions between technology and law, and the balance between development and security. Additionally, it should establish requirements for security, reliability, and controllability for the standardized development of AI within the legal framework. To this end, it is necessary to strengthen the supply of relevant policies and systems, establish a diversified and long-term regulatory mechanism as soon as possible, and set standardized and unified responsibility rules. Sequentially, to establish a full-cycle, systematic, and three-dimensional practice framework of the rule of law, thereby ensuring the robust and normalized development of generative AI, while firmly maintaining safety as the baseline.

Keywords: generative AI; risk; extraterritorial rule of law; rule of law consideration; practice architecture

1. The Raise of the Problem

Various generative AI technologies and products such as Alpaca, GPT-4, PaLM-E, Wenxin Yiyan, and Security Copilot have entered into social and economic life. With the development of popular practices such as the explosion of ChatGPT, which brought generative AI into the public spotlight, the application of generative AI has gradually changed from a "tool" to a "decision-maker", whose important mission is in medical care, entertainment & recreation, livelihood, finance, and other industries. However, due to the wider and wider penetration of generative AI into social production and life, its ethical and legal risks have been amplified accordingly. Moreover, generative AI appears as the feature of algorithmic black boxes, which makes it difficult to supervise. As a result, society's doubts about generative AI are sharply increasing, and there is even a sense of suspending operation services conditions [0] Though this lack of trust is actually legitimate, in the long run it will seriously hinder the development of generative AI, holding the digital economy —and even the real

 doi:10.20944/preprints202502.1075.v1

economy back. Therefore, how to choose governance tools and control the limits of governance is of key significance in the international competition of artificial intelligence development and international economic and trade competition.

Reducing the risk of AI is not only a task that should be solved in the technical aspect but also a goal that should be faced from the institutional perspective [2] In order to promote the healthy development and standardized application of generative AI technology, on July 10th, 2023, seven of China's departments including the Cyberspace Administration of China jointly issued the Interim Measures for the Administration of Generative Artificial Intelligence Services (hereinafter referred to as the "Interim Measures". The Interim Measures, which clearly put forward the principles of "attaching equal importance to development and security" and "combining promoting innovation and ruling by law", clarify the following: (1) implementing inclusive, prudent, classified, and hierarchical supervision of generative AI services, (2) stipulating the requirements of laws and regulations, social morality and ethics of generative AI products or service, (3) clarifying the obligations and responsibilities that providers of generative AI services (hereinafter referred to as "providers") need to bear.

The promulgation of the Interim Measures makes them important topics, how to apply the rules better to coordinate development and security, how to provide a tolerant, credible, and controllable institutional environment for innovation and development based on consolidated safe development, and how to provide scientific, powerful, and robust institutional support for the realization of China's AI technology and industry overtaking in the curve with high-quality institutional opening.

Therefore, this paper intends to explore the risks posed by generative AI, combine the current governance of generative AI in China and compare it to foreign experience. In addition, it discuss the intervention and restrictions methods of the rule of law on generative AI, analyze the internal goals and basic requirements of the healthy development of generative AI, and then put forward relevant suggestions for the rule of law promotion of the development of generative AI.

2. The Various Risks to the Development of Generative AI

The mission of jurisprudence is not to appreciate the brilliant achievements brought about by the development of science and technology, but to examine the irrational consequences that technology may bring, and to reduce the risks of scientific and technological development through the rule of law [3] At present, generative AI, as an algorithm for training large data models, has gradually decreased its controllability and increased autonomy, bringing convenience and risks to human society. The risk factor lies in generative AI may violate laws and regulations, resulting in negative social effects, and there is room for debate on whether laws and regulations should be amended. By exploring the types of risks and the generation paths, we can provide theoretical support for the practice of the rule of law and outline the framework for its implementation. Specifically, there may be the following legal risks.

2.1. Major Legal Risks

2.1.1. Legal Risk of Intellectual Property Rights

The training of generative AI requires a large amount of data, including not only content that has lost prior rights such as copyrights and trademark rights, but also content that is still protected by intellectual property rights such as copyrights. In the context of the application of artificial intelligence technology and the development of industrial innovation, especially in the training of generative artificial intelligence, if the act of automatically crawling and parsing learning other people's works and content involves the reproduction of the original work, then the act is likely to infringe the copyright of others. In the United States, there are already painters who brought a suit against a software company for its AI-generated works,[4] posing both physical and procedural challenges to the capture and use of data in generative AI training [5] However, if AI crawling is included in the scope of fair use, it will not only infringe on the legitimate rights of the prior rights

 doi:10.20944/preprints202502.1075.v1

holders[6] but also crowd out their living space. It is worth considering how to design a path that balances the interests of the two.

In addition, the content generated by generative AI may be similar to other people's content or have intellectual property infringement such as plagiarism. As for whether AI-generated content should be regarded as a work and granted copyright protection,[7] whether the liability for infringement should be borne by the service provider or the service user,[8] there is currently no clear legal provision, which has caused great controversy in the academic community.

In terms of law, a work protected by copyright (copyright) must be created by a human being, be original, and be a form of expression containing certain ideological content, and not be excluded by the Copyright Law such as laws and regulations, general number tables, formulas, etc. At present, there are three forms of generative AI, which are created entirely independently by AI, created with the assistance of natural persons, and generated according to prompt words entered by natural persons. Only one of the three forms described above directly involves human involvement, in which case generative AI-generated content may be copyrightable. "With the remaining two forms, it is problematic to define generative AI as a 'work.'" This is because artificial intelligence does not have independent thoughts, cannot "create" independently, let alone have copyright. In fact, the content generated is often generated by learning and analyzing large amounts of existing data, lacking originality. Therefore, there is no clear legal definition as to whether content generated by generative AI should be considered a work and granted copyright protection [9] There is a certain amount of controversy in academic and legal circles, which needs further study and discussion.

When it comes to tort issues, the attribution of liability is an important theoretical and practical problem. According to general principles of tort liability law, the party responsible for the actual tort is liable for the tort. Therefore, in the case of infringement of AI-generated content, if the infringement results from the service user's own operation or instructions, the service user typically assumes liability. However, in some cases, the service provider may also be liable if there is a technical or platform design defects lead to infringement.

Article 9 of the Interim Measures explicitly stipulates that "the provider shall bear the responsibility of an online information content producer in accordance with the law and fulfill the obligation of ensuring network information security." Furthermore, when personal information is involved, "the personal information processor shall assume the responsibilities of a personal information processor in accordance with the law and fulfill the obligation to protect personal information." These provisions significantly increase the product liability of the provider. When this requirement was solicited for comments in the Interim Measures, it sparked discussions from all walks of life, arguing that it was inappropriate to increase the responsibilities of providers and was not conducive to the development and utilization of AI technologies and products [10]

In summary, there are controversies about copyright protection and infringement liability for generative AI-generated content. Due to the complexity of this area and the fact that the relevant laws are not yet complete, further research and discussion are needed.

2.1.2. Legal Risk of Data Security and Personal Information

Generative AI requires a large amount of data to form a training database, and after it is officially operational, it continuously collects personal information about users. Artificial intelligence usually requires the user's general authorization, and if the user does not pay specific and careful attention to the authorization required by the artificial intelligence, the relevant private information will be invisibly crawled during the operation of the artificial intelligence, resulting in the risk of information leakage. Not only that, even after the user agrees to the relevant authorization, if the data and information crawled by the user exceeds the scope of authorization, there will be a risk of information leakage.

