

Ethical issues and countermeasures of applying artificial intelligence to psychological counseling—Focusing on privacy and data protection issues

Meng Liu

*Robert H. Smith School of Business, College Park, University of Maryland, Maryland, 20742, USA
Mengpleasant2018@163.com*

Keywords: Psychological counseling; artificial intelligence; privacy; data protection

Abstract: With the rapid development of artificial intelligence (AI) technology, its application in the field of psychological counseling is gradually increasing. With its efficient and convenient characteristics, AI psychological counseling provides psychological support and help for more people. However, this process also comes with a host of ethical issues, particularly privacy and data protection challenges. This paper aims to explore the ethical issues of privacy and data protection in AI psychological counseling, and put forward corresponding countermeasures and suggestions to promote the healthy development of AI psychological counseling. The research results show that although AI psychological counseling has the advantages of efficiency and convenience, there are also ethical issues such as privacy protection, data abuse, and human emotion neglect. This paper proposes to ensure the healthy development of AI psychological counseling by strengthening legal supervision, enhancing the ethical awareness of AI technology, and promoting human-computer collaboration.

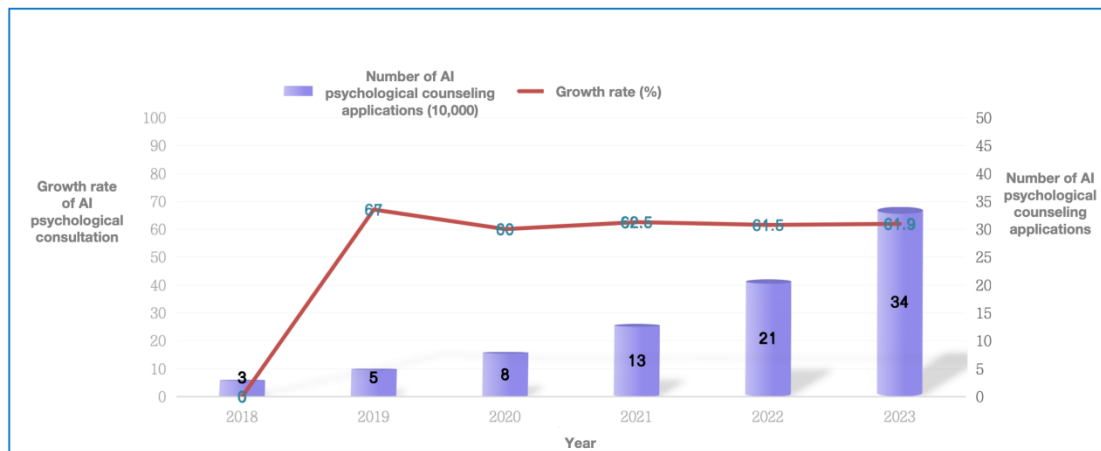
1. Introduction

AI psychological counseling is a type of therapy based on an AI program that provides patients with the prevention, management or treatment of psychological problems. Digital mental health services is the application of digital therapy in the field of mental health services, through digital platforms, smart watches and other tools, to provide consumers with services to prevent or treat mental disorders, such as mobile apps and online platforms, virtual reality (VR) therapy, intelligent dialogue and chatbots, biofeedback and monitoring[1]. With the continuous progress of artificial intelligence (AI) technology, its application in the field of psychological counseling is becoming more and more extensive (As shown in table 1 and figure 1). As a new psychological service model, AI psychological counseling has been widely concerned for its high efficiency, convenience and personalized characteristics. At the same time, however, privacy and data protection issues have come to the fore. When seeking psychological counseling, users often need to share a lot of personal information and sensitive data, the disclosure and abuse of these information will bring great harm to users. In order to ensure the healthy development of AI psychological counseling and protect users' privacy and data security, this paper delves into the ethical issues of applying artificial intelligence to

psychological counseling, focusing on privacy and data protection issues, and exploring countermeasures in AI psychological counseling[2].

