Macrothink Institute™

International Research in Education
ISSN 2327-5499
2025, Vol. 13, No. 1

Issues between Artificial Intelligence and Personal Data in Education

Konstantinos T. Kotsis

Department of Primary Education, University of Ioannina, Greece

Received: January 27, 2025 Accepted: April 30, 2025 Published: May 11, 2025

doi: 10.5296/ire.v13i1.22850 URL: https://doi.org/10.5296/ire.v13i1.22850

Abstract

The purpose of this paper is to investigate the complex relationship that exists between AI and personal data used in educational settings. The paper also highlights the importance of having a strong thesis statement to direct the research. A particular emphasis is placed on data privacy, security, and algorithmic bias in this study, which investigates the ethical concerns that are associated with the integration of artificial intelligence. In order to protect the students' right to privacy, it emphasizes the significance of obtaining informed consent and maintaining transparency in the data collection and processing processes. In spite of the fact that it acknowledges the difficulties that are posed by concerns regarding data privacy and security, the research highlights the potential benefits of artificial intelligence in terms of improving educational outcomes and personalizing learning experiences. Additionally, the paper emphasizes the importance of developing ethical guidelines and policies that are in line with the rapid advancements in artificial intelligence technology. This will guarantee that students' data rights are maintained and honoured. By addressing these important concerns, this paper seeks to add to a thorough knowledge of the ethical and legal difficulties related with including artificial intelligence into education. Furthermore, the study promotes a multidisciplinary approach to properly negotiate these complexity.

Keywords: Artificial Intelligence, Education, Data Privacy, Data Security, Ethical Implications

1. Introduction

As artificial intelligence technologies develop quickly, educational institutions use them increasingly to improve teaching and learning environments for teachers and students. This modern approach seeks to personalize education, increase involvement, and simplify administrative procedures, enabling learning to be more effective and fit individual requirements. However, this integration begs serious questions about the security and privacy of the personal information gathered from teachers and students across these procedures. The ethical consequences of how this information is handled, kept, and used are becoming increasingly important as artificial intelligence systems compile and examine enormous volumes of private data. In educational environments, where sensitive data, including academic performance and personal information, is often involved, data privacy, consent, and control over personal information become central points. This study intends to investigate the complicated interaction between artificial intelligence and personal data in education by analyzing the several difficulties that develop and the possible remedies to guarantee that the integration of AI technologies is morally right and responsibly carried out. Examining these relevant problems will help us create thorough policies and practices that protect individual privacy and rights, especially in the context of education, and guarantee that the advantages of artificial intelligence in education are used responsibly and respectfully of reference for personal data. This harmony is necessary to create an environment in which technology supports education without sacrificing the integrity or privacy of the engaged individuals.

2. Theoretical Background

By including AI in the classroom, personalized learning experiences and creative ideas have drastically changed the education scene. From conventional approaches to AI-driven technologies, educational technologies have historically changed to offer individualized, quick, easily available learning environments (Singh et al., 2024; Chen et al., 2020). Intelligent tutoring systems, personalized learning platforms, and educational chatbots, among other AI technologies, help teachers to understand student learning patterns better, pinpoint areas for development, and modify their teaching plans (Farahani & Ghasmi, 2024). These technologies provide individualized support to students with various needs and learning styles, fostering inclusivity (Farahani & Ghasmi, 2024). Artificial intelligence has improved higher education's study efficiency and personalized learning support, possibly leveling the academic playing field for students with different needs (Donnell et al., 2024). AI integration into education does not, however, present without difficulties. Major problems that demand attention are ethical ones including data privacy, algorithmic bias, and the digital divide (Kaddouri et al., 2024). Concerns about equity, teacher preparation, and possible student reliance on artificial intelligence could also cause less knowledge and skill development (Feng & Li, 2024). With AI turning their attention to more strategic and creative facets of the learning process, teachers' roles are also changing (Kujundziski & Bojadjiev, 2024). Educational institutions have to include these technologies into their pedagogical strategies while guaranteeing ethical and fair use if they are to exploit AI (Feng & Li, 2024)

fully. To close technology gaps, this entails building suitable regulatory frameworks, offering thorough teacher training, and encouraging world collaboration (Kaddouri et al., 2024; Feng & Li, 2024). As artificial intelligence technologies develop, they present fresh chances for cooperative learning, skill development, and lifelong education, so stressing the need of careful implementation strategies that give equity, inclusiveness, and ethical issues top priority (Farahani & Ghasmi, 2024). By tackling these issues, artificial intelligence can greatly improve educational systems by arming students for the possibilities and challenges of the future (Micheni et al., 2024).