In this process, AI not only collects the user's personal information, but also portrays the persona according to the frequency, purpose, and method of the user's use of artificial intelligence, and private information initially shared in confidential conversations with the AI may be incorporated into the

 doi:10.20944/preprints202502.1075.v1

training database. Whether this data entry process constitutes a breach of privacy is also a subject of debate [11] In addition, due to the existence of the black box of artificial intelligence algorithms, it is difficult to clearly understand the internal process of artificial intelligence operation, which has a greater risk of personal information leakage.

The privacy policy of OpenAI, the company that developed ChatGPT, indicates that when users use ChatGPT, information about user access, use or interaction will be collected, and the relevant person in charge said that ChatGPT will use a small sample of data from each customer to improve model performance, and users who do not want the data to be used to improve performance need to send a request to OpenAI by email [12] This means that data containing user privacy and user conversations may be collected and stored in OpenAI's data centers, and as the number of ChatGPT users skyrockets, the amount of user data it collects and stores will also be huge.

Although, in recent years, data security protection technology has become more mature, and operators providing generative AI services have promised to ensure data security. However, on March 20, 2023, OpenAI officially stated that there are 12% of ChatGPT Plus users' data may have been compromised. Some users may see snippets of other people's chats, as well as information such as the last four digits of other users' credit cards, expiration dates, names, email addresses, and payment addresses [13] It can be seen that data security problems are unavoidable, and if data security is not effectively guaranteed, it will be difficult for AI technology to gain people's trust, which will hinder the development and application of AI.

The Interim Measures stipulate in the chapter "Technology Development and Governance" that generative AI service providers shall use data and underlying models with legal sources, and in the chapter on "Service Specifications", they stipulate that providers shall assume the responsibilities of online information content producers and fulfill network information security obligations in accordance with the law. Where personal information is involved, they must bear the responsibility of personal information processors in accordance with law, and perform obligations to protect personal information. All of this reflects the importance attached to data security issues.

2.1.3. Legal Risk of Fair Competition in the Market

The rise of generative AI raises another important question, namely the potential to strengthen the monopoly of tech giants in the market, creating a huge digital divide. The digital divide refers to the fact that "there may be a deeper hierarchical divide in the skills required to use the network effectively than just accessing it",[14] and this is particularly evident in the development of generative AI. In addition, the continued development of the digital divide may bring about an equal gap, and wealth and information will quickly gather in the technology giants, and the market structure will be further solidified [15] Although there are many generative AI applications on the market today, most of them are made by companies such as Microsoft, Google, Facebook, DeepMind, OpenAI, etc. Considering that Microsoft is still a major shareholder in OpenAI and Google is in control of DeepMind, the entire AI market is just a stage for tech giants. Judging from the statements of several giants so far, the main reason for their strong support for generative AI is to integrate them with their existing businesses, so as to strengthen their business advantages and market power.

After the formation of an oligopoly market, the market entry of artificial intelligence has formed extremely high commercial barriers. This commercial barrier stems from the cost of operation, which is astronomical even though core technologies such as the Transformer architecture are fully disclosed. In reality, there are very few companies that can afford to enter this high-yield market, and few companies can afford the high cost of training models. After the market barriers are generated, the potential monopoly risks generated by the technology giants using the transmission effect of the platform will also continue to emerge.

2.2. Ethical Risks in Science & Technology at Different Stages

Science and technology ethics are the values and behavioral norms that need to be followed in carrying out scientific research, technological development, and other scientific and technological

 doi:10.20944/preprints202502.1075.v1

activities, including the academic norms that scientists must abide by in their research behaviors, as well as the boundaries of basic principles and norms between scientific and technological achievements and the real society [16] They are an important guarantee for promoting the healthy development of scientific and technological undertakings.

2.2.1. In the Development Phase

Generative AI is a deep learning model trained on large amounts of textual data, , which often includes the work of humans. As a result, it is likely to inherit the discriminatory factors contained in human works. As a result, the content of the output may conflict with the current mainstream values, and may even produce discrimination, insults, and other content. Based on the self-learning nature of the algorithm model, such problematic outputs can quickly and deeply penetrate into the content generated by artificial intelligence, resulting in a wide range of false value transmission. If left unchecked, it may be perceived as acquiescing in the recognition of the existence of such illegal methods, undermining the credibility of the rule of law. Whether or not to impose obligations on providers to eliminate immoral or discriminatory content requires careful consideration of the current status and cost of technological development, as well as the balance between development and security.

2.2.2. In the Application Stage

The application of artificial intelligence to generate content is common, but artificial intelligence, as a non-human subject, has a thinking logic close to that of human beings, and whether the reuse of its generated content is in line with the ethics of science and technology is highly controversial. For example, ChatGPT can help users with a variety of tasks such as writing news stories and essays, and has become a tool used by some people to create rumors and fake papers. Recently, the author who won first prize in the Sony Photo Contest publicly acknowledged that his photographs were generated by artificial intelligence, and indicated that he confirmed that humans do not currently have the ability to recognize and discern whether content has been generated by AI [17]

2.2.3. In the Relief Phase

As artificial intelligence gradually becomes intelligent and autonomous, there is controversy over how to attribute the liability for various infringements arising from its operation. In practice, machines assist humans in reasoning, decision-making, and actions through artificial intelligence algorithms under preset goals, and the relevant entities of liability may involve AI algorithm designers, producers, distributors, users, etc., making it difficult to define the subject of tort liability [18] Whether AI should be the subject of responsibility[19] and whether non-legal moral responsibility should be attributed to artificial intelligence, which has no emotional value [20] ,are matters of controversy. An imbalance in the attribution of blame not only triggers a crisis of trust in society, but also hinders the development of generative AI.

In addition, in the investigation and collection of evidence in AI-related litigation, the authenticity and reliability of the evidence may be doubted in the face of algorithmic black boxes, whether it is the relevant data provided by the operator or the relevant information obtained by the judicial authorities in accordance with the law. It is difficult for even professional and technical personnel to fully analyze the AI algorithm, and it cannot be ruled out that the designers and producers of AI have a strong will and motivation to cooperate with AI to complete this series of operations. The algorithm black box induces the risk of man-machine collusion, and the causal relationship of tort liability is more difficult to judge, which aggravates the dilemma of AI infringement relief.

 doi:10.20944/preprints202502.1075.v1

2.3. Major Risks in Social Governance

2.3.1. The Non-Authenticity of Generative AI

It is difficult for generative AI to guarantee that the information it outputs is true and accurate. In practice, for example, when asked about topics that ChatGPT has not yet been trained or that does not have relevant information in its database, generative AI will often choose to fabricate false information or transplant other content, resulting in misuse and further dissemination of false information by users.

In fact, even before the emergence of artificial intelligence, disinformation could still be extremely confusing and cause social chaos [21] and the false content generated by generative AI, based on large-scale datasets is even more difficult to identify, which not only undermines the credibility of AI, but also greatly increase the cost of information credibility detection, resulting in a serious waste of social resources.

2.3.2. The Non-Reliability of Generative AI

Generative AI faces challenges in guaranteeing the quality of all generated content. For example, for relatively complex matters and value judgments, such as court decisions, the current trust in AI-generated content is still not as good as that ruling made by natural persons. However, with the continuous development of technology, the use of artificial intelligence to assist decision-making has become the general trend, but if artificial intelligence has always appeared corresponding defects and errors, the recognition and trust of society in artificial intelligence will be greatly reduced, forming a vicious circle and hindering the development of artificial intelligence. In addition, due to the widespread dissemination of AI, "it is easier to see small omissions that occur in unforeseen sequences in succession, which can become larger and more devastating accidents" [22] and the greatest risks posed by immature AI technologies actually stem from their high permeability and high integration to society, resulting in a knock-on effect.

At the same time, the non-reliability of generative AI will also bring risks to users. In the case that most of the content can be generated by AI, it is difficult for users to distinguish which content can be directly applied and which cannot be directly applied. In addition, the detection cost of this part is quite high, and it is difficult for users to afford once the benefits are damaged.