Table 1: Growth trend of AI psychological counseling application

A given year	Number of AI psychological counseling applications (10,000)	Growth rate (%)
2018	3	-
2019	5	67
2020	8	60
2021	13	62.5
2022	21	61.5
2023	34	61.9



(Data source: AI Market Report, Gartner, 2018-2023)

Figure 1: The growing trend of AI psychological counseling application

2. The importance of privacy and data protection in AI psychological counseling

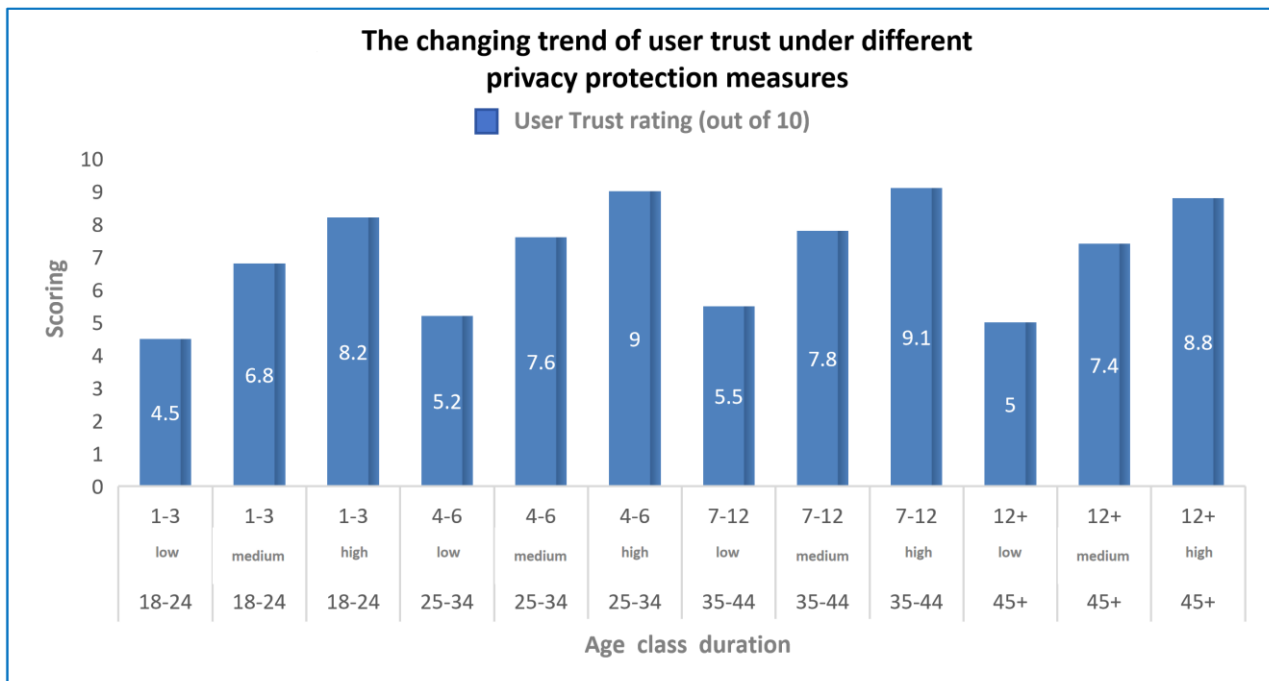
2.1 Basis of user trust

In AI psychological counseling, the importance of privacy and data protection is self-evident, and they form the basis of user trust. First of all, personal privacy is one of the basic rights of everyone. In psychological counseling, the user's mental health status and inner world belong to the sensitive and private field, and its privacy needs to be respected and protected. When users' personal privacy is properly protected, they will feel respected and understood, making them more willing to build a trusting relationship with an AI psychologist. Secondly, if the user's psychological counseling data is improperly used or leaked, it may lead to a series of problems, such as being used for malicious marketing, discrimination or invasion of privacy. These problems will not only damage the rights and interests of users, but also destroy the reputation and trust of the AI psychological counseling industry. Therefore, protecting the security and privacy of user data and preventing data abuse are important measures to maintain user trust. Finally, when the AI psychological counseling platform can clearly inform users about how their data is collected, stored and used, and comply with relevant privacy protection regulations, users will more easily build trust in the platform[3]. This transparency not only helps users understand how their data is being used, but also helps the platform build an image of integrity and reliability. At the same time, in the psychological counseling process, cooperation and communication between users and AI psychological counselors is crucial. If users have doubts

or concerns about privacy and data protection issues, it may affect the effectiveness of their communication and cooperation with AI psychological counselors. Therefore, the protection of user privacy and data security helps to eliminate users' doubts and concerns and promote cooperation and communication between the two sides.(As shown in table 2 and figure 2)

Table 2: Growth trend of AI psychological counseling application

User age	Privacy protection measures level	Duration of use of AI Psychological counseling platform (month)	User Trust rating
18-24	low	1-3	4.5
18-24	medium	1-3	6.8
18-24	high	1-3	8.2
25-34	low	4-6	5.2
25-34	medium	4-6	7.6
25-34	high	4-6	9
35-44	low	7-12	5.5
35-44	medium	7-12	7.8
35-44	high	7-12	9.1
45+	low	12+	5
45+	medium	12+	7.4
45+	high	12+	8.8



(Data source: online questionnaire survey platform user feedback)

Figure 2: The changing trend of user trust under different privacy protection measures

2.2 Requirements of laws and regulations

In the field of AI psychological counseling, the importance of personal privacy protection is self-evident, and relevant laws and regulations at home and abroad have made detailed provisions on this, providing a solid legal support for the AI psychological counseling platform (As shown in table 3).