For modern students in particular, personal data is essential for improving learning results and encouraging reflective practice. As the exploratory research project (Li, 2006) emphasizes, digital storytelling is a creative way to include multimedia technologies in the classroom so that students might consider their knowledge and viewpoints in teacher preparation. By means of digital storytelling, students confront professional challenges and practice self-assessment and introspection, so improving their language, media literacy, and visual skills. Furthermore, the possible influence of digital storytelling in higher education environments includes balancing traditional methods with new teaching approaches and meeting up-to-date educational technology standards, stressing the need to use personal data for complete educational experiences (Li, 2006). This focus on digital storytelling emphasizes the need for personal stories and reflections to enhance the learning process and support critical thinking and self-efficacy among students, so stressing the indispensable part of personal data in education.

Personal data is very important in education and presents both possibilities and problems. Digital platforms using personal data to improve learning experiences, track student progress, and raise institutional performance increasingly depend on educational institutions. However, since it tracks and profiles staff members and students, so influencing their educational and professional futures, this datafication process generates major social justice concerns (Pangrazio et al., 2024). Personal User Models for Life-long, Life-wide Learners show how personal data can empower learners by enabling them to control and use their data for self-monitoring and reflection, thus supporting metacognitive processes (Kay & Kummerfeld, 2019). Integrating technology into the classroom raises privacy issues, especially for culturally varied students who might be anxious about data intrusion and lack of control over their personal data (Kumi–Yeboah et al., 2023). In this context, trust is very important since students often trade personal information for supposed benefits—such as improved learning opportunities—but yet remain worried about privacy and the ethical use of their data (Slade et al., 2019). Although they provide some privacy protections, technological solutions are insufficient on their own; a thorough approach, including student agency and literacy, is required to properly handle privacy concerns (Prinsloo & Slade, 2015; Prinsloo et al., 2022). Proposed to guarantee student autonomy and guarantee data usage transparency are informed consent systems and privacy dashboards (Jones, 2019). Third-party vendors and the possibility of data leaks complicate the ethical consequences of data usage in education even more, so stressing the need of strong legal and organizational systems to safeguard student privacy (Alier et al., 2021). Effective integration of artificial intelligence in education, which

mostly depends on personal data, depends on knowledge of data flows and stakeholder practices, according to the educational data journeys framework (Howard et al., 2022). In learning analytics, privacy and data protection should ultimately be based on educational values, balancing legal, cultural, and pedagogical concerns to protect student privacy while using data for educational advancement (Hoel & Chen, 2018).

Artificial intelligence and personal data in education is a fast-developing area with great chances for tailored learning, but major obstacles are mostly related to data privacy and ethical issues. Analyzing enormous volumes of educational data to customize instructional content to individual students' needs improves learning outcomes and engagement. AI technologies help to enable personalized learning experiences (Zaman, 2024; Xiong et al., 2024; Kaswan et al., 2024). AI-powered tools like intelligent tutoring systems and recommendation engines, for example, use machine learning algorithms and data analytics to offer adaptive content delivery and customized feedback, enabling students to learn at their own pace and according to their particular strengths and weaknesses (Kaswan et al., 2024). Since these systems sometimes gather sensitive student information, including test scores and social interactions, which can lead to problems like too high surveillance and possible data breaches, the integration of artificial intelligence in education raises serious questions about data privacy and security (Ismail & Ahmad, 2024; Jose, 2024). Often insufficient to handle these issues, current rules call for creating thorough data governance rules and improved digital literacy to guard student privacy (Ismail & Ahmad, 2024). Furthermore, open algorithms and strong data governance systems will help to solve ethical issues including algorithmic bias and possible decline of student autonomy (Singh & Thakur, 2024). Effective integration of artificial intelligence with human-centered teaching approaches (Mappisabbi et al., 2024; Yılmaz, 2024) depends on major expenditures in technology infrastructure, teacher training, and pedagogical strategies as well. Provided ethical complexity is navigated responsibly to foster equity and inclusivity, AI has promise for transforming education by making learning more personalized, efficient, and accessible—despite these obstacles (Singh et al., 2024; Singh & Thakur, 2024). Thus, responsible integration of artificial intelligence in educational environments depends on a balanced approach that uses its advantages while safeguarding privacy and addressing ethical concerns (Zaman, 2024; Ismail & Ahmad, 2024; Jose, 2024).