2.3.3. The Weak-Controllability of Generative AI

Generative AI has a great breakthrough compared to previous artificial intelligence, and its autonomy has been improved after deep learning. Human intervention is no longer a rule definer but rather corrector of errors in the process of generative AI programming. AI developers cannot predict what results the model will produce under corpus training.

At the same time, as AI gradually moves from a professional field to a general-purpose AI, the broadening scope of its application places higher demands on knowledge reserves, and the role of human beings in it is weakened, so thar it is difficult to strike a balance between the controllability and ability of AI [23] and once it is out of control, it is difficult to count on people's blind trust [24] it can even cause fear in society. Therefore, how to balance the controllability of artificial intelligence and the limits of functional development is of profound significance.

2.4. Analysis of the Risk Causes

At present, part of the risk problem of generative AI belongs to the inherent risk of natural person-generated content, and the application scope of AI has increased on the basis of artificial generation, from one-to-one risk to one-to-many risk; The other part belongs to the special risks of AI itself. Under the risk of natural persons as the main cause, it is debatable whether AI should be held accountable, or how to grasp the limits of the requirements for AI, so as to balance the development of AI and AI security. In the case of non-natural person risks, how to prevent them and which

 doi:10.20944/preprints202502.1075.v1

methods to adopt require continuous innovation in regulatory methods and improvement of innovation capabilities.

In fact, the classification and attribution of risks (see Table 1) shows that the fundamental contradiction of risk lies in how to control the limits between safety supervision and support for technological development, and what concepts and methods to uphold to balance the contradiction between the two, which has become an important research direction for generative AI in the future.

Table 1. The Types and Attribution of Risks of Generative AI.

Types of Risks	Specific Risk	Superficial Causes	Root Cause	Governance Tendency
Legal risks	Legal risk of intellectual property rights	Current IP-related laws and regulations are not suitable for generative AI generation models	Lack of governance norms	Strengthen the safety supervision of generative AI
	Legal risk of data security and personal information	The data security system is not in place		
	Legal risk of fair competition in the market	Driven by an oligopoly economic model		
Ethical risks in science & technology	Ethics risks in the development phase	Training techniques are imperfect and moral requirements are lacking	Lack of governance norms Training techniques are imperfect	Strengthen the safety supervision of generative AI Accelerate the technological development of generative AI
	Ethical risks in the application stage	The rules for exploiting generated content have faultiness		
	Ethics risks in the relief phase	Lack of governance norms		
Risks of social governance	The non-authenticity of generative AI	Training techniques are imperfect		Accelerate the technological development of generative AI
	The non-reliability of generative AI			
	The weak-controllability of generative AI	Lack of governance norms		Strengthen the safety supervision of generative AI

3. The Extraterritorial Investigations into the Development of Normative Generative AI

At present, although the regulation and supervision of artificial intelligence outside the territory are in the development stage, some governance experience has been formed, and has a certain scale of research in terms of governance principles, implementation rules, and responsibility rules, so it can be localized and used for reference in combination with the current situation of foreign supervision. Since generative AI is mostly not discussed separately from the context of artificial intelligence, the following discussion is also based on the context of the overall regulation of artificial intelligence.

 doi:10.20944/preprints202502.1075.v1

3.1. The European Union

In April 2021, the European Commission presented a proposal for an AI Act [25] The European Union's main regulatory approach to artificial intelligence is horizontal supervision, and the Artificial Intelligence Act has been called "the world's first attempt to horizontally regulate artificial intelligence systems". The bill focuses on risk management and compliance, with a focus on threats to personal safety and fundamental rights.

The AI Act classifies AI risks into four main levels: unacceptable, high risk, limited risk and minimal risk [26] AI systems with unacceptable risks trigger a full or partial ban, while high-risk systems are subject to EU products security methods for regulation. The Act focuses on "high risk" and imposes specific requirements on establishing and maintaining risk management systems, addressing biases and issues in training data, ensuring system traceability, providing comprehensive instructions to users, requiring manual supervision, and enhancing the security and robustness of the network.

On September 28, 2022, the European Commission published a proposed Directive on the Responsibility of Artificial Intelligence. The European Commission considers that existing liability legislation at the level of EU Member States is not appropriate to regulate liability claims for damage caused by AI products and services [27] The proposed AI Liability Directive introduces two additional measures specific to AI to complement these rules, namely reducing the burden of proof on victims through a "presumption of causation" and empowering a court to order a supplier of high-risk AI systems to disclose relevant information.

The EU has adopted a strict regulatory model, trying to coordinate issues related to AI systems with a new separate body based on a newly created law. However, on the one hand, it imposes too many restrictions on the development of AI, and there is a view that the AI law promulgated by the EU will make AI companies bear too high costs in Europe, with most of the compliance requirements are being technically achievable [28] On the other hand, compared to strict regulation, the compliance assessment obligations imposed on AI providers by the Act only involve internal procedures and lack external constraints, and the self-assessment by providers to prove that AI with high risks is complying with the Act, which may also reduce the effectiveness and enforceability of this governance tool.

3.2. The United States

In October 2022, the United States released The Blueprint for an AI Bill of Rights: Making Automated Systems Work for The American People (hereinafter referred to as the Bill of Rights Blueprint). It identifies five principles: the security and effectiveness of the system, freedom from algorithmic discrimination, ensuring data privacy, notification of the use of AI systems and their potential impact on users, and the ability to exit AI systems [29] However, the Bill of Rights Blueprint is not a mandatory and binding U.S. system or policy, and does not have the force of laws and regulations, but only provides a guide in principle.

In January 2020, the White House issued the Draft Memorandum on Regulatory Guidance for AI Applications (the "Draft Regulatory Guidance"), which is intended to provide guidance for the federal government to take regulatory and non-regulatory measures for the development and application of AI. The Draft Regulatory Guidance aims to promote development rather than protect security, with non-regulatory and non-legislative measures as a starting point, and a laissez-faire approach if the current state of development can sustain cost-effectiveness.

In general, the United States pursues the concept and principle of non-intervention unless necessary, and exerts maximum tolerance for the development of AI in enterprises. It can be seen that there is no systematic generative AI governance bill in the United States, and many documents, including the Regulatory Guidance (Draft) and the Bill of Rights Blueprint, have been issued in the form of guidelines and do not have mandatory effect. In terms of regulatory rules, although the regulatory principles for artificial intelligence are proposed, the way to achieve them is not through the formulation of additional laws and regulations, but through the non-regulation or transformation

 doi:10.20944/preprints202502.1075.v1

of existing laws and regulations, which has great uncontrollability and is difficult to ensure the implementation of the principles. In terms of regulatory strategy, the United States relies more on local policy regulation and corporate self-discipline to control risks, while the government chooses to focus on support and encouragement in policymaking.

3.3. The United Kingdom

On March 29, 2023, the UK government published a proposal for a new regulatory framework for AI – A Pro-Innovation Approach to AI Regulation (White Paper). In contrast to the US and EU approaches to AI regulation, the UK government has proposed a "common-sense, results-oriented approach" that seeks to balance the goal of becoming an "AI superpower" by 2030 with the serious risks posed by "proportional regulation" of AI, all while building a concrete regulatory framework around soft "principles."

Specifically, the UK has adopted a principled approach to eclectic regulation, which does not impose specific additional obligations and rights, but rather supports the regulation and development of AI through explicit regulatory principles. Although this method has flexible adjustment space and can quickly adapt to a variety of problems arising from general AI, it will inevitably bring problems such as unclear regulatory scope and ambiguous regulatory rules. For instance, the method of flexibly assessing the risk level in specific scenarios is essentially inoperable or requires extremely high observation costs.

