2023 13th International Conference on Information Technology in Medicine and Education (ITME) | 979-8-3503-1915-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ITME60234.2023.00023

Legal Risks and Governance Paths for Generative AI--A Case Study of ChatGPT

Wang Zhenfeng
Key Laboratory of Big Data and Artificial Intelligence in University of Fujian Province，MinNan Science and Technology University
Fujian；China
1372056709@qq.com

Lin Quanwang
Minnan Science and Technology University
Fujian；China
25490461@qq.com

Gao Huihui
Minnan Science and Technology University
Fujian；China
2667293520@qq.com

Yu Xiehua
School of Computer and Information,MinNan Science and Technology University,Quanzhou, China
Key Laboratory of Big Data and Artificial Intelligence in University of Fujian ,Quanzhou, China
hiphop_yu@163.com

Abstract:The release of OpenAI's ChatGPT chatbot has sparked widespread concern around the world about the threats and legal issues of generative AI. Although this technological innovation has opened a new chapter in the field of artificial intelligence, it has also caused the public to worry about its possible negative effects. In order to solve the above problems and reasonably regulate the legal risks of generative artificial intelligence, this paper mainly adopts the literature, quantitative and qualitative analysis methods, etc. The first part mainly introduces the development process and current situation of generative artificial intelligence, the second part mainly discusses the impact of generative artificial intelligence on tort law, the third part mainly discusses the legal risks of generative artificial intelligence, and the fourth part mainly discusses the governance path of generative artificial intelligence legal risks. The last part is the conclusion of the research. Among them, the fourth part is the focus of this paper. By taking these issues into account, we can provide legal guarantees for the sustainable development of the generative AI industry and ensure that the widespread application of AI benefits human society[1] **.**

Keywords:Generative Artificial Intelligence;Legal regulation;ChatGPT

I. INTRODUCTION

As the hottest new technology at present, artificial intelligence brings new opportunities for economic development and social construction, it also brings huge challenges to the adjustment of legal relations and the application of legal rules. In April 2019, Beijing Chaoyang District People's Court heard the country's first case of copyright for artificial intelligence-generated content. The court believed that the analysis report did not meet the requirement of originality, and noted that neither the software developer nor the user enjoyed copyright protection of the author's rights. However, considering the communication value of the article and the need to protect the rights and interests, software developers and users are allowed to demonstrate their rights and interests through reasonable means. This judgment is a beneficial exploration of the legal protection of artificial intelligence-generated content under the current legal framework. Artificial intelligence, as the hottest new technology at present, not only brings many new opportunities for economic development and social construction, but also brings important adjustments and challenges to the application of rules in the legal field.

In response to these challenges, it is necessary to closely combine the characteristics of law and artificial intelligence, and formulate corresponding legal rules and policies. This includes clarifying the legal status of AI-generated content, identifying responsible subjects, and measures to protect users' privacy and personal rights. At the same time, there is a need to promote cross-sectoral collaboration and international cooperation, to develop common standards and principles to address legal challenges in cross-border data flows and cooperation. In addition, in the formulation of legal rules, attention should also be paid to public participation and extensive research of expert opinions. Through multifaceted discussions and consultations, we can better understand the impact of AI on society and make trade-offs around protecting human rights and values.

2474-3828/23/$31.00 ©2023 IEEE
DOI 10.1109/ITME60234.2023.00023

In general, in order to cope with the legal challenges posed by AI, it is necessary to continually pay attention to new progresses of technological development, strengthen research of related fields and innovation of intellectual property protection policies[2]. Only with the organic combination of law and technology, can we achieve the sustainable development of the AI industry and make this advanced technology benefit the whole society.