As AI keeps transforming many fields, its interaction with personal data in education has generated major questions about privacy, security, and ethical consequences. By customizing learning activities and offering focused interventions for each student, artificial intelligence technologies—including machine learning algorithms—have the ability to improve educational opportunities. But gathering and evaluating enormous volumes of personal data—including academic performance, behavior patterns, and even biometric information—including students' academic performance, behavior patterns, and even biometric information begs significant concerns about consent, data ownership, and protection. Teachers, legislators, and technology developers, among other interested parties, have to negotiate this challenging terrain to guarantee responsible and open use of student data. Privacy laws protect people's data rights and guarantee responsibility for using artificial

intelligence in the classroom by means of the General Data Protection Regulation and others. Establishing best practices and ethical rules supporting artificial intelligence's advantages while safeguarding personal data privacy and security in educational environments requires group efforts (Miao et al., 2021).

Protecting personal data becomes a major issue as artificial intelligence keeps merging into learning environments. Establishing a clear thesis statement summarizing the research's main argument is crucial to handling this paper. The paper statement should clearly express the main idea or goal of the study, so guiding the direction of the research and forming the later analysis. Clearly stating the main argument of the research helps the thesis statement to guide the study by telling the reader of the scope and emphasis of the inquiry. Therefore, great attention should be paid to developing a strong thesis statement that captures the main points of the research topic and provides the basis for a careful review of the current problems. Establishing a cogent and convincing argument that advances our knowledge of this important junction depends on a well-defined thesis statement when addressing the complicated junction between artificial intelligence and personal data in education (Holmes & Porayska-Pomsta, 2023).

3. Ethical Concerns

Consent is one of the main ethical questions around the junction of AI and personal data in education. It is imperative to make sure people are completely informed about how their information will be used and have the chance to provide express consent as artificial intelligence systems gather and examine enormous volumes of sensitive data from students. Students might unintentionally have their data shared or used in ways that violate their right to privacy without appropriate permission systems. Moreover, algorithmic bias in artificial intelligence systems runs the danger of extending and maybe aggravating already existing educational disparities. Transparency in data collecting and processing techniques has to be given top priority in order to handle ethical issues together with strong steps to get informed permission from people. Moreover, constant observation and assessment of artificial intelligence systems in education is crucial to identify and stop possible ethical transgressions or prejudices (Holmes & Porayska-Pomsta, 2023).

Although they present major privacy issues, collecting and using personal data have become absolutely essential for contemporary digital services. The fast development of technologies including IoT, big data, and artificial intelligence has aggravated these problems since data collecting operations sometimes take place without clear user permission, so raising ethical and privacy issues (Chen, 2024). Emphasizing the need for legal frameworks to safeguard user data, the General Data Protection Regulation sets strict data collecting and processing rules, especially for businesses functioning inside the European Union, so addressing these issues (Mironova, 2022). The ubiquitous nature of data collecting in daily contacts, including credit card transactions and medical consultations, emphasizes the need for strong data protection policies to defend individual privacy (Mondal et al., 2022). Big data poses privacy issues that need policies balancing data utility with privacy preservation even while it

helps organizational development (Alwabel, 2019). Public privacy issues, including those around vehicle GPS tracking, highlight the need for openness and control over personal data to reduce privacy risks and support service adoption (Rohunen & Markkula, 2019). Gathering behavioral data through IoT devices in smart cities has to consider data flaws and interpersonal interactions while guaranteeing privacy, which is absolutely essential for building human-centric urban environments (Sei, 2024). Lastly, user profiling for tailored online services calls for careful data classification and anonymizing to safeguard user privacy; hence, recommendations for frameworks that enable regulated data sharing and lower privacy risks suggest These revelations highlight the complex nature of privacy concerns in personal data collecting and the need of thorough plans including legal, technological, and ethical aspects to safeguard user privacy in a society driven by data more and more.

Artificial intelligence systems' collecting personal data in educational environments begs serious privacy issues. AI compromises personal privacy rights even while it can improve educational opportunities and offer insightful analysis of student performance. If not sufficiently guarded, personal information including students' academic records, biometric data, and communication patterns may be vulnerable to use or illegal access. This problem is exacerbated even more by the absence of clear rules and guidelines for the moral use of artificial intelligence in education. Strong data security policies and openness systems are desperately needed, claims Santos and Radanliev, to protect people's privacy in 2023. Similarly, teachers and legislators have to give great thought to the consequences of personal data collecting so that the advantages of artificial intelligence are counterbalanced with regard for privacy rights.