In summary, even though there are different regulatory attitudes and methods outside the territory, they are actually reasonable choices made based on their respective realities. The current relaxed supervision model and strict supervision model are not absolutely opposed. With the continuous development of artificial intelligence, the scope and impact of risks continue to expand, and the two models also have a gradual convergence trend. The United States is also proposing relevant specific regulatory bills, and the European Union is also paying more attention to the development trend of artificial intelligence and making policy adjustments. In short, the rule of law for the development of artificial intelligence should not only focus on reasonably preventing the potential risks of artificial intelligence, ensuring that it develops along a reasonable, compliant, and legal path, but also consider the actual enforceability and operability of various systems. It should not impose overly harsh regulations on enterprises, as this may stifle innovation and hinder the development of artificial intelligence technology.

4. The Considerations of the Promotion of the Rule of Law in the Development of Generative AI

In view of the development risks of generative AI and the current status of extraterritorial governance, the law should intervene in a timely manner to promote the standardized and healthy development of generative AI under the framework of the socialist rule of law with Chinese characteristics. At the same time, it must also be clearly recognized that the rule of law is an important tool for governing the country, not an omnipotent artifact, and that it is necessary to follow rule of law thinking and adhere to the rules and methods of the rule of law when governing generative AI technology and applications. However, the regulation and management of generative AI by laws and regulations should remain modest, respect the laws of scientific and technological development, balance development and security, and realize the safe, reliable, and controllable development of generative AI.

4.1. The Measures of the Rule of Law to Promote the Development of Generative AI

Since generative AI can exhibit self-learning characteristics to a certain extent and has high intelligence and adaptability, in view of the current problems and risks, it is necessary to observe various values and expressions in the development of generative AI from multiple dimensions under the premise of following the basic principles of the rule of law and the basic laws of scientific and

 doi:10.20944/preprints202502.1075.v1

technological innovation, seeking a balance between various values and expressions, with safety as the bottom line and innovation as the main line.

4.1.1. The Mutual Promotion of Technology and Law

The development of generative AI is a scientific and technological issue, while the legal, social, and ethical risks arising from generative AI belong to the social sciences. When using generative AI in the rule of law to govern generative AI, it is legal scholars who put forward requirements for the technical issues of generative AI in terms of social risks. It is questionable whether this requires legal scholars to fully grasp the professional knowledge of AI or to what extent they need to understand the technical principles of generative AI.

In fact, law is a discipline that touches almost all areas of society, and if legal scholars are required to have complete professional knowledge of every industry, then legal scholars can hardly propose any legal provisions that address the relevant risks. The correct point is undoubtedly that if the focus is on "legal industry issues," industry experts should have a greater say; if it's a "legal issue for the industry," then legal talent is the ultimate authority, not the industry expert [30] However, even legal scholars can put forward relevant opinions on the professional issues of the industry through the embodiment of legal concepts, legal interpretation, analogy, and certain value judgment methods [31] The issue of the specifics of certain technologies and the accessibility of legal requirements remains unresolved, especially in the case of generative AI, where even AI experts themselves cannot predict what the AI will do.

Therefore, in the governance of artificial intelligence, the concept of technology and law interaction should be upheld, and the interaction system between technology and law should be designed. Countermeasures at the legal science and natural science levels should be put forward for legal risks, so as to properly address the relevant risks.

4.1.2. The Balance between Development and Security

The regulation of AI is intended to reduce various risks, thus protecting the interests and safety of operators, providers, users, and other parties, as well as the security interests of society. The ultimate goal of reducing or exempting certain responsibilities for AI at the regulatory level is to remove obstacles to the development of AI as much as possible and promote its further development. The above-mentioned disagreements on AI governance among countries outside the region have essentially formed a security-centered model of heavy regulation and a development-centered model emphasizing enterprise autonomy. The ultimate goal of legal intervention in AI is to maintain a balance between development and security. Therefore, in the process of governance, both development and security should be taken into account, and indicators should be reasonably set to control the intensity of supervision.

In view of the development status of generative artificial intelligence in China, in addition to controlling the use of safety principles, we should also pay attention to promoting the development progress of generative artificial intelligence and foster the sharing and innovation of artificial intelligence enterprises on the bottom line of ensuring safety. The ultimate goal of regulation is to maintain the healthy and orderly development of a new round of science and technology, including generative AI. Therefore, the country needs to uphold the concept of balanced development and security, create a market atmosphere and institutional innovation for science and technology for good, innovation, and competition, and strengthen institutional incentives and policy support for the prevention of various risks in the development of artificial intelligence.

4.2. The Requirements of the Rule of Law to Promote the Development of Generative AI

The so-called rule of law requirements refers to the substantive requirements for AI, that is, the state that generative AI should ultimately achieve through legal regulation and governance, and these requirements in turn guide the formulation and implementation of regulatory measures.

 doi:10.20944/preprints202502.1075.v1

Drawing on the principles of extraterritorial AI governance and China's current development plan, the author intends to put forward three requirements for the rule of law objectives of generative AI: security, reliability, and controllability.

4.2.1. Security

At present, there is no clear and unified meaning of safety, and some scholars believe that "safety refers to the state of a rational person's body and mind in a certain time and space from external hazards" [32] while others are more absolute, holding that "safety is an event in which no accident occurs, and an accident is an event involving accidents and unacceptable losses" [33] But in short, in the context of safety science, safety is highly related to accidents and hazards in the outside world. The U.S. Bill of Rights Blueprint defines a "safe and effective system" as "a system that should not be intentionally or reasonably foreseen to endanger the safety of you or your community." It should be designed to proactively protect you from damage caused by the accidental use or impact of automated system" [34] The purpose is to require the concept of security to be embedded in the design of AI algorithms, to provide security guarantees, and to prevent damage from occurring. That is, it believes that security should be the goal of combining the security of artificial intelligence itself with the security of the subject dimension.

Combined with the interpretation of the meaning of relevant security, in the context of China's rule of law goals, the security of artificial intelligence should have the following meanings: First, the security of artificial intelligence itself. That is, a series of processes such as data collection, desensitization, model training, and manual annotation carried out by generative AI should be "free from threat" and "without danger" to prevent the occurrence of data leakage, privacy breaches, and the dissemination of dangerous social information by the system itself. Second, the security of the subject dimension of artificial intelligence. Providers of artificial intelligence should establish a security concept training system, set encryption protection measures for databases and information systems, form a system security guarantee architecture, and assume corresponding security responsibilities. The government should provide legal guarantees for the construction of data infrastructure and the subject compliance system framework of AI, clarify the rights and responsibilities of AI providers and users, and provide a security system guarantee for the development of AI.

Of course, under the above definition of security, all its requirements should not be absolute, and it is necessary to preserve the necessary institutional responsibility space for AI providers, and establish exemption or reduction clauses in the case of force majeure and malicious attacks.

4.2.2. Reliability

Generative AI is still in the development stage, and the goal of AI governance is still under development. Reliability means that AI does not deviate from ethical and legal requirements and is able to generate decisions accurately, fairly, and safely. People are ceding some decision-making power to AI in the expectation that AI will be able to solve problems more rationally and precisely. AI should be able to overcome human irrationality, bias, and limitations, and make accurate decisions with as little bias as possible, in a way that is more in line with realistic requirements. This requires enterprises to continue to invest in R&D resources, explore and improve various AI algorithms and models, participate in open-source communities, contribute to and benefit from open-source AI projects, and also requires governments to formulate regulations on data privacy protection, algorithm transparency, ethical principles, etc., and set up special institutions or departments to supervise the development and application of AI technologies, promote technical cooperation between the public and private sectors, and support AI-related R&D and innovation.

