https://doi.org/10.37420/j.mlr.2024.027

Research on Legal Risks and Responses of Generative Artificial Intelligence

Haoqi Zhang
Law school,Guangzhou College of Commercr, Guangzhou, China
***Corresponding author,E-mail: 854728125@qq.com**

Abstract

In November 2022, the U.S. OpenAI company released "ChatGPT", which as a chat program can not only process the input language, image, video, audio, etc., but also respond instantly according to the user's questions, so that it can achieve barrier-free interactive communication with humans, and there are many similar programs that have appeared. There are a lot of similar programs out there. Although the emergence of these artificial intelligence has brought great convenience to our life and study, at the same time, it has also generated a series of legal risks such as the crisis of personal information protection, copyright infringement, information leakage, etc. In the face of the rapid development of artificial intelligence, we should put forward countermeasures in a timely manner to cope with these potential legal risks.

Keywords

Generative Artificial Intelligence, Legal Risks, Prevention

1 Legal Risks of Generative AI

Generative artificial intelligence technology, represented by GPT-4, has indeed brought convenience and improved efficiency, but it has also triggered real problems such as unemployment panic to a certain extent, and at the same time, legal risks such as algorithmic discrimination, data leakage, etc., and has affected the operation mechanism of our current legal system. [1] The development of generative AI has brought innovative opportunities in multiple fields, but it has also brought risks of data abuse that threaten social stability, such as the spread of false information and rampant AI fraud.

1.1 Risk of violating personal information

First of all, AI has the risk of illegally collecting personal information. The application principle of AI technology looks, it contains three stages of data acquisition, pre-training and content output, in the pre-training stage inevitably need to collect a large amount of data. When acquiring data, technology developers may obtain information through illegal trading, illegal collection and storage, and even when using AI, the corresponding program will store and secondary process the information, and even retain some sensitive information, which is a serious violation of the principle of informed consent to collect personal information, and a serious violation of the security of personal information.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Secondly, there is the risk of improper use or abuse of personal information. For example, the use of "AI face-swapping" technology to commit fraud or infringement; or the use of voice simulation for extortion or other illegal acts. Bringing threats and damages to the property security of the information subject. In addition, this AI synthesized audio and video may also infringe on the privacy rights of others. Second, the Chat-like GPT model promotes academic fraud. Currently, several academic journal publishers have explicitly rejected results created or co-created by language modeling tools. Finally, chatbot developers are able to perform accurate profiling through user input. Misuse of the provided user information for improper commercial marketing and competition not only violates users' privacy, but also violates business ethics and market order.

Finally, there is a risk of personal information leakage. Although the developers of AI take measures to prevent the leakage of personal information, AI is after all dependent on human technology, which may lead to the leakage of personal information in the event of technological errors.2023 In March 2023, a problem with an open-source library on ChatGPT led to the visibility of Plus users' payment information within a nine-hour window, including name, email address, the last four digits of the credit card number, and the credit card number of the credit card holder. and the last four digits of the credit card number and the expiration date of the credit card, the Korea Personal Information Protection Commission determined that the personal information of 687 South Korean users had been compromised, and fined ChatGPT's operator, OpenAI, 3.6 million won (approximately $2,829). [2] In addition, the security of personal information is also related to the information security of the country, and once the personal information has been leaked across national borders, it is important for the country to protect the personal information. personal information is leaked across national borders, it may cause national security to be affected, which is a great threat to national data sovereignty and data security.

1.2 Risk of Copyright Disputes

ChatGPT can use algorithms to make timely and logical responses to the questions posed, then inputting a topic can produce the corresponding content according to the requirements, therefore, the use of artificial intelligence involves the issue of copyright in the process. On the one hand. In the data collection stage, the process of data collection by AI may involve intellectual property disputes such as copyright and trademark infringement. On the other hand, does the content it generates constitute a work? To whom do its rights and interests belong? And how should it be used? These issues have not yet been finalized.

