International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 7 Issue 6, November-December 2023 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Legal Risks and Preventive Measures in ChatGPT Applications

Chen Jiaqi, Zhen Yunuo, Guo Simeng

Beijing Wuzi University, Beijing, China

ABSTRACT

In November 2020, OpenAI officially launched their new generation of generative artificial intelligence, ChatGPT, based on large language models. ChatGPT garnered the attention and usage of over a billion people in less than two months, making it the fastest consumer-level application to reach this milestone. As a generative AI, ChatGPT not only achieved remarkable success in the market but also contributed to the advancements in the field of generative AI, with its representation of 2022's top ten scientific breakthroughs in the international reputable journal, "Science."

Generative artificial intelligence is having a profound impact on our lives and work, with one of the most critical aspects being its algorithms. These algorithms directly influence the learning performance of the entire intelligent system and the quality of recommendations. However, with the widespread application of algorithms and the continuous evolution of artificial intelligence, a series of regulatory and management issues have arisen. Many countries worldwide are continually strengthening algorithm oversight to ensure transparency, fairness, and security. This project, part of a university student innovation training program, will primarily focus on researching personal information security risks among the potential risks associated with generative artificial intelligence. The following will provide an introduction to what generative artificial intelligence is, the personal information security risks and preventive measures involved in generative artificial intelligence.

How to cite this paper: Chen Jiaqi | Zhen Yunuo | Guo Simeng "Legal Risks and Preventive Measures in ChatGPT Applications" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-7 | Issue-6, December 2023, pp.83-86, URL: www.ijtsrd.com/papers/ijtsrd60109.pdf

IJTSRD60109

KEYWORDS: *ChatGPT; Generative artificial intelligence; Legal risks*

1. What is Generative Artificial Intelligence

Generative Artificial Intelligence is a type of artificial intelligence technology that can create new content in the form of text, images, music, and videos. A typical example of generative artificial intelligence is chatbots, which can generate dialogue text similar to humans and have gained popularity worldwide. They can express complex ideas synthesized from the vast amount of information they have been trained on. In the business domain, they can assist in composing or enhancing emails and presentations, aid in brainstorming new marketing campaigns, and more. Generative artificial intelligence relies on machine learning models that mimic the human neural network, a concept dating back to early artificial intelligence research. Key algorithms developed in the 1980s propelled the advancement of this field, and in recent years, the emergence of new training algorithms and dedicated processing units has further accelerated its progress, along with improved training datasets. These developments have given rise to the systems we use today, resulting in generative artificial intelligence models that seem capable of creative output beyond imagination, much like humans. With businesses worldwide experimenting with generative AI and entrepreneurs and investors introducing new business concepts based on it, innovation in generative artificial intelligence is rapidly advancing at an astonishing pace. Generative artificial intelligence has ushered in a new technological era, offering the potential not only to enhance productivity but also to address business problems in entirely new ways that were previously unattainable.

2. Personal information security risks involved in generative artificial intelligence

The dynamic utilization of data, algorithmic mechanisms, and generative attributes in generative artificial intelligence determine its multi-stage personal information security risk.

A. The issue of personal information leakage

In today's digital age, we are entering an era where issues of cybersecurity are closely intertwined with each individual. Therefore, the governance of cybersecurity is becoming increasingly urgent. In the following, this research will elaborate on the subject from three aspects: data, algorithms, and generative content in the context of Generative Artificial Intelligence (GAI).

Firstly, during the pre-training phase, a series of GAI models like ChatGPT collect vast amounts of data, which often involves data collection practices that are not entirely legal or compliant with regulations. It appears to deviate from the norm and contradicts the principle of informed consent stipulated by the "Personal Information Protection Law." Meanwhile, the collection of personal information through web scraping techniques may potentially violate Article 27 of China's "Cybersecurity Law," which prohibits the unauthorized acquisition of personal information, and in more severe cases, may constitute the crime of infringing upon citizens' personal information.

During the operational phase, major application platforms require users to agree to their privacy agreements before logging in or registering. While this may appear to grant rights to customers, it is, in fact, a coercive tactic employed by the application platforms. If users refuse to accept the privacy agreement set by these platforms, they cannot access the complete services and are compelled to agree. The collection of personal privacy information fundamentally represents improper data collection from users.

Lastly, during the content generation phase, OpenAI's privacy policy statement indicates that when users interact with the application, the questions posed and the content generated by the application will be stored in some form, and data will be automatically collected. The process of users conversing with the application is essentially the process of automatic data collection. In this process, users' personal information may be collected again in a generated form by the application, and this behavior is not clearly and explicitly communicated to the user before usage.

