Journal of Artificial Intelligence Practice (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2024.070317
ISSN 2371-8412 Vol. 7 Num. 3

Research on Security and Privacy Protection Policies of Artificial Intelligence in Primary and Secondary Education

Liu Che

Beijing National Day School, Haidian District, Beijing, 100039, China

Keywords: Artificial Intelligence; Public Policy; Large Model; education Security and Privacy Protection

Abstract: In primary and secondary education, the application of artificial intelligence (AI) technology has brought many conveniences and innovations, but it has also raised concerns about security and privacy protection. To ensure the healthy and sustainable development of AI technology in education, it is necessary to formulate and implement a series of security and privacy protection policies. By formulating and improving relevant laws and regulations, strengthening network security protection, implementing data anonymization, and providing user exit options, we can ensure the safe, fair, and transparent use of AI technology. Only in this way can we truly play the positive role of AI technology in the field of education while protecting the privacy rights and interests of students.

1. Introduction

At present, UNESCO has adopted the world's first normative framework for AI ethics, the "Recommendation on the Ethics of Artificial Intelligence," which has been formally adopted by its 193 member states. This framework aims to guide the construction of the necessary legal framework to ensure the healthy development of AI and realize the advantages of AI for society.

In addition, the European Union has also released the "Ethical Guidelines for Trustworthy Artificial Intelligence", which is a document on ethical considerations for the application of artificial intelligence in education, emphasizing the ethical challenges faced in the field of education. The U.S. Department of Education has also issued relevant guidelines to provide guidance for the application of AI in education. China is also actively formulating relevant policies and standards. For example, in January 2024, the Ministry of Education of China announced that it will implement the artificial intelligence empowerment action to promote the deep integration of intelligent technology with education, teaching, and scientific research. At the same time, the National Commission for UNESCO of China participated in relevant discussions and policy formulation.[1]

2. The rapid development of artificial intelligence technology in the field of primary and secondary education

Artificial intelligence technology has made remarkable achievements in the past decade, which are manifested in eight aspects: knowledge engineering, data mining, pattern recognition, natural language processing, intelligent machines, expert systems, automatic programming, and artistic

creation. These breakthroughs have provided impetus for the development and transformation of education.

The Chinese Academy of Educational Sciences has conducted a comprehensive survey on the current situation of artificial intelligence curriculum teaching and technology-empowered education in primary and secondary schools in China, aiming to provide effective path references for future primary and secondary school artificial intelligence education. Artificial intelligence technology is gradually surpassing its traditional role as a technical tool and becoming one of the main forces driving educational transformation and innovation.[2]

In summary, the application of artificial intelligence in primary and secondary education is gradually deepening, from personalized learning to intelligent assessment, from teaching assistance to curriculum development, AI technology is reshaping the educational ecosystem, providing new ideas and tools for building a more efficient and equitable future education system.[3]

3. Urgency of Security and Privacy Protection Issues

The application of artificial intelligence in primary and secondary education has indeed brought many conveniences, such as personalized learning, automated assessment, and intelligent management. However, with the widespread application of these technologies, privacy protection and data security issues have become increasingly prominent, becoming urgent problems that need to be addressed.

Firstly, artificial intelligence technology in education requires the collection of a large amount of student personal information, including biometric data such as facial recognition, fingerprints, and expressions. If these data are improperly used or leaked, it will seriously infringe on the privacy rights of students and may have adverse effects on their future development. Therefore, formulating strict privacy policies and data security measures is an important means to ensure the rights and interests of students.[4]

Secondly, there is a contradictory relationship between the open sharing and privacy protection of educational data. On the one hand, the open sharing of educational data can promote the optimal allocation and utilization of educational resources; on the other hand, excessive openness may lead to the compression of students' privacy space and even cause data leakage risks. Therefore, in promoting the governance of educational data, it is necessary to dynamically balance the relationship between the two and reconstruct the institutional ethical space based on privacy protection and open sharing.

In addition, AI applications in the field of education also face the problems of technology abuse and over-reliance. For example, the information collection methods of some educational products may infringe on the privacy rights of students. To address these issues, educational institutions and technology providers should take various measures, such as conducting security tests, evaluating systems, and other appropriate measures to ensure the security of the system. At the same time, it is also necessary to regulate the application of AI technology through legislation and regulatory frameworks to prevent illegal data storage, analysis, and sharing.[5]

Finally, enhancing the ethical risk awareness of teachers and students is also a prerequisite for ensuring the safe and reliable application of artificial intelligence technology.

In summary, while the application of artificial intelligence in primary and secondary education holds tremendous potential, the issues of privacy protection and data security it brings cannot be overlooked. Only through strict policy formulation, technical safeguards, and ethical education can we effectively address these challenges and ensure the healthy and sustainable development of artificial intelligence technology in the field of education.[6]

4. The deficiencies of existing security and privacy protection policies

In the process of applying artificial intelligence (AI) technology in primary and secondary education in China, there are obvious deficiencies in security and privacy protection policies. The following is a detailed analysis:

Inadequate laws and regulations: Currently, China lacks comprehensive laws and regulations, as well as corresponding punitive measures, for protecting student privacy. Although some local governments have introduced specific implementation details, there is still a need for further strengthening overall.

Low transparency in data collection and use: Educational platforms are capable of collecting and analyzing a large amount of behavioral data, but users do not truly understand how the data is collected, processed, and interpreted, which leads to issues of privacy protection and inequality. In addition, excessive reliance on artificial intelligence for tasks such as essay or report writing may hinder the development of students' critical thinking and creativity, and lead to issues such as personal information leakage or infringement.