II. DEVELOPMENT PROCESS AND STATUS QUO OF GENERATIVE AI

According to the Administrative Measures for Generative Artificial Intelligence Services (Draft for Comment) issued by the Cyberspace Administration of China on April 11, 2023, generative artificial intelligence is defined as a technology that uses algorithms, models and rules to generate text, pictures, sounds, videos, codes and other content. Among them, a kind of generative artificial intelligence named ChatGPT introduced by OpenAI in 2022 is regarded as one of the important components of the metaverse technology architecture. The appearance of ChatGPT advanced the time of the realization of the meta-universe and provided a good technical operating environment for it. The rapid development of generative artificial intelligence has also promoted the further development of the concept of metaverse. Especially with the advent of generative artificial intelligence such as GPT4 that can understand, speak and interact, all industries are facing varying degrees of impact. Compared to previous AI technologies, generative AI such as ChatGPT presents real and urgent potential risks. People think that if the Internet had raised a revolution in space and smartphones had raised a revolution in time, technologies like ChatGPT are leading to a knowledge revolution. Elon Musk thinks it is no less than the iPhone, Bill Gates thinks it is no less than reinventing the Internet, and Zhou Hongyi compares it to the invention of the steam engine and electricity.

Technologies like ChatGPT pose more pressing potential risks than other AI technologies. For the harm of AI, Geoffrey Hinton, deep learning pioneer, believes that most people, including himself, previously thought it was far away. But now that has changed. Therefore, analyzing the potential risks of generative AI and proposing appropriate legal governance paths is no longer a pure fantasy, but a rational thinking based on reality. How to combine the operational mechanism and security risks of generative artificial intelligence to conduct legal regulation has become a common concern of science and technology, industry and legal circles[3].

III. THE IMPACT OF GENERATIVE ARTIFICIAL INTELLIGENCE ON TORT LAW

(a) The complexity of the behavior subjects. Traditional network infringement usually involves two subjects, that is, the network service provider and the victim, or three subjects, that is, the network service provider, the network user and the victim. The former case refers to the network service provider directly commit infringement , while the latter case refers to the network user commit infringement by using network services.

(b) The intelligentization of harmful behavior. The injurious behavior in traditional network infringement is directly executed by people. However, in generative AI, the harm is not done directly by the human, but by the "actions" of the AI. People are not directly involved in the content generation process. Although fundamentally, the infringing content generated by AI is still the result of the algorithm designer and caused by them, the difference with traditional infringement is that the designer cannot foresee the specific harmful behavior when designing the algorithm program, that is, the designer does not know what content the AI will generate[4] .

(c) Uncertainty of the consequences of damage. The characteristic of generative AI is that it varies from person to person and from time to time, which determines the uncertainty of the infringing content. In different conversations, there may be different infringement content, which is different from traditional infringement. Traditional network infringement may have personalized push, such as news feed, but the specific content of the push itself is usually fixed, such as a specific news report. However, the variable nature of the content of generative

artificial intelligence makes it difficult to judge the damage caused by infringing content.

(d) The multiplicity of causality. The infringing content generated by artificial intelligence involves a combination of multiple factors, including algorithms, computing power, data sets, and human-computer interaction. However, due to the complexity of the algorithm, it is difficult to judge the specific role of these factors in the generation of infringing content. While algorithms can be considered as key factors, data sets and human-computer interactions are only "raw materials" for generating content and do not need to be evaluated in tort law. However, the reality is complicated, because users may consciously use algorithms to achieve a certain infringing result, that is, deliberately "teach" the algorithm, and ultimately cause the algorithm to generate infringing content.

(e) The novelty of fault identification. In the traditional network infringement, the mainstream view is that Internet service providers do not have a general censorship obligation to the content posted by users, although scholars have proposed the obligation of filtering in advance. Therefore, in traditional network infringement cases, fault determination is mainly based on thestandard that the network service provider is aware of the infringing content but didn't take appropriate measures, and the standard that the network service provider should know will serve as an aid when the situation is obvious. However, in a generative AI environment, unless the algorithm designer intentionally intended to generate specific infringing content, it is difficult to determine fault based on the "ought to know" standard[5] .