Common across all sectors including biometric systems, financial markets, healthcare, and IoT devices, data security risks in artificial intelligence systems are many and include threats from adversarial attacks, data breaches, and unauthorized access. Adversarial attacks and identity theft pose major threats to AI-based biometric systems. Thus, strong validation and user authorization policies are absolutely necessary to preserve data integrity and privacy (Choudhry et al., 2024). AI-based code understanding systems such as OpenAI Codex can unintentionally create code snippets, including sensitive information in software development, causing possible illegal access and use (Adhyapak et al., 2024). Highly dependent on artificial intelligence and machine learning, financial markets are vulnerable to data mishandling and cyberattacks, causing financial losses and erasing system confidence (Gupta & Shah, 2023). Although they lower central points of failure, decentralized artificial intelligence systems are vulnerable to illegal access and call for thorough frameworks like Nesa to guarantee data and model integrity by means of zero-knowledge proofs and trusted execution environments (Zhang et al., 2024). Though they also bring issues with bias and system integration, AI-driven threat detection systems improve data security in healthcare by allowing proactive threat identification and response (Arefin, 2024). Combining RPA and Generative AI in corporate operations exposes the dangers of illegal data access and model manipulation, so stressing the need for strong encryption and ongoing surveillance (Balaguru, 2024). Particularly in industrial environments, on-device learning systems are prone to data poisoning attacks that can compromise anomaly detection accuracy by means of sensor data

manipulation (Ino et al., 2024). Low-memory IoT systems run particular cyber risks that are needed for customized risk assessment models to manage (Radanliev et al., 2024) properly. Safeguarding AI systems against privacy violations and adversarial attacks requires cryptographic methods including homomorphic encryption and digital signatures, so guaranteeing the confidentiality and integrity of AI-generated content (Garcia et al., 2024). These research highlight the urgent need of thorough security plans including ethical and technical aspects to safeguard AI systems in many different uses.

Using AI systems in the classroom raises serious data security issues that need careful thought. As Konstantinidis and Apostolakis, 2024 emphasize, using AI technologies in healthcare—which also involves sensitive personal data—has resulted in privacy and security concerns. Using artificial intelligence in the classroom could lead one to wonder about safeguarding personal data and the possible weaknesses in AI systems managing such data. Moreover, (Dey, 2023) emphasizes the need to tackle privacy and security concerns in AI applications and the need for responsible use of AI in physical education and sports to safeguard athletes' data. These revelations make it clear that including artificial intelligence in the classroom calls for strong data security policies to protect student privacy and stop illegal access to private data. This calls for an all-encompassing evaluation of data security concerns in artificial intelligence systems to guarantee these technologies' ethical and safe application in learning environments.

4. Bias and Discrimination in AI Algorithms

As these technologies become fundamental for decision-making in many different fields, bias and discrimination in artificial intelligence algorithms raise serious questions. Algorithmic bias comes from many different sources: biassed input data, the development process, and algorithm execution that might have negative effects on some demographic groups (Moussawi & Joshi, 2024; Pulivarthy & Whig, 2024). The widespread application of artificial intelligence in sectors including public policy, employment, and healthcare has exposed ethical and legal hazards, including privacy concerns and mistakes in health protocols that could negatively impact patient health (Albarashdi, 2024). In artificial intelligence systems, bias usually results from unintentionally being introduced during algorithm development or prejudices ingrained in training data, producing systematic discrimination against particular groups (Chadha, 2024). Ethical governance, openness, responsibility in AI development, and the application of fairness-aware algorithms and bias detection techniques (Pulivarthy & Whig, 2024), are desperately needed to solve these problems. Moreover, different teams and worldwide policy coordination are crucial to guarantee that artificial intelligence systems follow moral standards and respect justice and responsibility. Encouragement of inclusive and fair AI systems helps to protect basic human rights and dignity while reducing the possibility of AI-induced discrimination.

Transparency and responsibility are, therefore, absolutely vital in AI decision-making to guarantee that these systems run fairly and ethically. Transparency in artificial intelligence algorithms helps people understand and follow the decision-making process, enabling them to

know how and why a given choice was made. Minimizing prejudices and developing trust in artificial intelligence systems depend on this transparency. Conversely, accountability in artificial intelligence refers to making creators of AI systems answerable for the results of their choices. Clear systems of responsibility help to prevent AI systems from either extending or even aggravating already existing inequality. Establishing explicit rules and guidelines that control these systems' growth and implementation will help attain transparency and responsibility in artificial intelligence decision-making. By doing this, we can help maximize the advantages of artificial intelligence technologies in many spheres, including education (Dropzdz, 2020) and help reduce possible hazards.