In Europe, the legal framework, with the General Data Protection Regulation (GDPR) at its core, sets high standards for data processing[4]. The GDPR adheres to the principle of minimization of data processing, that is, the amount of data collected should be strictly controlled to the extent necessary for the purpose of the consultation, and gives users key rights such as the right to access, correct and delete data. These regulations require AI psychological counseling platforms to strictly comply with all aspects of data collection, processing, storage, etc., to ensure that user privacy is fully protected.

China has established a comprehensive personal privacy protection system through laws and regulations such as the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law. These regulations are not only in line with international standards, but also put forward strict requirements for personal information processing activities in light of the actual domestic situation. The AI psychological counseling platform shall follow the principles of legality, legitimacy, and necessity to collect user data, and adopt technical means such as encryption and de-identification to protect data security.

In the operation process of the AI psychological consultation platform, users should be clearly informed of the purpose, method and scope of data processing to ensure that users provide personal information under the premise of full knowledge. At the same time, the platform shall establish a sound data access control mechanism to prevent data leakage and abuse, and ensure the security and privacy of user data.

Relevant laws and regulations at home and abroad provide a clear direction and guarantee for the protection of personal privacy of AI psychological counseling platforms. The platform should actively respond to regulatory requirements, put user privacy protection in the first place, and provide users with safer and more reliable psychological counseling services through technological innovation and compliance management.

Table 3: Overview of privacy regulations in major countries and regions around the world

Country and region	Privacy protection statute name	Implementation date	Key features or highlights
European Union	General Data Protection Regulation (GDPR)	May 25, 2018	Strict data protection principles, high fines, and enhanced rights for data subjects
America	California Consumer Privacy Act (CCPA)	January 1, 2020	Give California residents more control over their personal information, including access, deletion, and opt-out of selling
China	Personal information protection Act	November 1, 2021	Clarify rules for handling personal information, strengthen supervision over cross-border data flows, and set up personal information protection agencies
Japan	Personal Information Protection Act (APPI, Revised Version 2022)	April 1, 2022	Strengthen the responsibility of enterprises to manage personal information, and establish a personal information protection committee
Brazil	General Data Protection Act (LGPD)	August 18, 2020	Set up a data protection authority and impose severe penalties on companies that violate privacy protection rules

(Data source: official government websites, professional legal databases)

2.3 Sustainable development of AI psychological counseling system

The importance of privacy and data protection in AI psychological counseling is not only reflected in the establishment of user trust, but also directly related to the sustainable development of AI psychological counseling system. In the highly competitive AI psychological consulting market, systems that attach importance to privacy protection can form their own competitive advantages and attract more users. When users confirm that their privacy is properly protected in an AI psychological counseling system, they are more likely to use the system for a long time, thus improving the system's user retention rate. A successful AI psychological counseling system must pay attention to the needs of user privacy protection while complying with laws and regulations, and constantly innovate to improve service quality and user experience. Only in this way can the system be invincible in the competitive market.

2.4 Guarantee of technological development

Privacy and data protection provide a solid foundation for the technological development of AI psychological counseling systems. Only on the premise of ensuring the security and privacy of user data can the system collect and analyze more user data, so as to optimize algorithms, improve service quality and user experience. By adopting security technologies such as advanced data encryption technology, access control, and multi-layer firewalls, AI psychological counseling system can provide users with more secure and reliable services. Privacy and data protection are not only legal requirements and technical basis, but also an important driving force to promote the continuous innovation of AI psychological counseling system. In the face of changing legal environment and user needs, the system needs to continuously improve and optimize its privacy protection measures to meet higher standards and requirements. By strengthening the research and application of privacy protection technology, the AI psychological counseling system can develop a more advanced and efficient service model to bring better experience and value to users.