With regard to the current legislative status in China, combined with the existing jurisprudence at home and abroad, there are three mainstream views in the academic community on the copyright of generative artificial intelligence ---"AI can become the author + AI content can constitute a work"." AI can not become the author + AI content can not constitute a work" and "AI can not become the author + AI content can constitute a work." [3]For the problem of ownership attribution, domestic academics have formed affirmative, negative and differentiated views on this issue. Distinction is to distinguish the degree of development of artificial intelligence and deal with the situation: when the output content is highly dependent on human participation, artificial intelligence is equivalent to the extension of human thought, at this time, there is no legitimacy basis for copyrightability, artificial intelligence can not become a copyright owner; but when the

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

artificial intelligence has a high degree of energy, the generated content has the legitimacy basis for copyrightability, the artificial intelligence can be the creator level of the Copyright owner. [4]. This view distinguishes the role of human beings and has rationality. The affirmative view, on the other hand, holds that artificial intelligence can be copyrighted. For example, the U.S. Copyright Office made a groundbreaking move in the late twentieth century to publish "works" "created" by computers and registered Racter as the author of The Policeman's Beard is Half Constructed. Beard is Half constructed" [5]. In contrast, in a case heard by the Beijing Internet Court, the decision held that content generated by computer software cannot constitute a work, and neither the developer of computer software nor the user of the software can be credited as the author. Therefore, the current emergence of artificial intelligence has also posed new challenges to China's current copyright law.

Regarding the question of whether AI-generated content can be a work, there are views that the content generated by chatbots is only an algorithm-driven program, which cannot reflect the originality of the creator, and therefore cannot be regarded as a "work" in the Copyright Law. This paper argues that the content generated by chatbots actually reflects the personality and emotion of the designer or questioner, represents human will and behavior, and has the characteristics of originality in copyright law, so the content generated by AI should be regarded as a work in the legal sense.

1.3 Data Bias and Falsehood

The operation mechanism of ChatGPT is still regarded as an algorithmic black box, and OpenAI does not disclose the details of its data sources, which raises questions about whether its training database is fully legally authorized. [6] And the AI generates information based only on its huge database, so it has not gone through deductive reasoning and cannot judge the authenticity and accuracy of the corresponding information. If someone maliciously uses the data of artificial intelligence to produce false data, it may affect the normal social order, and even illegal and criminal behavior. The data output by artificial intelligence lacks argumentation, and it is difficult to analyze the authenticity. At the same time, because the algorithms behind AI are compiled by technicians, it is inevitable that corresponding values or preferences will be fused when creating the corresponding programs, resulting in the final outputs that are also biased. For example, there have been cases where AI has been biased against women, jeopardizing women's legal rights and spreading wrong values that affect the social climate. Or if wrong information is stored for the AI at the initial data collection stage, reversing black and white, it will naturally output wrong information and produce data bias, resulting in adverse consequences.

2 Response to legal risks

In order to better utilize the performance of AI, it is necessary to regulate the use and operation of AI, which requires the joint efforts of technology producers, users and the government to work together to build a healthy and safe environment for the use of AI and avoid risks.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

2.1 Establish a multi-dimensional long-term regulatory mechanism

Optimize and upgrade the AI safety regulation model, establish a multifaceted and long-term regulatory mechanism, and achieve full-chain legitimacy regulation of generated content. On the one hand, the government can consider establishing an independent regulatory department, formulating a unified liability framework for generative AI, establishing a comprehensive risk management system in a timely manner, reasonably balancing the protection boundaries between data security and technological innovation, and further refining and improving the risk management system for generative AI. Regulators conduct regular monitoring and compliance checks of generative AI applications to ensure the legitimacy of generative AI in market operations. Service providers are promptly notified of deviations and errors as soon as they occur and urged to detect and remove them to prevent generative AI from being used for illegal or unethical purposes.

On the other hand, AI development companies themselves should operate in compliance. It should follow the provisions of the current relevant laws and regulations in China to collect data in a compliant and reasonable manner, to ensure that the data source is legal and compliant, and at the same time to protect the realization of the rights of the data subject through a variety of channels and measures to effectively prevent and control the risk of compliance with the data source.[7] If the AI acquires data independently, the R&D enterprise will formulate a corresponding data compliance plan in advance according to the operation principle of the AI to avoid risks and ensure that the AI is compliant with the process of acquiring data in the early stage and the data source is legal. If the R&D enterprise obtains data and stores it in the AI, the R&D enterprise should actively review whether the corresponding data source is legal and compliant, and may request the data provider to provide corresponding proof, and shall not infringe upon the intellectual property rights enjoyed by others in accordance with the law.