5. Legal and Regulatory Framework

Regarding AI in the context of education, the protection of personal data depends critically on the legal and regulatory environment. Educational institutions have to follow strict rules and regulations, including the General Data Protection Regulation in the European Union or the Family Educational Rights and Privacy Act in the United States, in order to safeguard students' "sensitive information." These rules control the gathering, keeping, and usage of personal information—including data produced by artificial intelligence systems. But the junction of artificial intelligence and personal data presents special difficulties that present themselves for which present laws might not be entirely appropriate. Problems including algorithmic bias, data privacy, and openness call for careful thought to balance innovation with respect to personal rights. Policymakers and teachers have to cooperate as artificial intelligence technologies develop to negotiate this complex terrain and create a regulatory environment encouraging data protection and innovation.

Compliance with strict data protection laws such as the General Data Protection Regulation and the California Consumer Privacy Protection Act is vital in negotiating AI's complicated terrain in education and personal data handling. The developments in artificial intelligence technologies have made it possible to gather and examine vast volumes of personal data, posing questions regarding autonomy and privacy (Ahluwalia, 2021). These laws are essential frameworks to protect people's data privacy and guarantee openness in using personal information in educational environments. Adherence to data protection rules becomes more important to reduce data breach risks and preserve ethical standards as artificial intelligence technologies keep developing and invading many spheres of education, including personalized learning and student assessment (Pavlenko, 2021). Understanding and applying these data protection rules should be a top priority for educators and institutions if they are to respect students' privacy rights and keep faith in educational programs, including artificial intelligence technologies.

Data handling in educational institutions falls mostly on regulatory compliance, ethical issues, and intellectual property protection. Scientific integrity and defense against allegations of misconduct depend on responsible data management practices, which institutions are charged with teaching researchers (Joshi & Krag, 2010). Data justice is a critical social issue since the development of digital platforms and datafication in education has brought complicated

difficulties, including privacy concerns and the possibility of data influencing educational and professional paths (Pangrazio et al., 2024). Institutions have to negotiate these difficulties by building strong infrastructure and legal systems guaranteeing informed involvement of stakeholders (Pangrazio et al., 2024). Moreover, the digitization of education—especially through MOOCs—has underlined the need for builders to address ethical and social aspects of data use by increasing scrutiny of data infrastructure (Johanes & Thille, 2019). In postgraduate programs, the balance between data utility and privacy is crucial, and privacy-preserving strategies and ethical frameworks must be used to attain sustainable data use that matches educational goals (Ncube & Ngulube, 2024). Furthermore, good data management techniques are crucial for obtaining and safeguarding intellectual property, so highlighting the need for academic institutions to control data properly (Geller, 2010). These obligations call for a thorough strategy combining best practices, new technologies, and ongoing monitoring to protect data integrity and privacy while using educational data analytics for both institutional and society advantages.

Examining these institutions' responsibility in managing student data is crucial in view of the growing integration of AI technologies in educational institutions. Given that AI-based learning tools gather and examine vast volumes of personal data, their increasing reliance begs questions about data privacy and security. Implementing strong data governance rules and security policies helps educational institutions give student data top priority. They should also guarantee openness about the gathering and application of data, so securing informed permission from parents and students. Moreover, institutions have to give employees enough instruction to guarantee correct data handling methods. By acting early, educational institutions can satisfy their responsibility to protect student data privacy and maximize the advantages of artificial intelligence technologies to improve the learning process (Miao et al., 2021).

6. Ethical Guidelines for Use of AI in Education

The ethical rules for artificial intelligence application in the classroom cover several spheres including responsibility, openness, cultural sensitivity, and academic honesty. Emphasizing the need of student assignments reflecting individual knowledge and keeping human oversight to ensure moral and legal responsibility for AI-related actions, universities worldwide are starting to react to the ethical challenges posed by generative AI (Dabis & Csáki, 2024). With rules that support ethical, honest, and fair use of AI in education and learning, a balanced approach is advocated allowing flexibility at both institutional and personal levels (Cacho, 2024). Including artificial intelligence in education also calls for a localized ethical framework emphasizing pedagogy, student agency, and access that considers the negotiating between teachers and students (Vetter et al., 2024). Information sessions that show both the advantages and disadvantages of artificial intelligence, so trying to equip students with the knowledge to make informed decisions, show that students still lack clarity about AI use despite the development of rules (Ross & Baines, 2024). Furthermore, cultural values greatly affect opinions of the ethical use of artificial intelligence; differences in these

clusters highlight the need of culturally sensitive methods in the integration of AI (Mumtaz et al., 2024). These revelations imply that even if general rules are important, they have to change to fit local situations and cultural quirks in order to properly handle AI's ethical consequences in education.