IV. KEY RISKS OF AI-GENERATED CONTENT

A. Risks to national security and public safety

Generative AI has the ability to quickly mimic language styles and synthesize various kinds of information. If it is used to fabricate politically inflammatory information, the efficiency will be higher than that of pure manual operation, and it can quickly and purposefully incite social public emotions and interfere with or influence national political choices. Artificial intelligence's "deep forgery" capabilities make it easy to be used to create false information that harms public order and safety. For example, a property owner in a community group in Hangzhou tried to use ChatGPT to generate a press release similar to the official manuscript about the cancellation of Hangzhou's driving restrictions, which was mistaken for real by others and widely spread on the network, causing adverse effects.

B. Risk of violation of personal reputation and personal safety

Generative AI has the ability to generate false information that is combined with reality. If used maliciously, false text, pictures, audio and video information can be generated and disseminated against individuals to mislead them as acts that have been carried out in reality. This can seriously damage an individual's reputation and, in some cases, lead to attacks and reprisals against the subject of rumors, putting them at risk. Among them, a typical risk is "revenge porn", which means disseminating indecent information of the victim such as nude photos and videos in order to achieve revenge. In the past, the execution of revenge porn required a high technical threshold and was limited to technical experts. However, generative artificial intelligence has greatly lowered the threshold of execution, so that ordinary people and even people who have never met can use "deep forgery" technology to process the real photos of the victims, and replace the face through "AI face change "and other technologies to generate non-existent nude photos, pornographic videos and other content[6].

C. Risk of infringement of corporate rights and interests

The "deep forgery" capability of generative artificial intelligence has potential risks, which can be used to create false public statements by leaders, corporate announcements and other information, spreading wrong corporate information. Due to the fast and extensive dissemination speed of artificial

intelligence-generated content and network, it is difficult for business leaders to respond to the generation and dissemination of false information in a timely manner, which may lead to the public and investors being misled and making wrong decisions, causing a serious blow to corporate reputation and economic interests. For example, there is a "deepfake" video circulating about Facebook founder and CEO Mark Zuckerberg, in which he is captured confessing to a data breach plot and saying, "Imagine one person having complete control over the stolen data of billions of people, all their secrets, lives, futures." Whoever controls the data controls the future." Speaking on behalf of the company, the CEO's statement could have a significant impact on Facebook's reputation if the video is actually circulated by users, and,then affect the company's financial interests[7] .

V. LEGAL REGULATION PATH OF ChatGPT APPLICATION

A. Domestic legal systems should insist that generative AI itself is a non-legal subject

There are debates about whether artificial intelligence should have subject status in law. In the field of criminal law, most criminal law scholars are opposed to treating AI as the subject of criminal responsibility. In the field of private law, the legal status of artificial intelligence is mainly divided into three categories: all, part and none. These views respectively advocate that it is completely equivalent to the natural person, or it has quasi-subjectivity, or only is considered as the existence of things opposite to the subject. The author argue that although AI is "generative" and breaks through traditional boundaries, it should not be considered a subject of law. While generative AI exhibits the ability to learn in some ways and can come up with answers on its own, its algorithms are still its underlying logic. In other words, generative AI still lacks the ability to think independently and free will, does not serve as a basis for rational agents, and does not conform to the premise set by human-centered legal norms[8].

B. The domestic market raises the threshold forgenerative AI to enter the market

China's strategy for new technologies, new things and new forms of business is to "minimize prior access and strengthen post-event supervision." However, to the development of generative AI, it is not entirely laissez-faire. At present, generative AI like ChatGPT is mainly in English and cannot enter the Chinese market yet. Three issues need to be considered before it is approved for entry: reviewing sensitive information, assessing data security and analyzing development barriers to indigenous generative AI. The review of sensitive information needs to pay attention to differences in different cultural backgrounds, including the regulatory focus on pornographic, political and illegal content and the potential risk of discrimination. The data security assessment should consider the exploitation and protection of ChatGPT's user data and the risk of leakage caused by third-party intrusions. In addition, it is necessary to analyze the obstacles faced by domestic enterprises to independently develop generative AI, and ensure that the introduction of foreign products will not occupy the domestic market on a large scale to maintain the development of local products[9].