B. Problems in Protecting Personal Information in the Development of Generative Artificial Intelligence

a. Chinese Legal Provisions on Generative Artificial Intelligence

Currently, in China, regulations related to artificial intelligence are scattered throughout various laws such as the "Cybersecurity Law," "Data Security Law," "E-commerce Law," "Personal Information Protection Law," "Antitrust Law," "Anti-Unfair Competition Law," as well as normative documents like the "Anti-Monopoly Guidelines for the Platform Economy."

As a result, the dispersed nature of legal provisions concerning artificial intelligence has given rise to a series of issues. Firstly, the relevant legal regulations on artificial intelligence lack specialization and specificity. Various laws related to artificial intelligence lack cohesion, while the risks associated with generative artificial intelligence algorithms are complex. The effectiveness of these laws and legal documents is not consistent, making them challenging to manage and standardize.

Moreover, there is a limited number of regulations in China concerning artificial intelligence, which leads to insufficient detail and relatively coarse content in the management and regulation of generative artificial intelligence. This could potentially provide opportunities for unlawful actors, causing generative artificial intelligence to deviate from its intended course. As generative artificial intelligence continues to develop, there is a growing need for specialized legislation to govern it.

b. EU Legal Provisions on Generative Artificial Intelligence

In the European Union, current discussions regarding AI legislation tend to focus more on traditional AI rather than specifically addressing legislation for generative AI. However, overall, the EU region is at the forefront of AI and related legislation, using regulation to drive the development of artificial intelligence. Additionally, certain regions within the EU place significant emphasis on the protection of personal information and have taken appropriate measures to address the risks associated with ChatGPT.

c. Laws and regulations in the United States regarding generative artificial intelligence.

The United States was the first to explore artificial intelligence and is also the birthplace of ChatGPT. In order to maintain its leading position in the field of artificial intelligence, the United States has made various legislative efforts in this area. In May 2020, the United States released the "Generative Artificial Intelligence Network Security Act" specifically related to generative artificial intelligence. On April 13, 2023, the United States issued a notice for soliciting opinions on AI accountability policies, which included issues related to the prevention and control of generative content in generative artificial intelligence. In May 2023, based on the current state of artificial intelligence development, the White House updated and released the "Artificial

Intelligence Research and Development Strategy Plan: 2023 Update." It is evident that the United States has relatively advanced and targeted legislation in the field of artificial intelligence.

d. Laws and regulations regarding generative artificial intelligence in other countries and regions.

While there are currently fewer legal provisions regarding generative artificial intelligence in other countries and regions, measures have been taken in response, thanks to the development and promotion of ChatGPT. These measures include actions related to the protection of personal information.

3. Preventive measures against personal information leakage in generative artificial intelligence.

To prevent personal information leaks, strategies can be pursued in both legislative and practical dimensions.

At the legislative level, it is important to establish specialized and comprehensive regulations specifically designed for generative artificial intelligence, thus enhancing the legal framework governing generative artificial intelligence. In addition to enacting dedicated laws in China, it is crucial to align with international standards. Active participation in international cooperation is required to develop unified standards through collaboration with other countries and organizations. This collaborative effort aims to collectively research international standards and best practices for algorithm governance. An international cooperation mechanism should be established to promote consensus and mutual recognition in algorithm governance regulations and facilitate the coordinated development of a global algorithm governance system.

To prevent and regulate various legal risks associated with generative artificial intelligence (AI) and establish a legal framework for it, we should encourage innovation and prioritize risk prevention over punitive measures. In the Knowledge Property and Digital Economic Development Forum on July 6, 2023, and the Legal Forum of the 2023 World Artificial Intelligence Conference on July 7, Wang Liming shared his views on the topic of infringement by generative AI.

Wang Liming summarized that with regards to the infringement of personal information by generative AI, it has not yet completely exceeded the provisions of the Civil Code and the Personal Information Protection Law. Existing laws and regulations still have some applicability. However, he also emphasized that this does not mean that the existing laws are sufficient, and there is a need to establish relevant compliance standards.

Wang Liming suggests that when the conditions are ripe in the future, it is necessary to effectively address the various infringement risks caused by generative AI through special legislation in order to better protect the legitimate rights and interests of civil organizations and promote the healthy development of the artificial intelligence industry.