Including AI in the classroom brings a difficult ethical dimension needing careful thought. Developing and implementing AI-based conversational solutions in educational environments must fit an ethical, legal, socioeconomic, and cultural framework to protect users' dignity, freedom, and autonomy, as underlined by Piñeiro-Martínet al., 2022. Furthermore discussed in (Christoforaki and Beyan, 2022) including artificial intelligence in educational practices raises many ethical questions from data privacy to prejudice in decision-making. These ethical rules have to cover problems with algorithmic transparency, data collecting, and the possible social effects of artificial intelligence systems in learning environments. While negotiating the complexity of technology integration within the educational environment, the ethical use of artificial intelligence in education calls for a comprehensive approach that stresses student well-being, justice, and transparency.

When using artificial intelligence systems in educational environments, one must seriously consider international norms for data privacy. Governments and businesses all around understand the need to safeguard personal data, particularly in private settings like colleges and universities. Ensuring student data is handled securely and according to accepted rules depends on following laws including the General Data Protection Regulation in Europe and the Family Educational Rights and Privacy Act in the United States. Following these guidelines not only protects the privacy of teachers and students but also helps to build confidence in educational institutions applying artificial intelligence technologies. Strong data privacy policies help to preserve ethical standards and reduce possible risks related to gathering and handling personal data by means of educational environments (Hallinan et al., 2021).

7. Educational Impact

Recent developments in AI have spurred a tsunami of invention in educational technology, presenting fresh opportunities for tailored learning environments. However, growing reliance on artificial intelligence in education begs ethical concerns about using personal data. To safeguard student data, educational institutions must negotiate the difficult terrain of data privacy and security. Although artificial intelligence could improve learning results and offer customized support for students, questions regarding how personal data is gathered, kept, and applied in the context of education exist. To maximize the advantages of artificial intelligence in education and so protect student privacy and rights, educators, legislators, and technology developers must work together and create explicit rules for responsible use of AI in education. Shaping a sustainable and ethical future for education depends on balancing using AI for educational impact with safeguarding personal data (Miao et al., 2021).

Furthermore, applying tailored learning in learning environments has shown encouraging

success in raising student performance. Personalized learning systems can meet students' demands and learning styles by means of adaptive technologies and artificial intelligence. Personalized learning has been found in studies to raise student involvement, drive, and academic performance. For tests, for example, students who got individualized instruction did noticeably better than those who got conventional classroom instruction. Personalized learning also makes real-time assessments and comments possible, which helps teachers better monitor student development and, when needed, offer quick interventions. Combining tailored learning strategies will improve student performance and help to create a more inclusive and efficient classroom.

Successfully including AI in education depends on practical teacher training and continuous support. This training should cover the technical aspects of artificial intelligence, its ethical consequences, and its possible influence on student learning since teachers have the knowledge and skills to use AI tools in their classrooms properly. Teachers should also have access to professional development chances and ongoing support to keep current on the most recent developments in artificial intelligence technology and how best to include them in their daily work. Studies have indicated that teachers who get thorough training and support are more likely to effectively include artificial intelligence tools in their classrooms and observe favorable student engagement and results of performance. Thus, establishing a more effective and efficient learning environment depends critically on investments in teacher training and support for artificial intelligence integration (Miao et al., 2021).

Emerging technologies including mobile learning and artificial intelligence have been noted as transforming tools in the education industry (Meroto et al., 2024). These technologies present chances for more individualized and flexible learning environments by improving student involvement and motivation. Adoption of them, meanwhile, also brings difficulties including opposition to change and the necessity of ongoing teacher development. Including artificial intelligence TRiSM into education will greatly affect student involvement and drive in order to solve these problems. By means of AI tools, learning outcomes are better than those of conventional approaches and the burden of business executives and teachers is lessened, so optimizing educational processes (El Khatib et al., 2024). Though privacy and cost are issues, the integration of artificial intelligence into education has great potential to improve student involvement and motivation by means of customized learning environments and task automation.

