REVIEW

Ethics of Artificial Intelligence in Education: Student Privacy and Data Protection

Lan Huang

Guangxi Medical University, Nanning 530021, Guangxi, China

***Abstract**: Rapid advances in artificial intelligence (AI) technology are profoundly altering human societies and lifestyles. Individuals face a variety of information security threats while enjoying the conveniences and customized services made possible by AI. The widespread use of AI in education has prompted widespread public concern regarding AI ethics in this field. The protection of pupil data privacy is an urgent matter that must be addressed. On the basis of a review of extant interpretations of AI ethics and student data privacy, this article examines the ethical risks posed by AI technology to student personal information and provides recommendations for addressing concerns regarding student data security.*

Science Insights Education Frontiers 2023; 16(2):2577-2587.
Doi: 10.15354/sief.23.re202

How to Cite: Huang, L. (2023). Ethics of artificial intelligence in education: Student privacy and data protection. Science Insights Education Frontiers, 16(2):2577-2587.

***Keywords:** Ethics, Artificial Intelligence, Students, Data Privacy, Data Security, Data Protection*

***About the author**: Lan Huang, Guangxi Medical University, Nanning 530021, Guangxi, China. E-mail: 794594395@qq.com*

***Correspondence to**: Lan Huang in Guangxi Medical University of China.*

***Conflict of Interests**: None*

ARTIFICIAl intelligence (AI) has emerged as a key technology in the industrial transformation of the next generation by integrating a large number of new technologies and theoretical accomplishments. AI can perform intelligent screening of educational information and scenario reproduction, automated recognition and response to fuzzy learning tasks, and neural network simulation of human brain operation mechanisms with the assistance of speech recognition, computer vision, and natural language processing enabled by intelligent analytics. The application of AI can significantly enhance the efficiency and effectiveness of education, fostering intelligent education and interactive learning. Nonetheless, amidst the rapid development of intelligent processing technology, privacy infringement and data leakage risks emerge, posing grave threats to the security of student personal information, such as the disclosure of personal information due to the "secondary exploitation" of students' private data and network frauds caused by data trafficking. Problems such as the insufficient privacy protection system and the monopoly of network technologies have become increasingly threatening, necessitating research into the ethical risks of AI to student data security.

Interpretations of AI Ethics and Student Data Privacy

Ethical Principles Underpinning AI

The ethical risks associated with AI have attracted the attention of governments, organizations, and academics from various nations, prompting in-depth reflections on the relationship between humans and technology. The "*Ethical Rules for New-generation Artificial Intelligence*" released by the Ministry of Science and Technology of China in 2021, for instance, emphasized that the use of AI must contribute to maximizing human well-being. Identifying the ethical principles underlying AI technology is essential for mitigating its dangers to humanity.

Protection of Fundamental Human Rights and Dignity

As stated in UNESCO's *Recommendation on the Ethics of Artificial Intelli-*

gence, it is crucial for AI systems to respect, safeguard, and advance human rights, fundamental freedoms, and dignity at all stages of their development (UNESCO, 2022). AI technology offers several benefits to society, including the potential to free people from boring and repetitive work and the ongoing improvement of their decision-making and problem-solving skills. However, it is crucial that human beings always come first in the creation of AI and that their individuality is never infringed upon. Users of AI technologies should have enough autonomy to protect and support their individual rights and freedoms. Furthermore, it is crucial to safeguard human agency and refrain from objectifying people in any way that compromises their dignity in the context of the popularization of intelligent functions such as automated processes and tailored recommendations. People should still have the chance to develop the qualities essential to humanity and grow into their full potential.

Right to Privacy and Data Protection

The right to privacy is crucial to the protection of human dignity, autonomy, and agency. AI technology is based on the collection of vast volumes of data in all of its subfields. It is critical that data processing and consumption adhere to the notion of privacy and security. The retention period of information has been greatly expanded thanks to the Internet. As a result, data for AI systems must be gathered, used, shared, stored, and removed in accordance with information security standards. Personal information involved in the lifespan of AI technology should be safeguarded by legal frameworks as well as ethical norms. To ensure informed consent for data usage, personal information must not be collected, used, or disclosed without the approval of the data subjects (UNESCO, 2022).

Responsibility and Accountability

All AI actors are held accountable for the protection and promotion of human rights and dignity and are required to assume their respective ethical and legal responsibilities based on their positions in the lifecycle of the AI system's decisions and actions. To ensure accountability for AI systems and their effects, appropriate oversight, impact assessment, and due diligence evaluation should be developed.