By enacting clear legislation to regulate the issue of personal information leakage in generative artificial intelligence, the subject of infringement in generative AI is different from traditional and online infringement behaviors. This is because generative AI is provided to specific users, so the infringement itself is not public, and there are no large-scale direct infringements on personal and property rights. Instead, it mainly infringes on personal rights and intellectual property. However, one should not lower their guard just because the mode of infringement is different, as this type of infringement may pose significant legal risks. Generative AI may generate false images, videos, and information, and once these false information spreads widely, it can cause significant infringement of rights and interests, such as personal rights, for individuals in society and even lead to serious societal problems. Therefore, it is essential to strictly manage the sources of data collection, ensuring that data collection and usage are legal and compliant, and establishing a tiered data governance system.

In terms of the responsibility and regulatory framework, current law does not recognize artificial intelligence as having independent personhood. Generally, the responsibility for AI lies with its creators, designers, and users. As a result, the issue of AI responsibility is relatively complex. It can arise due to the negligence of service providers, leading to data breaches and the generation of false information. It can also occur when users intentionally induce the generation of false information during usage. Additionally, inherent defects in generative AI production can pose infringement risks. Furthermore, joint wrongdoing by users and service providers can also lead to infringement.

Therefore, it is necessary to enhance the legal framework for responsibility, distinguishing different scenarios to clarify the responsibilities of various entities and refine the responsibility allocation system. This includes differentiating the responsibilities of platforms and users to avoid unnecessary liability issues. Additionally, it is important to strengthen regulatory and enforcement capabilities. According to Article 19 of the "Interim Measures for the Management of Generative Artificial Intelligence Services," relevant competent authorities shall conduct supervision and inspections of generative AI services in accordance with their duties. Service providers must cooperate in accordance with the law, provide explanations regarding the source, scale, type, labeling rules, algorithm mechanisms, and other aspects of training data, and offer necessary technical support and assistance. Organizations and individuals participating in the security assessment and supervision of generative AI services shall, in accordance with the law, keep national secrets, trade secrets, personal privacy, and personal information confidential, and shall not disclose or illegally provide them to others.

Therefore, it is necessary to establish a robust regulatory mechanism and enforcement system, strengthen the supervision and enforcement of the algorithm registration system. Enhance the technical capabilities of regulatory authorities, improve their ability to review and assess algorithms, and ensure the effective implementation and execution of the registration system.

On a practical level, administrative agencies should enhance their oversight, clarify the allocation of responsibilities and management. Strengthen the collaborative efforts of the Ministry of Industry and Information Technology, the State Administration for Market Regulation, and the National Big Data Bureau to achieve coordinated and unified systematic, data-driven, and penetrative regulation. Severe action should be taken against infringements, and any violations of public order and good morals or legal regulations in generative artificial intelligence should be rigorously addressed and rectified. In cases where public opinion and public interests are compromised, relevant authorities should offer swift, precise, and decisive solutions. Real-time monitoring of generative artificial intelligence application companies and software companies is essential, with rigorous scrutiny by technical departments, and timely warnings issued in case of problems and anticipated potential risks.

4. Conclusion

Finally, in the development stage of generative artificial intelligence, the preventive measures taken are aimed at preventing risks rather than suppressing the development of generative artificial intelligence. The preventive measures for generative artificial intelligence should be oriented towards encouraging innovation, preventing risks, ensuring the smooth operation of generative artificial intelligence under legal regulation, and promoting the development and innovation of generative artificial intelligence.

Beijing Wuzi University Student Innovation and Entrepreneurship Project: Legal Risks and Preventive Measures in ChatGPT Artificial Intelligence Applications

Reference

[1] Bao Qianyu Research on Western Government Open Data and Personal Privacy Protection from the Perspective of Big Data [D] Southwest University of Political Science and Law, 2018

[2] Gu Qin, Zhou Tao, Zhong Shuli, Qin Zhimei, Zhang Yaoyao, Chen Yi Construction of data ownership system from the perspective of information data [J] [1] Chengdu Big Data Group Co., Ltd., 2022

[3] Meng Lu The Efficiency and Application Path of Soft Law in Network Social Governance [J] Zhongzhou Academic Journal, 2021

[4] Han Wei Privacy Protection and Abuse of Dominance in the Digital Economy [J] [1] University of the Chinese Academy of Social Sciences, 2020

[5] Zhang Junhong, Ma Ming New Breakthrough in Digital Security [J] Economy, 2022

[6] Li Yongjun On the "Dual System" Protection of Personal Privacy and Information in the General Principles of Civil Law and the Basis of Claim Rights [J] Journal of Zhejiang Business University, 2017