Current realities show that the complexity and uncertainty of AI technology led to its potential flaws and errors. Although we are constantly striving for perfection in algorithms, perfection can be difficult to achieve. Therefore, we need to be grounded in reality, recognize the limitations of AI, and provide it with the space for interpretability within the framework of legal objectives.

 doi:10.20944/preprints202502.1075.v1

The reality is that AI may never be perfect, but it will always be flawed [35] The ability to produce accurate and reliable results depends on the extent to which generative AI is developed, and in terms of legal objectives, it should be given room to interpret and relevant standards updated in a timely manner.

4.2.3. Controllability

The governance of generative AI should ensure that it is controlled by humans, rather than humans being at the mercy of AI. This requires that the right to decide whether and how AI is generated should be vested in humans, whether they are providers, users, or regulators. Controllability is not a transient requirement, but a procedural one. In the regulation of controllability for language models like ChatGPT, residual risk and hierarchical management are two key concepts.

Residual risk refers to the potential risks or problems in the development and use of AI systems, despite a range of regulatory measures. In the case of ChatGPT, although it exhibits excellent performance on many tasks, there may be errors or potentially harmful outputs in some cases. These risks may include inaccurate information, misleading answers, discriminatory remarks, etc. Therefore, the existence of residual risks needs to be controlled through regulatory means.

Hierarchical management is a management approach that ensures control over the system's behavior by dividing the use and access of AI systems into different levels. Taking ChatGPT as an example, it can be managed hierarchically based on the user's identity and purpose. For example, a general user may only be able to use basic features, while a user with expertise and responsibilities may be granted a higher level of access. In this way, the risk of the system being misused or misled can be reduced, and the supervision and control of the system's behavior can be ensured.

In order to effectively manage residual risks and implement hierarchical management, taking ChatGPT as an example, the following aspects should be considered:

The first is residual risk assessment. A comprehensive residual risk assessment framework should be established to conduct a detailed risk analysis of the ChatGPT system. This includes considerations such as model weaknesses, potential bias, privacy risks, and the potential for abuse. Based on the results of the assessment, measures can be developed to mitigate the residual risks.

The second is residual risk management measures. In order to reduce residual risks, controllable supervision requires a series of management measures. This may include continuously monitoring the performance and behavior of the system, fixing vulnerabilities and defects in a timely manner, improving the diversity and balance of model training data, and establishing mechanisms for users to report issues and provide feedback.

The third is hierarchical access control. The ChatGPT system should adopt a hierarchical access control mechanism to restrict access to the system based on the user's background, purpose, and usage needs. This can be achieved through authentication, user auditing, and authorization mechanisms. Professional and trained users should be granted a higher level of access, while general users should be subject to tighter controls and restrictions.

Fourth, output auditing and filtering. To ensure the accuracy and compliance of the output, controllable supervision can establish audit and filtering mechanisms. This may include real-time checking, screening, and correction of generated responses to remove misleading, offensive, or inappropriate content. At the same time, mechanisms for user feedback and complaints should be encouraged to further improve the output quality and compliance of the system.

5. The Practical Frameworks for the Facilitation of Development of Generative AI

At present, the "Interim Measures" jointly issued by the Cyberspace Administration of China and other seven departments are the first departmental regulations in China to govern generative artificial intelligence. These measures condense the multi-dimensional evaluation of the risks caused by current generative artificial intelligence and put forward governance requirements in terms of pre-

 doi:10.20944/preprints202502.1075.v1

prevention, regulation, and relief during and after the event. Based on the above-mentioned risks in legal norms, social governance, and science and technology ethics, combined with the experience of extraterritorial governance, and under the guidance of the concept and goal of the rule of law, the following interpretations and prospects are made to improve the legal guarantee of generative AI and promote the further implementation of the Interim Measures.

5.1. Strengthen the Supply of Regulatory Institutions

5.1.1. System Design with Safety as the Bottom Line

(1) Complete the regime of ex-ante censorship

Article 17 of the Interim Measures stipulates that "those who provide generative AI services with public opinion attributes or social mobilization capabilities shall carry out security assessments in accordance with relevant national regulations and perform algorithm filing, modification, and cancellation formalities in accordance with the Provisions on the Administration of Algorithmic Recommendations for Internet Information Services." That is, some specific generative AI products need to undergo security assessment and algorithm filing before they are released. Increasing ex-ante review can not only improve the legitimacy of using generative AI products to provide services to the public and increase their credibility, such as safety, reliability, explainability, and accountability, but also help to better realize the inclusiveness of AI products and technologies, prevent risks more effectively, ensure safety, and promptly identify problems in their operating procedures and service content, thereby improving the acceptability of generative AI products for public service.

Of course, it must also be recognized that ex-ante review will increase the compliance cost of enterprises to a certain extent, and if the scope of the ex-ante review is not properly set, it may inhibit the R&D and training efficiency of generative AI products, objectively leading to a slowdown in the development of generative AI. In other words, if the scope of prior review is too large, it will lead to an increase in the cost of enterprise review. Clarifying the scope and methods of review can encourage and guide enterprises to self-examine, promote enterprises to standardize the application of generative AI, and, on the other hand, reduce the possibility of risks and avoid adverse effects.

(2) Detail the content of disclosure information

Paragraph 1 of Article 19 of the Interim Measures stipulates: "The relevant competent authorities shall supervise and inspect generative AI services in accordance with their duties, and the providers shall cooperate in accordance with the law, explain the source, scale, type, labeling rules, algorithm mechanism, etc. of the training data as required, and provide necessary technical and data support and assistance." In fact, this regulation puts forward new requirements for the transparency of generative AI algorithms, so that the protection of privacy and personal information is no longer limited to passive, after-the-fact remedies. With the protection chains moving forward, more active and effective standardization of the AI training process will help enhance user trust and enable the better development of generative AI products.

It is important to note that the pursuit of absolute transparency is not desirable for the development of generative AI and is not in line with the basic position of the state to support and encourage innovation. Therefore, on the basis of the Administrative Measures for Generative AI Services (Draft for Comments) (hereinafter referred to as the "Consultation Paper"), the Interim Measures add the confidentiality obligations of relevant institutions and personnel involved in the security assessment, supervision, and inspection of generative AI services to state secrets, trade secrets, personal privacy, and personal information, balancing the tension between the protection and supervision of AI innovation.

In practice, the extent and limits of disclosure should be further clarified to avoid unreasonable requirements that force the disclosure of key information of generative AI algorithms, resulting in the disclosure of technical secrets of enterprises and irreparable losses to the innovation and development of enterprises. In addition, the disclosure of copyrighted data is also closely related to data scraping infringement. At present, the act of crawling copyrighted works is quite controversial,

 doi:10.20944/preprints202502.1075.v1

and some scholars believe that this kind of crawling should be regarded as falling under the applicable scope of the fair use rule, and it should be given the status of unconditional crawling [36] Some scholars believe that the interests of copyright holders and AI service providers can be balanced through statutory licensing and collective management systems [37] The majority of scholars still hope to grant an exemption for the development of artificial intelligence to crawl others' copyrighted data, but it is still necessary to pay attention to protecting the legitimate interests of copyright holders. The path of protection can be balanced by refining the disclosure obligation and allowing copyright owners to claim without crawling or requiring removal.

(3) Concretize the obligation of information accuracy

Although Article 4 of the previous Draft for Comments stipulates that the content generated by generative AI should be true and accurate, from the perspective of current mainstream technology, generative AI cannot distinguish the authenticity of content like humans, so it is the obligation of the provider to make the content generated by generative AI true and accurate, which means that domestic generative AI providers must meet the obligation through manual review. This will affect the efficiency of generative AI operations and generated content, greatly reducing the consumer user experience, and will also greatly increase the burden on businesses, spending a lot of human and technical resources on reviewing information.

