ChatGPT Legal Risk and Regulation Study

Weijian Zhou

Constitutional and Administrative Law, Jiangxi Normal University, Jiangxi, China

Abstract. ChatGPT is a high-profile artificial intelligence chatbot, and although it brings great convenience to society, it also brings a series of legal risks, including disputes over the ownership of intellectual property rights, the legality of data sources, and the quality of data used for training, the generation of undesirable or illegal information, and challenges to schools and academic ethics codes. The reasons for this are the specificity of this type of product and the fact that it has not yet developed a mature system at the technical level, while regulators and legislators are too conservative in their regulatory philosophy.

Keywords: ChatGPT, Legal Risk, Regulatory Countermeasures.

1. Introduction

ChatGPT, a new generation of AI language model developed by Open AI, marks the entry of humanity into an era of general AI, which will have a profound impact on the progress of human society. The core of ChatGPT is to provide user-centered intelligent interaction services based on natural language processing technology to achieve deep interaction between humans and machines. the emergence of ChatGPT may trigger technological changes in the AI field, thus promoting innovation in human production methods and facilitating a new round of technological and industrial changes. At the same time, social risks such as data privacy leakage, social unemployment, industry monopoly, and algorithmic bias may come along, and these risks may negatively affect people's lives.[1]

2. Chatgpt

2.1. ChatGPT operation principle

ChatGPT uses the architecture of natural language processing and search engine integration to build a large language and reinforcement learning fine-tuned training model that connects a large corpus and processes the large model sequence data by pre-training methods to make it capable of language understanding and text generation so that it can perform the task of user instructions. The model automatically acquires target utterances from a large-scale speech database, builds a knowledge base based on the extracted features, and uses artificial intelligence to predict whether the target sentence is the desired outcome. ChatGPT is a high-level language generation model that combines generative pretraining and algorithmic language transformation and is unique in its organic combination of the two. The method makes full use of deep neural networks in machine learning and combines research results from the field of computational linguistics to improve prediction accuracy.

2.2. ChatGPT characteristics

With the flourishing development of cutting-edge technologies such as deep learning technology and natural language processing technology, ChatGPT is highly interactive, and this strong interactivity is reflected in four main aspects. First, ChatGPT demonstrates an amazing memory capacity that is breathtaking. It can store and extract a large amount of corpus in a short period and can perform the extraction of complex relationships between text or speech signals through automatic machine analysis.[2] LLM, as a large language model, has a memory capacity of hundreds of billions of level parameters, providing the necessary prerequisites for ChatGPT's large-scale data information input. It is also an accurate grasp of the relationship between user input intent and results. Second, ChatGPT demonstrates self-learning ability. Big Language Model is a new type of machine

intelligence system built based on artificial intelligence technology, which can automatically analyze and process a large amount of content such as text and images. LLM, as a deep and giant neural network architecture, uses massive data information for pre-training to achieve uninterrupted real-time human-machine dialogue with the premise of autonomously learning knowledge points in the Internet space. This technology can help us better understand and master the Internet knowledge system. Third, ChatGPT demonstrates a deep understanding of information. RLHF has the natural language ability to conduct multiple rounds of situational dialogues with users, and the dialogue process is highly flexible and diverse. It has strong expressive capabilities as well as high self-adaptability. Fourth, ChatGPT demonstrates its excellence in reasoning capabilities. The context-aware mechanism based on semantic features allows users to automatically access their potential knowledge and exploit it when using the machine learning approach. ChatGPT's context learning is done by modeling the probabilistic distribution of contextual phrases to expand and mine the large-scale and large-scale implicit relationship recognition, and finally generate a language style that is easy for users to understand.

3. Chatgpt Legal Risks

3.1. Data Privacy Risks

ChatGPT can meet the needs of users, developers, and other related subjects with its powerful features such as big data, deep learning, and cloud computing. However, without user authorization, ChatGPT may collect, store and export private data, which may lead to the risk of personal information and privacy leakage, thus providing a breeding ground for crimes. ChatGPT is a pre-trained model based on a corpus of 300 billion words, which has 175 billion parameters, with GPT-4's parameters being GPT-3.5, a large model with over 1 trillion level parameters, and its internal neural network is even comparable to the size of the human brain. In this case, personal and business data input by users may be used to train ChatGPT, which in turn uses the data for its corpus, making it difficult to ensure the security of personal privacy.[3]