In the midst of the present surge of expedited advancement in the field of artificial intelligence, the technology is progressively being assimilated and implemented across various domains. The emergence of machines that resemble humans has presented a novel challenge in determining accountability (Zhang, 2022). Educational AI holds promise for enhancing school management and services, optimizing instructional efficacy and re-

sults, and fostering self-development among students. Notwithstanding the advantages of AI applications, it is imperative to acknowledge the underlying concerns pertaining to accountability. Within the conventional educational framework, communication between teacher and student is a bilateral exchange that encompasses emotional interactions. When utilizing educational AI tools like intelligent guidance systems and intelligent learning partners, students can receive prompt feedback on their learning outcomes through self-assessment. However, these automated responses may not provide sufficient encouragement for students who are less academically resilient and lack self-motivation. The implementation of machine assessment and its automated marking feature has proven advantageous in enhancing the efficiency of teachers. However, in the event of marking errors, who bears the responsibility for such inaccuracies? The inquiry pertains to whether the individual in question is the programmer or the user. It is imperative to address such concerns within legal and ethical paradigms to ensure the sustainable advancement of educational AI.

Studies have examined AI ethics from a variety of perspectives. Regarding risks of AI, Zhao et al. (2021) asserted that current AI ethical concerns are primarily over issues such as undermined human decision-making autonomy, privacy protection, social equity, security responsibility attribution, and ecology, whereas Tan and Yang (2019) argued that risks of AI technology arise from the black box of algorithms, the difficulty in balancing value rationality and instrumental rationality, and the limitations of humans in risk perception and decision making. Existing research on the ethics of AI applications has examined topics such as the attribution of responsibility for intelligent driving (Si & Cao, 2017), the judicial fairness of intelligent justice (Luo & Li, 2021), the "information cocoon" effect in information push services (Peng, 2020), and the dignity of elderly individuals under robot care (Sharkey, 2014). Algorithms are the driving force behind the development of artificial intelligence. In the age of algorithms, issues such as the leakage of private information, asymmetric power of knowledge, covert operations, and algorithmic infringement are inevitable, according to Guo (2021). Decision-making based on algorithms may exacerbate inequality, opaqueness, and manipulation in human society. As for the governance of ethical issues in artificial intelligence, existing research has proposed mitigating measures from the perspectives of public policies, technological optimization, human-machine relationship modification, etc. Xue and Zhao (2019) proposed that the government should establish agile governance-based frameworks for the development and supervision of AI and other emerging industries; Jia and Jiang (2017) mentioned that the AI era's effective public policy making depends on improved algorithms and data governance frameworks, social governance mechanisms, and global governance systems.

Hao et al. (2019) proposed that the implementation of educational AI technology and systems should prioritize student-centered education and encourage collaboration between educational actors and machines. This approach can effectively support the digital transformation of education. The significance of the association between educational agents and educational AI is underscored by Liu et al. (2021) as a crucial element of research on ethical considerations regarding educational AI.

Student Data Privacy

Privacy is commonly viewed as the right of individuals to maintain a personal space free from interference or invasion by other individuals or entities. Clarke (1999) divides privacy into privacy of the person (concerning the physical integrity of the individual), privacy of personal conduct, privacy of personal communications, and privacy of personal information. Data privacy refers to the claims of individuals that information about them should not be accessible to other individuals and organizations and that when data is in the possession of a third party, the individual must have the right to control the data and its use.

The proliferation of the Internet and big data, coupled with the growing prevalence of online academic, social, and personal activities, has led to a significant increase in the volume of private information that is being uploaded to and stored by various platforms. This includes basic personal information, such as name and mobile phone number, which is required to access a platform, as well as personal computer information, such as IP address, which is recorded by the browser. Additionally, interactive behavior information, such as browsing history and purchase records, is being retained on the Internet. Although media and platforms may anonymize collected private information to generate data that does not disclose personal identity, big data mining and analytics can still make relevant personal data accessible, thereby enabling the direct or indirect identification of specific individuals. The unauthorized acquisition and exploitation of said information by external entities or individuals may result in significant detrimental effects on the well-being of the individuals whose data is concerned.

The capacity of AI systems to identify information about student users has significantly increased in the educational setting thanks to improved intelligent processing technology and the proliferation of big data applications, and the security boundary of personal information privacy is becoming more and more blurred. Private student information includes data traces left over from the online learning process, like network browsing history, download history, and location, among other things. Learning status, behavioral preferences, and even personality features of specific students may be

able to be extracted from these data through intelligent collection and analysis, which are essential elements of student data security.