With this in mind, in the officially released Interim Measures, the obligation to ensure accurate information has been revised to "take effective measures to improve the transparency of generative AI services and improve the accuracy and reliability of generated content based on the characteristics of the type of service".

(4) Strengthen the guarantee of data security

In the chapter on "Technology Development and Governance," the Interim Measures propose the establishment of a public training data resource platform, and at the same time, stipulate that generative AI service providers should ensure the legitimacy of data sources. Data security is the underlying requirement of digital technology, including generative AI technology, especially public data with rich dimensions, wide-use scenarios, and many user subjects. Preventing data risks is key to ensuring the coexistence of generative AI development and security. It is necessary to combine the characteristics and functions of the data required by the underlying technology of generative AI to establish and improve the data classification and hierarchical protection system, such as the classification and management of data in the training database.

First, data can be classified based on the data subject, such as personal data, enterprise data, government data, etc. Secondly, the data can be classified according to the degree of data processing, including raw data, processed data, derived data, etc. In addition, the right attributes of data can also be considered, such as personal privacy data, trade secret data, public data, etc. Also, we can integrate into account the effective classification and management of data.

On the basis of data classification and grading, data protection standards and sharing mechanisms should be established that match the data type and security level. This means that different types of data and levels of security should be protected accordingly. At the same time, in order to promote the sharing and rational use of data, it is necessary to develop corresponding data sharing mechanisms to ensure that data can be shared legally and effectively under the premise of meeting privacy and security needs.

In addition, generative AI also involves the cross-border flow of data, and reasonable cross-border data security law enforcement rules should be formulated on the basis of considering international standards and practices. The convergence with rules of other countries and regions should be strengthened to promote cross-border law enforcement cooperation on data security. By establishing a cross-border data security law enforcement cooperation mechanism, international information sharing and collaboration can be strengthened to jointly address cross-border data security challenges [38]

In summary, to ensure data security, data subjects, data processing degrees, data rights attributes, etc., should be considered in the data classification and hierarchical protection system.

 doi:10.20944/preprints202502.1075.v1

Data protection standards and sharing mechanisms should be established that match the data type and security level, and reasonable cross-border data security law enforcement rules should be formulated to strengthen international cooperation and promote the sustainable development and application of digital technology.

5.1.2. Policy Supports as Oriented to Development

(1) Overall policy support

Objectively speaking, there is a lag in the development of generative AI technology in China [39] Although China has put forward the slogan of "leading artificial intelligence," the corresponding hardware conditions and soft support have not been put in place in time. Although the explosion of generative AI in this round is due to the update of training architecture and models, it is essentially the improvement of computing power that has led to the improvement and development of related technologies. It could even be argued that the risks of generative AI can be greatly reduced if there is enough computing power, because the amount of computation and training it can carry, as well as the human standards, can be developed on a large scale.

In fact, only by independently developing artificial intelligence, mastering core technologies, and advancing artificial intelligence technology ahead of the world's artificial intelligence technology, can artificial intelligence governance truly develop independently. The independent development of generative AI will inevitably involve long-term, wide-ranging, and in-depth scientific and technological innovation, which is an arduous task that cannot be accomplished by any individual or organization alone [40] For this reason, it should be at the bottom of the safety zone to promote development above the line and provide policy incentives for the improvement of generative AI computing power, data, and other technologies. At present, the Interim Measures mainly follow the principles of attaching equal importance to development and security, promoting innovation and governing according to law, and make provisions in terms of encouraging the R&D and application innovation of generative AI and the requirements for generative AI technology itself. In terms of supporting application and promotion, industry-university-research collaboration, independent innovation, international cooperation, infrastructure, and the construction of public training data resource platforms, the state's support and encouragement measures for generative AI are refined, which fully reflects the state's support for the artificial intelligence industry. The openness, sharing, and improvement of data, algorithms, and models should be further taken as the starting point to build a more solid technical and resource foundation for the development of generative AI enterprises, give full play to the role of a service-oriented government, and promote sharing and cooperation among enterprises.

(2) Pilot regulatory sandbox

The regulatory sandbox is a pilot model of regulatory policies first applied to the field of financial supervision. It specifically refers to the promotion of regional financial innovation and financial technology development, where financial regulatory authorities allow some licensed financial institutions or start-up technology enterprises to test new financial products, new financial models, or new business processes within a certain time and limited scope, while lowering the entry threshold for the test projects or deregulating regulatory restrictions [41] However, the current regulatory boundaries of generative AI are blurred, and many risks have not yet been clearly determined, which has certain similarities with financial development supervision, so it has reference significance.

On the one hand, through the regulatory sandbox, law enforcement agencies can pilot relevant regulatory measures in advance, provide early warning of possible risks, and fully address the problem of information asymmetry. Concentrating regulatory resources to fully communicate with the enterprises in the sandbox improves the quality of supervision, avoids the occurrence of "one tube and die," and then promotes and applies the verified and effective regulatory plan when the time is ripe. On the other hand, enterprises in the regulatory sandbox can fully communicate with regulators, provide feedback on the current status of technical practices, and participate in the formulation of

 doi:10.20944/preprints202502.1075.v1

regulatory boundaries for generative AI, so that the regulatory plan aligns with the development goals of the enterprise.

5.2. Establish a Multi-Faceted and Long-Term Regulatory Mechanism

The life of the system lies in the implementation, and the efficient implementation of the regulatory system and rules needs to be strengthened, and the implementation of the generative AI regulatory system needs to establish a diversified and long-term regulatory mechanism.

5.2.1. Replenish Provisions to Verify the Rectification and Optimization Methods

The Consultation Paper stipulates that for the generated content that is found and reported to be non-compliant, in addition to measures such as content filtering, it shall be prevented from being regenerated within three months through model optimization and training. The regulations address the key issues of generative AI and enrich and improve the handling of generative AI violations. In the officially promulgated "Interim Measures," this article was deleted due to the lack of operability of the provision.

In fact, if the legal provisions or practice departments can supplement the verification of the ways and means of rectification and optimization, the generative AI violation handling process will be improved. The verification of the results of rectification and optimization should be implemented in technical practice, supplemented by regulatory guarantees. It is necessary to set the basic threshold for the use of technology, coupled with regular and irregular monitoring, to ensure the safety and credibility of its rectification and optimization results. After the optimization and rectification, it can be used to check whether there is still non-compliant generated content after rectification and optimization by means of manual testing and simulation and setting up a regulatory transition period.

5.2.2. Rationalize Allocations on the Cost of Generative AI Regulation

Due to the large variety and scale of generative AI, and the limited regulatory resources of the government, the allocation of regulatory resources should be optimized, and the regulatory authorities should set different regulatory costs according to the scale and business activities of different generative AI service operators.

On the basis of cost-effectiveness, the regulator establishes the criteria for incurring costs and determines the costs that the regulator needs to pay in the course of carrying out its mandate. At the same time, the fee standards should be reviewed and updated regularly to improve the efficiency and transparency of supervision and ensure the reasonableness and fairness of the fees. According to the characteristics of the supervised objects and the different tasks of supervision, the supervised objects should be divided into different categories, and different regulatory fee standards should be formulated according to the different categories of supervised objects. In addition, it is also necessary to introduce market competition factors to carry out certain market-oriented competition for generative AI service providers, and achieve the purpose of reducing costs through price comparison. At the same time, the regulatory process should be optimized, and more efficient and convenient management methods and technical tools should be adopted to improve regulatory efficiency and reduce costs.