3. Risk analysis of privacy disclosure in AI psychological counseling

3.1 Improper collection and use of user information

First, in the field of AI psychological counseling, the protection of user information has increasingly become a focus, especially regarding the improper collection and use of information. With the continuous evolution of AI technology, psychological counseling platforms can collect and analyze a large amount of data from users, aiming to provide more accurate psychological support. This capability also comes with the potential risk of user privacy breaches.

A key problem is that platforms may over-collect user information, far beyond the immediate needs of psychological counseling. In AI-assisted psychological counseling decision-making, if the system collects information that is not directly related to the purpose of counseling, it will significantly increase the risk of privacy disclosure[3]. For example, basic user information (such as name, contact information) and mental health data should be strictly confidential, but if it is improperly collected and used for non-psychological purposes, such as advertising or user profile analysis, it will seriously violate users' privacy rights.

Second, data collection without the explicit consent of users is also a problem. When collecting user information, the AI psychological consulting platform must clearly inform the user of the purpose, scope and use of the data, and obtain the explicit consent of the user. Otherwise, even if user

data is used for legitimate purposes, it may undermine user trust due to a lack of transparency.

In order to avoid the above problems, AI psychological counseling platforms should strictly comply with privacy protection regulations, such as the General Data Protection Regulation (GDPR) in Europe, to ensure the legality and security of user data. The platform should also strengthen internal management and strictly monitor the collection, storage, use and sharing of data to prevent data leakage and abuse.

Improper collection and use of user information is an urgent problem in the field of AI psychological counseling. Only by strengthening regulatory compliance, enhancing transparency, and strengthening internal management can we ensure that user privacy is fully respected and protected, thus promoting the healthy development of the AI psychological counseling industry.

3.2 Unauthorized data sharing and transfer

AI psychological counseling systems may behave improperly when sharing data with third-party institutions or partners. For example, without the explicit consent of the user, the system will share the user's psychological counseling data with advertisers or other non-relevant institutions, which directly violates the user's privacy rights. In order to protect privacy and realize data sharing, open standards and norms should be established, and principles such as sharing purpose, permission requirements, and access control should be clearly defined. Unauthorized data sharing violates these principles and may lead to data abuse and privacy disclosure. During data transmission, if appropriate security measures, such as encryption technology, are not taken, users' private data may be intercepted or tampered with. This unauthorized transfer of data can occur in cloud storage, network transmission, or data exchange between different systems. At the same time, AI robots need to store large amounts of data in the cloud or local servers and transfer it over the Internet. In the process, the data may be at risk of being hacked or stolen. If data is not adequately encrypted and protected, it will be easily accessed by hackers. Finally, insiders of AI psychological counseling systems, such as technicians or administrators, may also lead to privacy breaches if they access, copy, or transfer user data without authorization. This usually occurs when system security controls are not strict or when internal personnel are operating in violation.(As shown in table 4)

Table 4: AI psychological counseling privacy disclosure risk event table

No.	Time	Platform	Event description	Compromised data type	Consequence/ impact
1	July 2021	Mind helper AI	The hacker attack resulted in the leakage of user data	User's personal information, consultation records	User privacy is exposed, and the reputation of the platform is damaged
2	April 2022	Zhiyue Consulting	Unauthorized data sharing	User's personal information, consultation records	User complaints, regulatory penalties
3	January 2023	Chat without worry	Improper access to user data by internal employees	User personal information	Internal review, employee discipline

(Data source: Report issued by National Cybersecurity and Informatization Commission and Mental

4. Dilemmas and challenges of data protection in AI psychological counseling

4.1 Insufficiency of encryption algorithm and security protection technology

The encryption algorithms currently in use, while capable of providing some level of data protection in most cases, still have their limitations. With the enhancement of computing power and the continuous evolution of encryption technology, some traditional encryption algorithms may face the risk of being cracked. AI psychological counseling data has its particularity, including a large amount of text, audio and video data. This data may require more sophisticated encryption algorithms to keep it secure. However, the encryption algorithms currently on the market may not be fully adapted to this particular need. In addition, encryption algorithms need to be updated regularly to deal with new security threats and vulnerabilities. However, in the AI psychological counseling system, if the encryption algorithm is not updated in time, it may make the system face greater security risks. On the other hand, with the continuous evolution of network attack technology, security protection technology also needs to be constantly updated and iterated to meet new challenges. When users use AI psychological counseling systems, their behavior can be unpredictable. For example, users may use the system in an insecure environment, or use insecure behaviors such as weak passwords, which can pose challenges to security protection technologies[5].