The preservation of people's data privacy has been a focus of policymaking and scholarly research since information about students' learning behavior is "semi-transparent" due to the usage of intelligent learning analytics. The phrase "right to be forgotten" was first used in Europe (Shi & Zhou, 2022). More recently, in 2018, the strict *General Data Protection Regulation* was updated, emphasizing the right of data subjects to request that data controllers delete their personal information in certain situations (Hoosnagle et al., 2019). In order to improve the security of student data in use, Zhao and coworkers (2016) investigated the problem from a technical perspective and recommended developing privacy protection frameworks in the processes of data collection, data processing, and data application. The establishment and operational procedures of agencies for student privacy protection are outlined in Wang's (2016) study of the legislative and governance structure of educational privacy regulation in the United States.

Current Challenges in the Protection of Student Data Privacy

Schools, teachers, and students become the primary producers of copious amounts of private data in digital formats as a result of the digital transformation of education, but they have little autonomy over this data. As a result, there are serious issues with protecting student privacy because vast amounts of educational data are instead controlled and in the possession of third-party institutions, with schools, teachers, and students acting as simply passive data suppliers.

Increased Risks of Information Monopoly by Intelligent Educational Platforms

Educational platforms of major Internet corporations, including open online course platforms such as Coursera, Udacity, and EdX, store and keep data from educational actors. The inclination of these technologically and financially privileged Internet businesses towards data monopolies is cause for alarm. Since mining processing and subsequent correlation analysis of personal data have become major means of creating value, online educational services tend to prohibit users from modifying standard data formats or structures with the goal of acquiring user information resources. Following extensive processing, student information obtained by these businesses may be turned into data that differs from its original form and used for other profit-seeking or even criminal purposes. Edmodo is a startup that provides

communication, collaborative learning, and course guidance platforms for students and teachers through educational technology. Its application was named one of the "Top Apps for Teachers" by PC Magazine (Thongmak, 2013), and it claimed to have more than 78 million users globally as of July 2017. The platform's built-in Double-Click advertising service was discovered to be capable of intelligently tracking user data flow, including web pages browsed, time spent on the website, IP addresses, and e-mail addresses, in the same year. These data, once analyzed, could be used to identify more personal information about the user. As a result, information monopolies not only hinder data sharing by erecting data barriers and divisions, but they also severely limit students' control over their personal information.

Breaches of Educational Data Security Due to the Lack of Privacy Protection Regulations

The process of digitization confers digital characteristics on the human experience. In the current era of AI, the interconnectedness of all entities and the coexistence of humans and computers have led to the ubiquitous documentation of individuals' conduct within data network systems. According to Jiang (2019), the pervasive nature of surveillance poses potential risks to the privacy of both teachers and learners.

As an emerging technology, AI is constantly evolving, which means its applications may be susceptible to a variety of vulnerabilities. Security issues with "3D" facial recognition systems, fingerprint recognition systems, and other management-related application systems, as well as the prevalence of data system hacking, have prompted extensive public debates. AI applications such as smart headbands and facial recognition check-ins have raised grave concerns regarding the security of student data in the educational setting. In spite of the fact that AI educational technology enables personalized education, the risk of data breaches and associated dangers will increase substantially as both things and people become data generators and media.

Given that data can be used as resources and instruments to pursue profits, relevant entities may violate educational ethics by misusing data to maximize its value. In contrast to explicit phenomena of infringement, black box algorithms in the AI era (Audet et al., 2016) have the potential to embed discrimination and infringement into decision-making automatically. Routine algorithmic discrimination, information control, and invasions of privacy will result in institutionalized violations. In scenarios involving AI in education, teacher and student data are not only crucial for educational decision-making but also have substantial commercial value. The data monopoly of educational platforms can lead to the exploitation of instructor and student data for profit-driven, non-educational purposes.

Deviation from the Original Intention of Informed Consent

In the traditional information society, the notice-and-consent mechanism ensures that data subjects have the autonomy to determine by who and how their private information is processed. The "notice-and-consent framework," such as the EU's Data Protection Directive, stipulates that system developers must embed privacy statements into the application system when designing the software to inform the user what data will be collected and for what purpose, and to allow the user to decide whether or not to authorize the use of their personal information (Cate & Mayer-Schonberger, 2013). Nonetheless, as a result of AI technology, the flaws of this practice are becoming increasingly apparent. Users of AI educational technology are typically required to consent to the privacy policy in order to access the corresponding software, which violates their right to autonomy. In addition, students find the concept of informed consent to be an intolerably time-consuming burden. Typically, software developers generate lengthy and obscure privacy statements in order to comply with legal requirements. In the majority of instances, students tend to disregard the detailed provisions of the privacy statement and instead select "I agree" to save time, contrary to the original intent of the notice-and-consent framework.