The implementation of this idea requires a clear premise: that is, it is necessary to fully understand and recognize the risks of AI systems, and to this end, it is necessary to improve the filing and review system of relevant information technology and data resources, and strengthen the government's technical supervision to improve the regulatory capacity and efficiency.

5.2.3. Pay Attention to the Digitization of Rule of Law Supervision

In the next step of regulatory capacity building, attention should be paid to the further integration of rule of law supervision and digital technology. Specifically, policymakers should turn

 doi:10.20944/preprints202502.1075.v1

their focus from regulating the code and the results of generative AI algorithms to the code and the algorithm process itself. That is, by converting legal rules into code, and using code to regulate the "legal technicalization" of code, and the "technical legalization" of industry rules that attach importance to "code is law."

In the technologization of law, legal rules are transformed into machine-readable forms so that computer systems can understand and enforce them. Through technical means, the subjectivity and uncertainty of artificial interpretation and operation of legal rules have been eliminated, and the predictability and consistency of laws have been improved. Legal rules can be more easily communicated, understood, and applied, reducing the potential for human error and disputes. Such an approach could strengthen industry regulation and self-regulation of generative AI, providing greater transparency and credibility to its applications. Therefore, the use of automation technology to counter the risk generated by automation should become the mainstream of supervision in the digital era, so it is necessary to further strengthen the construction of digital government and improve the supervision ability of government digitalization.

5.2.4. Give Full Play to the Regulatory Role of Enterprises and Users

Enterprises are more motivated to implement safety supervision. For example, there is a technical term for discriminatory language, hate speech, and insulting speech called toxicity. In fact, people in the scientific and technological circles are more concerned about this issue than legal professionals, and once large-scale language model products are exposed to this toxicity—often generating content that contains insults and discriminatory tendencies—the products will be boycotted by the public, which will directly affect commercial interests [42] As manufacturers and providers of generative AI, enterprises are also more capable of verifying whether their products have legal and social risks at the institutional level. Therefore, at the level of enterprise system implementation, enterprises should improve the construction of self-examination systems and increase the intensity of self-examination.

On the one hand, it is necessary to strengthen users' awareness of self-protection, increase reporting and review channels for user supervision, let users know and understand the generative process of generative AI, and lay relevant policy and institutional foundations for strengthening users' trust. On the other hand, users are also an important training nourishment for generative AI. The requirements for users' moral and ethical risks should be strengthened, the ethical rules and requirements for product use should be clarified to users, and the channels for obtaining illegal information by artificial intelligence should be prevented from the source level.

5.3. Clarify and Refine the Responsibility System

Paragraph 1 of Article 9 of the Interim Measures provides detailed provisions for the responsible entity: "The provider shall bear the responsibility of the producer of network information content in accordance with the law and perform the obligation of network information security." When personal information is involved, the provider must bear the responsibility of personal information processors in accordance with the law and perform personal information protection obligations. This provision is, in effect, a designation of the producer of generated content. If the provider of generative AI products is the producer of the generated content, the producer here is responsible for the entire generation process, such as the process of generating the content, the authenticity of the specific data information, and the appropriateness of the use of the algorithm. In such cases, the provider should, of course, be held responsible. However, if the user of the product deliberately induces the production of relevant false information, illegal information, or infringing information, the user should be regarded as the content producer and bear legal responsibility for the relevant infringement and illegal acts.

In view of the similarity between the current situation of generative AI and Internet information service providers, the scope of liability of the provider should be reasonably set with reference to the "safe harbor" principle, and the reasons for the provider's exemption should be clarified in

 doi:10.20944/preprints202502.1075.v1

combination with the characteristics of generative AI. Specifically, if the provider fulfills the corresponding duty of care, in terms of liability, given its contribution to innovation and development, it is not appropriate to impose strict liability. Otherwise, this would not be conducive to the development and future commercialization of the technology [43]

How to determine whether the provider has fulfilled its duty of care should be distinguished based on the nature of the content it produces. First, despite the technical difficulties, the provider has the ability to control whether the content produced complies with the four basic principles, whether it is suspected of racial discrimination, and whether it is transmitting or sowing cults. This is not only a reality but should also be an expectation [44] Therefore, when such content violates the bottom line, the provider should be directly responsible for it, and there should be no reason to exempt it from liability. Second, when generating general infringing content, the "safe harbor" principle should be used as the standard approach. Since generative AI is even more autonomous than traditional Internet information service providers, and traditional information service providers can still apply the "safe harbor" principle, generative AI providers should also apply it. That is, they should only bear tort liability in the case of failure to delete and notify users to delete relevant content in a timely manner.

Finally, since generative AI generates content in a dynamic rather than static way, the way of responsibility should be to remove the generated content or make a promise that the same content will not appear again [45] There is controversy at present, and this should be discussed on a case-by-case basis. For high-risk generated content, it should be required to commit to not having "the same" or "similar" content again, which is not only within its competence but should also be within its responsibility. For non-high-risk content, the "safe harbor" rule should be applied first, after clarifying the specific meaning of the "notice-takedown" rule in AI scenarios, provided that the "safe harbor" rule can be applied.

It can be argued that the "notice-takedown" under the "safe harbor" rule should be understood as the self-removal of existing content and the notification to the user to delete the generated content. If the user believes there is no infringement or if the provider determines on its own initiative, the relevant content can be restored. It should not be construed as a commitment at this time. However, if it is finally determined that the generated content is infringing, the provider who made the deletion, notified the deletion, and did not restore it on its own shall not be liable, and the user who refuses to delete it or the provider who restores it on its own shall be liable. In such cases, the manner in which the provider assumes responsibility should be undertaken in light of the efforts made by the provider and the current state of technological development and cost considerations, in the form of a commitment not to repeat the "same" content.

On the one hand, this is because the content generated by generative AI is not publicly available, does not remain on a public platform, and is sometimes treated as private information between the provider and the user. On the other hand, the "similar" promise is too broad and vague in scope, and with the current stage of generative AI development, there is no need to bear such an onerous liability for general infringement. Of course, with the development of technology, if the verification path can be reduced to a reasonable cost, this part of the responsibility should gradually change from a "same" to a "similar" commitment. In addition, regarding whether the operating company needs to bear the corresponding supplementary liability, the scope of the infringement, the degree of damage, and the platform's ability to prevent the expansion of losses should be comprehensively considered.

6. Conclusions

The innovation and development of generative AI technologies and products are on the rise, and the legislative system should be gradual and based on the premise of clear information and sufficient evidence, so as to avoid unduly hindering the development of emerging technologies. It is also necessary to regulate in a timely manner to prevent the occurrence of large-scale social risks and irreversible damage. Balancing the relationship between the two is an important mission for legal researchers, so it is necessary to fully summarize the current risks, examine the existing regulatory

 doi:10.20944/preprints202502.1075.v1

situation, uphold a reasonable concept and goal of the rule of law, and respond to and optimize the legal supervision of generative AI from the perspective of strengthening system supply, establishing a long-term supervision mechanism, and improving responsibility, so as to effectively promote the balance between the safe application of AI and innovative development. For example, in the field of generative artificial intelligence technology and product development, where there is still a lot of room for development and the technology is still to be developed, there is still a certain amount of flexibility at the legal and policy level, and the setting of various obligations needs to be considered scientifically and carefully.

Author Contributions: Conceptualization, methodology, writing-original draft preparation, project administration, funding acquisition, data curation, writing-review and editing, B. C.

Funding: This research was funded by the.