Algorithmic Bias and Discrimination: AI systems may exhibit bias during the training process, which can affect their fairness. For example, algorithmic discrimination, opaque decision-making processes, and potential harm are issues that need attention. At the same time, bias in data training may also affect the fairness of the model.

Lack of a comprehensive ethical framework: Current regulations struggle to support a balance between fairness, individual teaching rights, data privacy, and effective data usage. Despite research recommendations for comprehensive policies to regulate the use of ethical AI and provide training and support for teachers, challenges remain in practical implementation.

Teachers lack sufficient awareness of security and privacy protection: Some teachers have a low level of understanding of new technologies and fail to prioritize the safety and personal privacy protection of students in the application of artificial intelligence. Therefore, teachers need to continuously learn and master the latest technological knowledge and applications to meet the teaching needs of the new era.

Balancing technology and regulation: To address the aforementioned risks, it is necessary to establish a scientific and impartial ethical framework, carefully consider data risks, actively implement the policy direction of United Nations conferences, support open educational resources and open science, and promote knowledge sharing and innovation.

When applying artificial intelligence in primary and secondary education in China, it is necessary to start from multiple aspects such as laws and regulations, data transparency, algorithm fairness, ethical framework, teacher training, and technical supervision to comprehensively improve the level of security and privacy protection, ensuring the healthy development of artificial intelligence technology in the field of education. [7]

5. Policy Suggestions and Implementation Strategies

The United States has formulated policies on security and privacy protection for the application of artificial intelligence in education. In the United States, the development of educational artificial intelligence not only includes innovation in teaching content and form, but also involves the realization of personalized learning and interactive learning, as well as providing universal opportunities for special students and conducting educational assessments. In addition, the United States has emphasized the development of relevant standards and the adoption of educational data privacy protection measures in its development strategy for educational artificial intelligence, indicating that the United States has already established certain security and privacy protection policies for the application of artificial intelligence in education.

In the application of artificial intelligence education, balancing the relationship between

technological development and personal privacy protection is a complex and multidimensional challenge. We have the following policy suggestions.

Firstly, technological development has brought about a huge demand for data, especially in mobile devices and intelligent systems. This data often contains sensitive information, and its security and privacy protection have become an important consideration. For example, Federated Learning proposes a method for model training without sending data to a central server, which helps reduce the risk of data leakage and protect user privacy.

Secondly, the application of machine learning and deep learning technologies has not only driven the revolution in multiple industries but also raised concerns about privacy protection. Therefore, it has become particularly important to study how to protect privacy during the machine learning process.

Thirdly, legal protection is crucial to ensuring the security of personal privacy. With the advent of the era of artificial intelligence, the security of personal information faces unprecedented challenges. Therefore, it is necessary to establish sound laws and regulations to protect personal information, clarify the principles and rules for handling personal information, and set up institutions dedicated to protecting personal information. In addition, it is also necessary to strengthen individuals' awareness of privacy rights and self-protection awareness.

Fourth, in the face of the dilemma of privacy protection in the era of artificial intelligence, it is necessary to redefine the scope of privacy, strengthen the enforcement of privacy protection, strengthen technical supervision, build industry self-regulatory mechanisms, and raise citizens' awareness of privacy protection. At the same time, it is necessary to clarify the scope and restrictions of data sharing through legislation, strengthen the supervision of data sharing, and improve the responsibility and relief mechanism for data sharing that infringes privacy, in order to achieve a balance between data sharing and personal privacy protection

In summary, although AI education systems have adopted various measures to protect student privacy and data security, they still need to be continuously optimized and improved to cope with increasingly complex challenges and risks.

6. Conclusion

Formulating policies for the security and privacy protection of artificial intelligence in primary and secondary education requires comprehensive consideration of various factors, including laws and regulations, ethics and morality, technical standards, and practical operations. The application of artificial intelligence in primary and secondary education faces significant challenges in security and privacy protection. The main problems include the high risk of student data leakage, unfair distribution of educational resources due to algorithmic bias, infringement of students' rights and interests due to technology abuse, and weak security awareness among teachers, students, and parents. In response to these problems, the following countermeasures are proposed: establishing and improving relevant laws and regulations, strengthening technical supervision and audit mechanisms, enhancing public awareness of artificial intelligence security and privacy protection, and promoting algorithm transparency and fairness to ensure the healthy and safe application of artificial intelligence technology in primary and secondary education.

References

[1] Alkaeed M, Qayyum A, Qadir J. Privacy preservation in Artificial Intelligence and Extended Reality (AI-XR) metaverses: A survey[J]. Journal of Network and Computer Applications, 2024, 2-3

[2] Bárcena C L J, Ducange P, Marcelloni F, et al. Increasing trust in AI through privacy preservation and model explainability: Federated Learning of Fuzzy Regression Trees[J]. Information Fusion, 2025, 1-4.

[3] Ferdowsi M, Hasan M M, Habib W. Responsible AI for cardiovascular disease detection: Towards a privacy-preserving and interpretable model. [J]. Computer methods and programs in biomedicine, 2024, 3-5.

[4] K N, P V. Federated Learning in Healthcare: A Privacy Preserving Approach. [J]. Studies in health technology and

informatics, 2022, 3-4.
[5] Jegadeesan, Subramani, Obaidat, et al. Efficient privacy-preserving anonymous authentication scheme for human predictive online education system[J]. Cluster Computing, 2021, (prepublish):1-3
[6] Korn F M, Filipe L N, Robyn D G, et al. Digital Education for the Deployment of Artificial Intelligence in Health Care. [J]. Journal of medical Internet research, 2023, 25 2-3
[7] AL-Ghamdi A S A, Ragab M, 234. Artificial Intelligence Techniques Based Learner Authentication in Cybersecurity Higher Education Institutions[J]. Computers, Materials & Continua, 2022, 72(2):1-2.