C. Pay attention to the security risk prevention of network user's data

ChatGPT applications involve multiple entities, such as developers, deployers, users, and recipients.To prevent and resolve the legal risks caused by ChatGPT, it is necessary to design a compliance plan with the developer as the main body. Developers should establish an ethical and legal bottom line, play a leading role in technical ethics and legal norms, avoid abusing of ChatGPT, and realize algorithms to be good. Code constraints and public oversight are not enough; the state must provide enforcement to ensure fair use. At the organizational level, a special privacy data protection department

can be established to take professional measures. In the context of the booming development of artificial intelligence, it is necessary to formulate more detailed laws and regulations. China has introduced laws such as the Personal Information Protection Law and the Cybersecurity Law to prevent related risks. The Regulation on the Management of Deep Synthesis of Internet Information Services came into effect on January 10, 2023, which is the first time for China to legislate deep synthesis algorithm services.

C. Regularly review and cultivate the safe use of generative AIisks to national security and public safety

To ensure the safe use of ChatGPT, the following are optimized regulatory measures:

(a) To ask sensitive questions (such as illegal, pornographic, political questions), once the AI provides inappropriate answers, immediately deactivate and retrain or modify the algorithm.

(b) Communicate and verify issues with affiliated enterprises that may involve trade secrets to avoid serious consequences of large-scale data leakage.

(c) Coerce generative AI research and development companies regularly check and modify algorithms to avoid irreversible consequences due to regulatory limitations.

(d) Clarify the scope of liability of generative AI development enterprises, and after regular inspections, if illegal acts are caused by intentional or gross negligence, the enterprises and their supervisors shall be investigated for civil or criminal liability.

VI. CONCLUSION

ChatGPT leads the beginning of the era of strong artificial intelligence, and its human-like nature and high intelligence bring convenience to human production and life, but it may also impact the existing rules. ChatGPT, however, is no Pandora's box; it was born with a mission to facilitate humanity. We need to face up to the potential risks behind scientific and technological progress and take effective regulatory measures to make innovation benefit mankind.For the possible cheating and plagiarism problems caused by AI like ChatGPT, plagiarism detection models should be actively developed to strengthen the construction of academic integrity. In the process of legal regulation, it is necessary to ensure the strict application of criminal law and avoid excessive generalization, so as not to stifle technological innovation. When other departmental laws can effectively regulate artificial intelligence risks, criminal law should be avoided[10].

ACKNOWLEDGEMENT

This work is supported in part by the Key Laboratory of Big Data and Artificial Intelligence in Universities of Fujian Province(GXKYSY201901);Fujian Province first-class undergraduate major construction site (SJZY-2022-01); Fujian Province Virtual Simulation Experimental Teaching First Class Course (SJKC-2020-03);School level research team (MKKYTD202302); School level virtual teaching and research room (MKXNJYS-2023-02); School level curriculum ideological and political education (MKKCSZ-2021-02, MKKCSZ-2022-08)

REFERENCES

[1] Zhu Jingwen. Jurisprudence [M]. Beijing: China Renmin University Press,2015.

[2] Liu Chuntian. Intellectual Property Law [M]. Beijing: China Renmin University Press,2014.

[3] Miao Jinchun. Context and Tools: The Approach to Interpreting Pragmatic Law [M]. Jinan: Shandong People's Publishing House,2004.

[4] Cai Zixing, Xu Guangfu. Artificial Intelligence and its Application [M]. Beijing: Tsinghua University Press,2018.

[5] Hua Yu Yuandian Legal Artificial Intelligence Research Institute. Let legal people understand Artificial Intelligence [M]. Beijing: Law Press,2019.

[6] Sun Jianwei, Yuan Zeng, Yuan Weiming. Brief Introduction to Artificial Intelligence Law [M]. Beijing: Intellectual Property Press,2019.

[7] Joe Road, Snow White. The Legal Future of Artificial Intelligence [M]. Beijing: Intellectual Property Press,2018.

[8] Wang Qian. Course of Intellectual Property Law [M]. Beijing: China Renmin University Press,2016.

[9] Wang Qian. Copyright Law [M]. Beijing: China Renmin University Press,2015.

[10] He Min. Basic Theory of Intellectual Property [M]. Beijing: Law Press,2011.