Data Availability Statement: All data underlying the results are available as part of the article and no additional source data are required.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhu Xiaohang, "Italy Announces Ban on ChatGPT," China Economic Net, http://intl.ce.cn/qqss/202304/03/t20230403_ 38476962.shtm-l?utm_source=UfqiNews, accessed on April 28, 2023. It should be noted that the report on Italy's "ban" on ChatGPT refers to the authorities issuing a "ban," which strictly speaking, was a temporary injunction, and ChatGPT has since been restored for use.
2. Zhang Xin, "From Algorithm Crisis to Algorithm Trust: Multiple Schemes and Localization Paths of Algorithm Governance", Journal of East China University of Political Science and Law, No. 6, 2019.
3. Han Dayuan, "The Constitutional Boundaries of Contemporary Science and Technology Development", Research on the Modernization of the Rule of Law, No. 5, 2018.
4. See Andersen v. Stability AI Ltd., January 13, 2023.
5. Lin Xiuqin, "The Reshaping of the Copyright Fair Use System in the Era of Artificial Intelligence", Legal Research, No. 6, 2021.
6. Ma Zhongfa and Xiao Yulu, "The Infringement Dilemma and Way Out of Artificial Intelligence Learning and Creation", Wuling Academic Journal, No. 5, 2019.
7. Yang Lihua, "Exploration of the Copyright Issues of Artificial Intelligence Generated Materials", Modern Legal Science, No. 4, 2021.
8. Zhou Xin, "Challenges and Countermeasures of Artificial Intelligence to the Traditional Civil Liability System", Rule of Law Forum, No. 3, 2021.
9. Pei Chenwei and Wu Chunxin, "The copyright of AI-generated content is not clearly defined", Science and Technology Daily, June 19, 2023, page 2.
10. Chen Bing, "Building a Scientific and Prudent Rule of Law Framework for the High-quality Development of AIGC", China Business News, April 19, 2023, page A11; Chen Bing, "Facing the Crisis of Trust in Artificial Intelligence and Accelerating the Development of Trusted AIGC", China Business News, April 25, 2023, page A11
11. Zheng Zhifeng, "Privacy Protection in the Age of Artificial Intelligence," Legal Science (Journal of Northwest University of Political Science and Law), 2019,No. 2.
12. Product safety standards, https://openai.com/safety-standards.
13. March 20 ChatGPT outage: Here's what happened，https://openai.com/blog/march-20-Chatgpt-outage.
14. Matthew Sindman: *The Myth of Digital Democracy*, Princeton, NJ : Princeton University Press, 2008.
15. Ma Changshan, "The Social Risks of Artificial Intelligence and Its Legal Regulation", Legal Science (Journal of Northwest University of Political Science and Law), No. 6, 2018.
16. Fan Chunliang, "Theory and Practice of Ethical Governance of Science and Technology", Science and Society, No. 4, 2021.
17. Gu Haibo, "AI-Generated Image Wins Sony World Photography Award," Youth Reference, April 28, 2023, 5th edition.

 doi:10.20944/preprints202502.1075.v1

18. Zhao Zhiyun, Xu Feng, Gao Fang, et al., "Some Understandings on the Ethical Risks of Artificial Intelligence", China Soft Science, No. 6, 2021.
19. Feng Jie, "Jurisprudence Reflection on the Legal Subject Status of Artificial Intelligence Body", Oriental Jurisprudence, No. 4, 2019.
20. Yu Xue and Duan Weiwen, "The Ethical Construction of Artificial Intelligence", Theoretical Exploration, No. 6, 2019.
21. Ministry of Civil Affairs of the People's Republic of China, "Statement on Cautioning Against Illegal Activities Involving the Forgery of Ministry of Civil Affairs Documents and Other Violations", https://www.mca.gov.cn/ article/xw/mzyw/202303/20230300046804.shtml?site=elder, accessed on April 28, 2023.
22. Eric Bryan Joferson and Andrew McAfee, "The Second Machine Revolution: How Digital Technology Will Change Our Economy and Society", translated by Jiang Yongjun, CITIC Press, 2016, p. 340.
23. Roman V. Janpolsky, Otto Barten, "ChatGPT and Other Language Models May Pose Existential Risks", translated by Wang Youran, China Social Science News, March 6, 2023 8th Edition.
24. Yuan Kang, "Legal Regulation of Trusted Algorithms", Oriental Jurisprudence, No. 3, 2021.
25. Zeng Xiong, Liang Zheng and Zhang Hui, "The Regulatory Path of Artificial Intelligence in the European Union and Its Enlightenment to China: Taking the Artificial Intelligence Act as the Object of Analysis", E-Government, No. 9, 2022.
26. Fang Xu, Wei Yan, Zhang Ying, Wang Xiaosa, Sun Linxiao, Xu Lei, "Overview of the EU Artificial Intelligence Act", Computer Times, No. 5, 2022.
27. European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts -General approach (6 December 2022), See https://data.consilium.europa.eu/doc/document/ST-15698-2022-INIT/EN/pdf.
28. Op. cit. [XXV]
29. The Blueprint for an AI Bill of Rights: Making Automated Systems Work for The American People, https://www.white- house.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.
30. Chen Jinghui, "Legal Attitude in the Face of Genetically Modified Issues: How Should Legal Persons Think About Scientific Issues", Law Science, No. 9, 2015.
31. Chen Jinghui, "The Doctrinalization of Departmental Law and Its Limits", China Law Review, No. 3, 2018.
32. Wu Chao, Yang Mian, Wang Bing: "The Scientific Definition of Security and Its Implications, Extensions, and Inferences," Journal of Zhengzhou University (Engineering Edition), 2018, No. 3.
33. Leveson N. A new accident model for engineering safer systems. Safety Science,2004,42(4):237-270.
34. The Blueprint for an AI Bill of Rights: Making Automated Systems Work for The American People, https://www.white- house.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.
35. Op. cit. [XXIV], Yuan Kangwen.
36. Jiao Heping, "Copyright Risks and Mitigation Paths for Data Acquisition and Utilization in Artificial Intelligence Creation", Contemporary Legal Science, No. 4, 2022; Zhang Jinping, "The Fair Use Dilemma of Artificial Intelligence Works and Its Solution", Global Law Review, Issue 3, 2019
37. op. cit. [VI], Ma Zhongfa and Xiao Yu Luwen
38. Chen Bing and Ma Xianru, "The Governance Dilemma and Rule of Law Response to Cross-border Data Flow under the System Concept", Journal of Anhui University (Philosophy and Society Edition), No. 2, 2023
39. Chen Yongwei, "Beyond ChatGPT: Opportunities, Risks and Challenges of Generative AI", Journal of Shandong University (Philosophy and Social Science Edition), No. 3, 2023.
40. Pu Qingping and Yearning, "Generative Artificial Intelligence: The Transformative Impact, Risks, Challenges and Coping Strategies of ChatGPT", Journal of Chongqing University (Social Science Edition), No. 3, 2023.
41. Zhang Jingzhi, "The International Model of the "Regulatory Sandbox" and the Development Path of Chinese Mainland", Financial Supervision Research, No. 5, 2017.

 doi:10.20944/preprints202502.1075.v1

42. Yu Xingzhong, Zheng Ge, Ding Xiaodong, "Six Issues of Generative Artificial Intelligence and Law: A Case Study of ChatGPT", China Law Review, No.2, 2023
43. Op. cit. [X] , Chen Bingwen, "Building a Scientific and Prudent Legal Framework for the High-quality Development of AIGC".
44. Xu Wei, "On the Legal Status and Responsibilities of Generative AI Service Providers: A Case Study of ChatGPT", Legal Science (Journal of Northwest University of Political Science and Law), No. 4, 2023.
45. Kacy Popye, Cache-22: The Fine Line Between Information And Defamation In Google's Autocomplete Function, Car- dozo Arts and Entertainment Law Journal, Vol.34:835, p.841(2016).