2.2 Personal Information Protection Mechanism

According to article 9 of the Interim Measures, if the services provided by a generative artificial intelligence service provider are associated with the personal information of users, the provider shall actively fulfill its personal information protection obligations in accordance with the law, and shall make clear provisions for the rights and obligations of both parties in the terms and conditions of the agreement by signing an agreement on the use of such services or a service agreement with the user. Therefore, when collecting personal information, it is necessary to strictly abide by the “informed consent rule”, obtain personal information within the scope of authorization, and protect the legitimate rights and interests of the subject of the rights. Service developers shall ensure that they are able to handle users’ requests for access, copying, correction, supplementation and deletion of their personal information in a timely manner, and safeguard the normal exercise of their rights to delete, correct, refuse and make decisions on their own with respect to their personal data.

R&D enterprises shall not unlawfully provide others with users’ input information and usage records, and shall not exceed their authority or arbitrarily use the personal information they have acquired. If it is impos-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

sible to avoid the circulation of data elements in the market, a series of technical processing methods should be used to blur the contents of the user's personal data in the possession of the identifiability of the content to be blurred, and ultimately make it impossible to locate a particular user, anonymization can ensure the rights and interests of the user's personal data to reduce the harmful consequences of the data leakage may cause.

In addition, the implementation of the principle of hierarchical classification protection, the data will be divided into levels, divided into public information, secret information and completely confidential information and other levels, for all types of information to implement different degrees of confidentiality measures. Access systems are set up for different levels of information to avoid unwarranted leakage of data. And the use of technical means to track access records, so as to identify the responsible data subject as soon as possible in the event of data leakage. At the same time, data leakage risk monitoring is strengthened, and data security obligations are implemented level by level to the specific person in charge in order to realize comprehensive security protection and risk management. In the event of a data leakage, disposal measures should be activated immediately, users should be informed in a timely manner and reports should be made to the relevant authorities.

2.3 Copyright risk regulation

Whether the generation of content by artificial intelligence constitutes copyright infringement depends on whether it is fair use. The purpose of the fair use principle is to balance the protection afforded by copyright to its owner with the greater interests of society [8] Article 24 of the Copyright Law of the People's Republic of China provides for 13 types of "fair use", and also clearly stipulates that fair use has a clear premise, i.e., it can be used without the permission of the copyright owner and without payment of remuneration to the owner, but it should specify the name of the author, the name of the work, the title of the work, and shall not affect the normal operation of the work. It shall specify the name of the author or the name of the work, and shall not affect the normal use of the work, and shall not reasonably jeopardize the legitimate rights and interests of the copyright owner. Whereas the use of corresponding protected data in the training of generative AI does not infringe the legitimate interests of the right holder, so the training of AI models with copyright-protected data can be regarded as fair use. However, as to whether the output results are infringing or not, it is entirely possible to rely on the common approach to determining copyright infringement - contact + substantial similarity.

Regarding whether the content of generative AI outputs is copyrighted. It should first be determined whether the AI enjoys the appropriate legal status. Chatbot creation is essentially the integration of pre-learning content, lack of creativity and unique emotions, does not have the ability to express meaning, therefore, should not have the corresponding subjective qualifications.[9] Secondly, does the content generated by artificial intelligence belong to the works protected by copyright? The output of artificial intelligence is still based on the output of previous knowledge reserves, since the copyright protection is the product of human creativity, then the output of artificial intelligence should be able to become a work, it can not be generalized that artificial intelligence works can not be protected by copyright law. As to whether the right of attribution of AI outputs should belong to the developer, the owner or the generator, it should be decided according to the agreement between the parties.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