Strategies for Protecting Student Data Privacy

Optimizing the Regulation of Personal Data Usage

In the creation of data privacy protection frameworks, the optimization of privacy-protecting regulatory policies is a challenge shared by all nations. Due to the immaturity of the personal data market, it is necessary to coordinate the complementary roles of market mechanisms and legal regulatory regimes in the regulation of data privacy and security in order to establish a scientific regulatory framework for the protection of personal information (Tang & Wang, 2020). To overcome the limitations of the unilateral regulatory model, it is necessary to establish a professional data supervision agency led by the government and involving multiple stakeholders, including schools and businesses, in order to ensure the effective usage of data that conforms to legal requirements and public norms.

Enhancing Students' Awareness of Personal Data Protection

Enhancing student self-protection awareness is particularly crucial while the legal framework for personal data protection is still being debated. First, through classroom instruction, case studies, or participation in data management, inform students of the extent of personal data privacy, the dangers of personal data leaking, and the basic, doable steps for protecting personal information. Second, educate students about the uses of data and the difficulties associated with big data and develop their awareness of assessing privacy risks in regular online activities. Tell them to install privacy security shields, exercise caution when authorizing open permissions, and carefully read the "authorization instructions" to determine privacy risks when using social media. Third, assist students in comprehending the fundamentals and features of big data and AI technologies. Also, urge them to keep track of network security issues and actively participate in training and education on the value of personal privacy and the dangers of information leaks.

Providing Students with Legal Remedies against Infringement of Data Privacy

Students have a legal right to privacy protection. There is currently no institutionalized legal protection for student personal data, and schools have not adequately addressed students' rights to privacy (Liu, 2016). Although school-based remedial procedures for student data privacy are currently lacking, the school administration is legally liable for protecting students' educational privacy (Sun, 2007). The school should strengthen its complaints mechanism and strike a fair balance between student privacy and its smart administration. In order to ensure that student-accessible AI applications are held accountable for student data protection, students should also have access to legal remedies from pertinent governmental bodies.

Improving IT Industry Self-Regulatory Mechanisms

The self-regulatory mechanism of the educational technology industry can play a positive role in developing a consensus about user privacy protection and balancing the interests of all stakeholders, whereas overly stringent legal regulations may discourage IT companies from investing in educational AI technology development. A sound IT industry self-regulatory mechanism provides AI practitioners with professional norms and acts as a conduit for supervision from peers, parents of students, education administrators, and other parties in society, which has significant effects on regulating their professional conduct (Chen & Yu, 2018). Compared to the enforcement of legal regimes, industry self-regulation is more practical for preserving student data privacy in the context of constant technological evolution and the exponen-

tial growth of AI. AI Industry associations can play a key role in optimizing network identity verification systems, enhancing security evaluation of AI applications, and standardizing ethical impact assessment for emergent AI technologies. Integrating scientific ethics and social responsibilities throughout the entire lifecycle of AI systems, from technological research and development to data collection, analysis, processing, and stewardship, can promote the sustainable, healthy development of AI and increase public confidence in the technology.

Conclusion

The widespread adoption of AI technology in education is necessarily reducing student privacy while gradually increasing the amount of student data. As difficulties relating to student data security become more complicated, educational institutions, governments, and AI actors must work together to create an efficient data protection framework. In a world that is rapidly changing and becoming more electronically connected, students' ability to grow and develop healthily depends on the preservation of their online privacy.

References

Audet, C., Le Digabel, S., & Tribes, C. (2016). Dynamic scaling in the mesh adaptive direct search algorithm for blackbox optimization. *Optimization and Engineering*, 17(2):333-358. DOI: http://dx.doi.org/10.1007%2Fs11081-015-9283-0

Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in the age of big data. *International Data Privacy Law*, 3(2):67-73. DOI: http://dx.doi.org/10.1093/idpl/ipt005

Chen, Y., & Yu, J. (2018). The Industry Self-discipline Mechanism of the Ontario Association of Early Education Personnel of Canada. *Journal of Shaanxi Xueqian Normal University*, 2018(2):118-122

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42(2):60-67. DOI: https://doi.org/10.1145/293411.293475

Guo, Y. (2021). The Cultural Implications and Ethical Risks of Algorithm Society. *Chinese Book Review*, 2021(9):45-53 DOI: https://doi.org/10.3969/j.issn.1002-235X.2021.09.006

Hao, X., Wang, F., & Qi, C. (2019). The current status and developmental trends of educational artificial intelligence. *Modern Educational Technology*, 2019(2):12-18.