3.2. Generate illegal or undesirable information

When users enter text commands in the input box, ChatGPT uses the big model behind it to deeply analyze and learn from that text combines the data in its corpus to extract valuable information from it, and finally draws the corresponding conclusions. This method of building its knowledge base by collecting and organizing domain-specific knowledge and corpus can effectively improve the accuracy and recall rate of the automatic Chinese abstract evaluation system. However, the huge model of ChatGPT is not sufficiently supervised during the autonomous pre-training learning process, so the acquired information data are difficult to be substantially reviewed and filtered.[4] ChatGPT is likely to generate false and undesirable information when the corpus collects data with illegitimate, discriminatory contents indistinguishable from the real ones, thus triggering the phenomenon of "Garbage in, Garbage out".

4. Chatgpt Legal Regulations

Currently, the subjectivity of AI in terms of criminal liability is rejected by most scholars. Although ChatGPT possesses human-like qualities, it's complete self-control and discriminatory ability still need to be improved. Therefore, when ChatGPT generates false information or undesirable information, it does not constitute the "crime of fabrication and intentional dissemination of false information" as stipulated in China's Criminal Law, nor can it become the subject of abetting or aiding and abetting. However, if a user uses ChatGPT as a criminal tool to generate and disseminate false information, or forces ChatGPT to provide criminal ideas using coercion and enticement to commit crimes such as online fraud, the user shall bear the corresponding legal responsibility. At the same time, since the account belongs to personal information and a certain extent can reflect the user's real

identity information, the netizen department should treat the account as an important clue to focus on monitoring. In response to ChatGPT account trafficking and leasing, it is recommended that the Office of the Internet Trustee and the Ministry of Public Security and other regulatory agencies consider launching a "ChatGPT account trafficking and leasing crackdown" concerning several previous regulatory crackdowns, strengthen the crackdown on unlicensed operations and illegal transactions, and once involved in crimes, transfer them to If a crime is involved, it will be handed over to judicial authorities for criminal responsibility.

China has established a relatively complete legal framework to regulate data and personal information protection and algorithms, including regulations such as the Network Security Law, the Data Security Law, the Personal Information Protection Law, the Regulations on the Administration of Deep Synthesis of Internet Information Services, the Regulations on the Administration of Algorithm Recommendation of Internet Information Services, and the Measures on Data Exit Security Assessment. Under the current legal order framework, the potential legal risks posed by ChatGPT have been largely addressed, but there is a lack of sufficient evidence to prove that strict regulation and mandatory intervention alone is the only or best way to regulate technological risks. Relying solely on strict regulation and ex-post penalties would consume significant resources that could prevent other types of risks, thereby undermining the higher levels of individual growth and social progress that should be achieved. Therefore, this potential threat should be averted through ex-ante intervention.

5. Conlusion

ChatGPT opens a new era of human intelligence, based on human-like and high intelligence, which brings great convenience to human production and life while potentially challenging the existing rules. The advent of the era of artificial intelligence is a product of human development to a certain stage. chatGPT is irresistible, yet it is not a Pandora's Box, but a mission to facilitate human beings at its inception. To deal with the problem of data leakage, technology innovation companies should legally clarify the rights and obligations between them and the data owners, and establish corresponding legal liability provisions. To deal with the problem of false information and undesirable information, STI companies need to develop a set of self-detection models and information source comparison systems, as well as establish a user challenge and disinformation mechanism and strengthen ethical and moral awareness training for ChatGPT-like models to ensure that companies can practice compliance systems. In addition, attention should be paid to the new challenges brought by the development of network technology, such as the increased risk of user privacy and security due to the popularity of smart terminals and social panic caused by data leakage, to improve relevant laws and regulations and build a reasonable balance of interests.

References

[1] Alec Radford, Karthik Narasimhan, Tim Salimans, et al. Improving Language Understanding by Generative Pre-Training, https://gwern.net /doc/www/s3-us-west -2. amazonaws. com/ d73fdc5 ffa8627bce44dcda2fc012da638ffb158.pdf.

[2] R. C. Andrew, Billy Perrigo. The AI Arms Race is Changing Everything, February 27/March 6, 2023: 45 - 48.

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

[4] Tiffany Hsu, A. T. Stuart. Disinformation Researchers Raise Alarms About A.I. Chatbots, The New York Times, February 8, 2023.