As several studies have shown, using artificial intelligence technologies in different educational environments presents several difficulties. Strong ethical frameworks to control AI use, so guaranteeing data confidentiality and addressing possible biases in AI models presents one major difficulty (Ali et al., 2024; Lin et al., 2024). Training AI systems on varied datasets to prevent bias and guarantee inclusivity also presents technical and operational difficulties (Ali et al., 2024; Salas-Pilco et al., 2022). Including artificial intelligence in the classroom also presents pedagogical difficulties for teachers who must modify their approaches to properly include AI tools, which could call for further education and resources (Salas-Pilco et al., 2022). Another difficulty is socioeconomic differences since unequal access to technology might aggravate existing disparities in educational possibilities

(Nykonkos, 2023). Moreover, there is a cultural aspect to consider since AI tools have to be sensitive to the several sociocultural settings of students, especially minority groups, to support inclusivity and involvement (Salas-Pilco et al., 2022). Although artificial intelligence has great potential to improve tailored learning experiences, careful coordination is needed to guarantee that human interaction stays central to educational methods (Toyokawa et al., 2023). Recommended are strategic solutions, including establishing thorough national AI strategies, encouraging AI literacy among teachers and students, and creating clear guidelines for AI use (Ali et al., 2024; Nykonkos, 2023). These steps seek to maximize the advantages of artificial intelligence in building more inclusive and efficient learning environments while so reducing the hazards related to its application.

Even if including artificial intelligence technologies in various educational environments has possible advantages, many obstacles have to be overcome. The lack of resources and infrastructure for putting artificial intelligence systems into use presents a significant obstacle, especially in underprivileged colleges or districts. Furthermore raising ethical questions about AI use in education are data privacy and security concerns. Since artificial intelligence systems depend on large volumes of data to operate, there is a chance of exposing teachers' and students' personal information to possible leaks or abuse. Moreover, the one-size-fits-all approach might not be appropriate for different student populations, thus there is a gap between the capacities of AI systems and the needs of particular learners. Dealing with these difficulties will need careful thought of the ethical, practical, and pedagogical ramifications of including artificial intelligence technologies into learning environments. Navigating these complexity and guaranteeing AI's responsible and efficient use in education will need cooperative efforts among legislators, teachers, and technologists (Miao et al., 2021).

8. Discussion

Particularly in controlling information overload, the constant development of software agents in the Information Age calls for urgent ethical rules to control their use. As shown by (Bignell, 2005), the autonomous character of software agents requires a universally accepted code of ethical behavior to protect personal privacy and stop abuse. Furthermore, since they depend on pattern recognition algorithms, the present uses of software agents in the same paper differ greatly from the intended "intelligent agents". Concurrently with this parallel discussion, the empirical research clarifies the transforming power of computer-aided design tools, such CAD programs, in simplifying the design process and improving decision-making efficiency. These revelations highlight the crucial point at which personal data and artificial intelligence cross and underline the need of ethical issues and technology development to negotiate educational environments properly.

Future studies must investigate how artificial intelligence affects personal data security and privacy in educational environments going forward. This can entail looking at how well present data security policies protect student data from possible AI system abuse or breach. Further research should also concentrate on creating moral rules and policies fit for the fast development in artificial intelligence to guarantee the respect and preservation of students'

data rights. A multidisciplinary approach including education, law, computer science, and ethics viewpoints would help research in this field to solve the intricate interaction between artificial intelligence and personal data in educational environments. Scholars can help to provide a more complete knowledge of the ethical and legal difficulties raised by including artificial intelligence in education by filling in these research voids.

Artificial intelligence and personal data in education abound in ethical questions and legal ramifications. The conflict between using AI technologies to improve learning results and protecting student rights and privacy is central here. Careful navigation of ethical issues related to data protection, consent, justice, and transparency will help guarantee that artificial intelligence developments do not compromise basic ethical values. Furthermore, with laws like the General Data Protection Regulation defining data processing and privacy protection criteria, legal frameworks significantly influence the limits within which artificial intelligence systems might operate in educational environments. Though artificial intelligence presents possible advantages for education, stakeholders have to be alert in handling ethical and legal aspects to guarantee that AI use complies with legal criteria and ethical standards.