4.2 Users have an increasing demand for data security and privacy protection

With the widespread use of the Internet and the frequent exposure of information leakage incidents, the public's awareness of personal data security and privacy protection has increased significantly. They pay more attention to the collection, storage and use of personal data during psychological counseling. In AI psychological counseling, the user's psychological data contains highly sensitive information such as mental health status, personal experience, and so on. Users are worried that the data will be improperly used or leaked, which may lead to social discrimination, psychological pressure and other problems. In addition, although encryption algorithms and security protection technologies continue to advance, they still face technical limitations[6]. At the same time, how to ensure that these technologies can adapt to the special needs of AI psychological counseling, such as processing large amounts of text, audio and video data, is a challenge. And with the increasing perfection of data protection regulations, AI psychological counseling systems need to ensure compliance with data processing. However, there are differences in regulations in different countries and regions, which creates challenges for the design and operation of the system.

5. Countermeasures and suggestions for applying artificial intelligence to psychological counseling

5.1 Technical countermeasures

(1) Strengthen data encryption technology

Adopt advanced encryption technology to encrypt users' personal information and consulting data, ensure the security of data during transmission and storage, strictly control the access rights of user data, ensure that only authorized personnel can access and use user data, and clearly explain the purpose and method of data collection, use and sharing to users. And data processing under the premise of user consent. It can also give users the control over their personal data, allowing them to view, modify and delete their data at any time, improve users' awareness and ability to protect privacy,

and help them better protect their personal privacy[7].

(2) Establish a data backup and recovery mechanism

The collected user data is de-identified to remove the information that can directly identify the user and reduce the risk of data leakage. At the same time, the user data is backed up regularly, and a sound data recovery mechanism is established to cope with possible data loss or damage. It is also necessary to invest more resources in the research and development of advanced AI technology, ensure that its application in the field of psychological counseling is safer and more reliable, conduct regular security assessments of AI psychological counseling services, and timely discover and repair potential security vulnerabilities. The trust assessment of AI psychological counseling services by independent third-party institutions will improve users' trust in them.

5.2 Management Level Countermeasures

(1) Strengthen staff training

Conduct privacy and data protection training for employees of psychological counseling institutions to enhance their awareness of privacy protection and ensure that they comply with relevant policies and regulations. At the same time, through publicity and education activities, improve users' awareness and attention to privacy and data protection, guide users to correctly use AI psychological counseling services, and protect their privacy and data security.

(2) Establish a sound supervision mechanism

On the one hand, psychological counseling institutions should formulate clear privacy and data protection policies, clarify the rules and processes of data collection, storage, use and sharing, and ensure the security and privacy of user data. It is also necessary to set up a special supervisory body or entrust a third-party institution to supervise and evaluate the privacy and data protection work of psychological counseling institutions to ensure the implementation and landing of the policy.

5.3 Countermeasures at the legal and regulatory level

(1) Establish industry standards and norms

First of all, it is necessary to formulate and promote industry standards and norms, guide psychological counseling institutions to consciously comply with relevant regulations, and improve the level of privacy and data protection of the entire industry. At the same time, we should strengthen cooperation and exchanges with the international community, learn from foreign advanced privacy and data protection experience and technical means, and enhance China's AI psychological counseling ability in privacy and data protection.

(2) Strengthen law enforcement

On the one hand, government departments should speed up the formulation and improvement of relevant laws and regulations, clarify the legal responsibilities and obligations of psychological counseling institutions in terms of privacy and data protection, provide legal protection for the development of AI psychological counseling, and promote cooperation between different departments in data protection, jointly develop industry standards and best practices, and ensure the compliance of AI psychological counseling services. On the other hand, the government should increase the penalties for violations of laws and regulations, and severely crack down on violations of user privacy and data security, forming an effective deterrent effect. Strengthen the supervision of AI psychological counseling services, and seriously deal with violations. Establish a complaint and reporting mechanism to encourage users to actively report violations and protect their legitimate rights and interests.

5.4 Improve the ethical awareness of AI technology

First, when discussing how to integrate ethical principles into the design and application of AI technical advisory systems, we should abide by ethical principles such as respect, do no harm, and fairness⁴. In order to realize these ethical principles, in the design of AI technical consultation system, we can set up a special ethical review committee to conduct an ethical evaluation of the system's algorithms and models to ensure that they meet the basic requirements of respecting user privacy and not infringing on user rights and interests.