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1):65-98.

Jia, K., & Jiang, Y. (2017). Three basic issues of artificial intelligence governance: Technical logic, challenges, and public policy making. *Chinese Public Administration*, 2017(10):40-45. DOI: https://doi.org/10.3782/j.issn.1006-0863.2017.10.07

Jiang, S. (2019). Rejecting surveillance cameras on campus. *Teachers' Perspectives*, 2019(12):2.

Liu, F. (2016). The protection of the rights of

college students. *Journal of Jiangsu College of Engineering and Technology*, 2016(3):59-62. DOI: https://doi.org/10.19315/j.issn.2096-0425.2016.03.014

Liu, S., Liu, S., Sun, J, Shen, X., & Liu, Z. (2021). Several key issues in the development of intelligent education. *Distance Education in China*, 2021(4):1-7+76. DOI: https://doi.org/10.13541/j.cnki.chinade.2021.04.001

Luo, H., & Li, X. (2021). Ethical issues in intelligent justice and countermeasures. *Journal of Political Science and Law*, 2021(1):148-160.

Ministry of Science and Technology of China. (2021). Ethical Rules for New-Generation Artificial Intelligence. Available at: https://www.most.gov.cn/kjbgz/202109/t20210926_177063.html

Peng, L. (2020). Multiple factors in the "information cocoon" effect and the paths to "breaking the cocoon." *Press Circles*, 2020(1):30-38+73. DOI: https://doi.org/10.15897/j.cnki.cn51-1046/g2.20191230.001

Sharkey, A. (2014). Robots and human dignity: a consideration of the effects of robot care on the dignity of older people. *Ethics and Information Technology*, 16(1):63-75. DOI: https://doi.org/10.1007/s10676-014-9338-5

Shi, Y., & Zhou, X. (2022). The debate on the "right to be forgotten" in the era of big data: To be remembered or forgotten? *Editorial Friends*, 2022(12):88-99. DOI: https://doi.org/10.13786/j.cnki.cn14-1066/g2.2022.12.012

Si, X., & Cao, J. (2017). On the civil liability of artificial intelligence: Using self-driving vehicles and intelligent robots as examples. *Science of Law (Journal of Northwest University of Political Science and Law)*, 2017(5):166-173. DOI: https://doi.org/10.16290/j.cnki.1674-5205.2017.05.016

Sun, P. Violations of student privacy in school management and legal considerations. *Journal of Teaching and Management*, 2007(5):17-19. DOI: https://doi.org/10.3969/j.issn.1004-5872-C.2007.05.005

Tan, J., & Yang, J. (2019). Ethical risks of artificial intelligence technology and collaborative governance. *Chinese Public Administration*, 2019(10):44-50. DOI: https://doi.org/10.19735/j.issn.1006-0863.2019. 10.07

Tang, Y., & Wang, L. (2020). An overview of theoretical research on data privacy protection. *Review of Industrial Economics*, 2020(5):95-108. DOI: https://doi.org/10.19313/j.cnki.cn10-1223/f.2020.05.008

Thongmak, M. (2013). Social network system in classroom: antecedents of Edmodo© adoption. *Journal of E-learning and Higher Education*, 2013(1):1-15. DOI: https://doi.org/10.5171/2013.657749

UNESCO. (2022). Recommendation on the Ethics of Artificial Intelligence. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000381137

Wang, Z. (2016). American student data privacy protection legislation and governance frameworks in the era of big data. *International and Comparative Education*, 2016(11):28-33. DOI: https://doi.org/10.20013/j.cnki.ice.2016.11.005

Xue, L., & Zhao, J. (2019). Paths to agile governance: The development of emerging industries and regulatory models. *Chinese Public Administration*, 2019(8):28-34. DOI: https://doi.org/10.19735/j.issn.1006-0863.2019.08.02

Zhang, Q. (2022). Transformation of modes of production in the age of artificial intelligence: An analysis based on the phenomenon of "human-like machines." *Journal of Socialist Theory Guide*, 2022(9):72-79.

Zhao, H., Jiang, Q., & Zhao, W. (2016). The security of big data-based learning analytics and privacy protection. *Modern Educational Technology*, 26(3):5-11. DOI: https://doi.org/10.3969/j.issn.1009-8097.2016.03.001

Zhao, Z., Xu F., Gao, F., Li, F., Hou, H., & Li, M. (2021). An evaluation of ethical risks in artificial intelligence. *China Soft Science*, 2021(6):1-12.

Received: 10 April 2023
Revised: 04 May 2023
Accepted: 30 May 2023