2.4 Data Bias Regulation

In recent years, China has issued a number of legal documents to regulate algorithmic bias.2022, the State Internet Information Office issued the Administrative Provisions on Depth Synthesis, which put forward a series of requirements for depth synthesis technology.2023, in response to the introduction of ChatGPT and the intensive dynamics in the field of big modeling, the Interim Measures were formally issued. Among other things, Article 4 of the Interim Measures stipulates that generative AI service providers and algorithm users should avoid discriminating against different races, genders, countries, occupations, ages, beliefs, etc., in the process of selecting training data and building and optimizing large language models. Article 17 of the Interim Measures stipulates that before providing the public with generative AI services that are prone to triggering social opinion or have a certain social mobilization function, prior safety assessment should be carried out in strict accordance with the law, and algorithmic record-keeping, alteration, or deregistration procedures should be carried out in accordance with the Algorithmic Recommendation Provisions. Therefore, AI application developers should actively fulfill the obligations of algorithm filing and safety assessment, and should provide the necessary information according to the requirements of regulatory agencies. Algorithm developers should adhere to the concept of technology development for the good, always follow the ethical norms of various industries as well as the ethical guidelines for algorithm design for R&D and design, and adjust and update the rules for algorithm operation in a timely manner, in order to maximize the avoidance of innate discrimination brought about by the algorithm itself.[10] In addition, the “Artificial Intelligence Law (Draft)” has also been included in the State Council’s 2023 Legislative Work Plan, which will further refine the regulations on algorithm filing, and should specify the extent and limit of algorithm disclosure in subsequent legislation to avoid infringing on commercial secrets, and give algorithm designers reasonable obligations to explain to reduce unnecessary disputes. In addition, in order to eliminate the black box of algorithms and algorithmic bias brought about by the blind spot in the rules, we should also improve the accountability mechanism of algorithms and implement the main responsibility of algorithms by clarifying the main body of responsibility, the principle of attribution of responsibility, the distribution of responsibility and the legal consequences.

3 Conclusions

Generative artificial intelligence is the inevitable result of technological development, which will bring great convenience to human life, and at the same time, it will also trigger some legal risks, we need to do a good job in advance to prevent the layout, and take the necessary means in a timely manner, and reasonably regulate the risks, in order to promote the better application of generative artificial intelligence in social life.

Reference

[1]Liu Xianquan, The Impact of Generative Artificial Intelligence on the Criminal Law Protection System of Data Legal Interests. Chinese Journal of Criminal Law, 2023,No. 4,20-34.
[2]OpenAI Fined by Korean Privacy Regulator for Failing to Report ChatGPT Leakage of User Information

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

in a Timely Manner. http://news.10jqka.com. cn/20230728/c649251537.shtml, 2023-07-28.
[3]Zhou Shuhuan. Research on the legal personality dispute and communication infringement liability of chatbots: based on the perspective of ChatGPT scene. Nanjing Social Science, 2023.No. 6,90-99.
[4]Liu Wenxian. The Legal and Philosophical Basis of 'Copyrightability' of Content Generated by Artificial Intelligence - Taking the Philosophical Theory of Artificial Intelligence as a Perspective. Politics and Law, 2020,No. 3,14-26.
[5]Leah Henrickson. Constructing the Other Half of The Policeman'sBeard .https://electronicbookreview.com/essay/constructing-the-other-half-of-the-policemans-beard/.2023-08-01.
[6]Author1 Liu Shuangyue.Author2 Zhang Xiaoyue. Research on Legal Protection and Regulation of Data Risks of Generative Artificial Intelligence--Taking ChatGPT's Potential Data Risks as an Example. Guizhou Univ.Journal of Guizhou University (Social Science Edition), 2023, No. 5,87-89 .
[7] Chen Anshuai .On the Statutory License for the Collection and Utilization of Artificial Intelligence Data. China Price Regulation and Anti-Monopoly.2024,No. 11,98-100.
[8]Hu Kaizhong, Zhang Yan . On the Situational Principle in the Judicial Protection of Copyright on the Reasonable Application of Situational Principle in the Judicial Protection of Copyright. Jianghan Academic, 2023,No. 4,84-93.
[9]Sun Yang. Copyright Law Dilemma and Way Out for Generative Artificial Intelligence Data Behavior. Yangtze River Forum . 2024.No. 05,61-71.
[10]Auther1, Wang Q. H. Auther2, Hu L. T. Technological and legal construction of generative artificial intelligence liability mechanisms.China Law Review. 2024,No. 04,114-130.



© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)