The ethics review committee can regularly review the algorithms and models of the AI technical advisory system, assess whether there are potential ethical risks, and make recommendations for improvement in a timely manner. Through ethical education and training for AI technology practitioners, we can cultivate their sense of responsibility and moral awareness, enabling them to make correct decisions when faced with ethical dilemmas.

It is an important and urgent task to integrate ethical principles into the design and application of AI technical advisory systems. By setting up ethics review committees and strengthening ethics education and training, we can provide a strong guarantee for the healthy development of AI technology, while ensuring that users' rights and privacy are fully respected and protected.

Second, when exploring how to improve the professionalism and effectiveness of psychological counseling, we found that man-machine collaborative model showed significant advantages in mental health services. This model not only integrates the convenience and efficiency of AI technology, but also gives full play to the professional advantages of human psychological counselors, so as to provide users with more personalized and professional psychological counseling services.

AI technology is able to provide users with initial psychological assessments and recommendations through data analysis and algorithm optimization, while human psychological counselors carry out in-depth interpretation and personalized intervention on this basis. This collaborative way of working not only improves the quality and efficiency of the service, but also enhances the user's trust and satisfaction with the AI psychological counseling system. After the initial interaction with AI, users can get further guidance from professional psychological counselors and the man-machine collaboration model also shows its unique value in dealing with complex psychological problems. For example, for some psychological conditions that require long-term tracking and intervention, AI technology can continuously monitor the user's state changes and provide timely feedback to psychological counselors. This enables psychological counselors to more accurately grasp the psychological dynamics of users, so as to provide more accurate and effective consulting services.

Promoting man-machine collaboration is the key way to improve the professionalism and effectiveness of psychological counseling. By giving full play to the advantages of AI technology and human psychological counselors, we can provide users with more comprehensive and personalized psychological counseling services, and then promote the sustainable development and innovation of the mental health service industry.

6. Conclusion

With the continuous progress of technology and the increasing perfection of the legal environment, AI psychological counseling is ushering in new development opportunities in terms of privacy and data protection. The rise of blockchain technology, with its decentralized and immutable characteristics, provides new possibilities for the privacy protection of AI psychological counseling. Building a blockchain-based user data management system is expected to achieve transparency, security and traceability of user data, so as to effectively prevent data leakage and abuse.

The application of distributed machine learning technologies such as federated learning has also

brought new breakthroughs to AI psychological counseling. These technologies can improve the accuracy and efficiency of AI psychological counseling while protecting user privacy, and provide users with safer and more reliable counseling services. Looking to the future, with the continuous innovation of technology, we have reason to believe that AI psychological counseling will make greater breakthroughs and progress in privacy and data protection.

Based on the discussion of the existing literature and the results of this study, future studies can further explore how to better integrate ethical principles in the AI psychological counseling system, and how to build a more perfect privacy protection mechanism[8]. Research should focus on the application potential of new technologies in AI psychological counseling, and propose implementation strategies and optimization programs.

References

- [1] Zhao Xiangshuang, Xiong Weirui. *New school mental health service based on artificial intelligence and its challenges* [J]. *Mental Health Education in primary and secondary schools*, 2024(9):4-8, 13.
- [2] Gao Hui, Yang Jiawei, Wang Man. *Artificial intelligence intelligent psychological counseling decision-making suggestions* [J]. *Journal of Curiosity*, 2019(10):12-13. (in Chinese)
- [3] Guo Yi, Hou Chenyu. *Application of artificial intelligence in mental health services of primary and secondary schools* [J]. *Chinese Journal of School Health*, 2021, 42(8):1124-1128. (in Chinese)
- [4] Guangzhou Hengyuan Health Information Technology Co., LTD. *A psychological counseling robot, system, control method and storage medium: CN202310743021.1* [P]. 2023-10-13.
- [5] Kosinski, M., Stillwell, D., & Graepel, T. (2013). *Private traits and attributes are predictable from digital records of human behavior*. *Proceedings of the National Academy of Sciences*, 110(15), 5802-5805.
- [6] Fogelman, E. A., & Kleinman, A. (2018). *Ethical considerations in the use of artificial intelligence in mental health*. *American Journal of Psychiatry*, 175(7), 615-621.
- [7] Gove, D., & Wang, H. (2020). *Artificial intelligence and mental health: Opportunities, challenges, and ethical considerations*. *JMIR Mental Health*, 7(1), e17470.
- [8] Wang Tao, Zhan Xiaojun, Yu Wei. *The impact of AI perception on employees' psychology and behavior and its theoretical explanation* [J]. *Progress in Psychological Science*, 2024, 32(07):1195-1208.