9. Conclusion

Examining the junction of artificial intelligence and personal data in education requires one to consider the educational opportunities and difficulties that develop. On the one hand, including artificial intelligence technologies into the classroom might customize learning environments, raise student involvement, and give teachers and students real-time comments. By helping to pinpoint areas where students might need more help or resources, artificial intelligence can also help to produce more efficient and successful learning results. However, using personal data in AI-powered learning environments begs serious questions about data security, privacy, and algorithmic bias. Policymakers and educators have to negotiate these difficult problems to guarantee that the advantages of artificial intelligence in education are fully realized while defending student rights and welfare. More studies are required to define precise policies and best practices for the responsible application of artificial intelligence technologies in learning environments.

Finally, the development of artificial intelligence in education offers a two-edged blade concerning data privacy. AI systems generate major questions about gathering, storing, and using private student data even though they present hitherto unheard-of possibilities for tailored learning and better educational results. Policymakers, teachers, and technologists have to strike a careful balance between defending personal privacy rights and applying artificial intelligence to maximize its possibilities. In educational settings, this means implementing robust data security systems, guaranteeing openness in data practices, and supporting ethical data use. Maximizing artificial intelligence's opportunities to assist students should ultimately be the goal of preserving respect for privacy and autonomy. Using deliberate and aggressive solutions for these issues, we can create a future whereby artificial intelligence and data privacy coexist peacefully in the field of education.

References

Adhyapak. Nair, S., & Mogare, S. (2024). Data Privacy and Security Risks in AI-Based Code Understanding. International Journal for Science Technology and Engineering, 12(6), 1913-1921. https://doi.org/10.22214/ijraset.2024.63423

Ahluwalia, M. (2021). Legal governance of brain data derived from artificial intelligence. Voices in Bioethics, 7, 1-5. https://doi.org/10.52214/vib.v7i.8403

Albarashdi, S. H. (2024). Discrimination Associated with Artificial Intelligence Technologies. Evolutionary Studies in Imaginative Culture (ESIC), 637-645. https://doi.org/10.70082/esiculture.vi.2099

Ali, O., Murray, P. A., Momin, M., Dwivedi, Y. K., & Malik, T. (2024). The effects of artificial intelligence applications in educational settings: Challenges and strategies. Technological Forecasting and Social Change, 199, 123076. https://doi.org/10.1016/j.techfore.2023.123076

Alier, M., Casañ Guerrero, M. J., Amo, D., Severance, C., & Fonseca, D. (2020). Privacy and E-Learning: A Pending Task. Sustainability, 13(16), 9206. https://doi.org/10.3390/su13169206

Alwabel, A.A. (2020). Privacy Issues in Big Data from Collection to Use. In: Tian, Y., Ma, T., Khan, M. (eds) Big Data and Security. ICBDS 2019. Communications in Computer and Information Science, vol 1210. Springer, Singapore. https://doi.org/10.1007/978-981-15-7530-3_29

Arefin, S. (2024). Strengthening Healthcare Data Security with Ai-Powered Threat Detection. International Journal of Scientific Research and Management (IJSRM), 12(10), 1477-1483. https://doi.org/10.18535/ijsrm/v12i10.ec02

Balaguru, S. (2024). Securing Automated Intelligence: Challenges and Solutions in RPA and Generative AI Integration - Saranya Balaguru – IJFMR, 6(5), https://doi.org/10.36948/ijfmr.2024.v06i05.27900

Bignell, K. B. (2005). Software agents: Ethical issues concerning agent autonomy. In Information Resources Management Association International Conference (IRMA), (549-552). IDEA Publishing.

Cacho, R. M. (2024). Integrating Generative AI in University Teaching and Learning: A Model for Balanced Guidelines. Online Learning, 28(3), 55-81. https://doi.org/10.24059/olj.v28i3.4508

Chadha, K. S. (2024). Bias and Fairness in Artificial Intelligence: Methods and Mitigation Strategies. International Journal for Research Publication and Seminar, 15(3), 36-49. https://doi.org/10.36676/jrps.v15.i3.1425

Chen, L., Chen, P., & Lin, Z. (2020). Artificial intelligence in education: A review. Ieee Access, 8, 75264-75278. https://doi.org/10.1109/ACCESS.2020.2988510

Chen, X. (2024). A preliminary discussion on data privacy and data security issues. Applied and Computational Engineering, 71, 219-224. https://doi.org/10.54254/2755-2721/71/20241710

Choudhry, M. D., Sundarrajan, M., Jeevanandham, S., & Saravanan, V. (2024). Security and Privacy Issues in AI-based Biometric Systems. In AI-Based Advancements in Biometrics and its Applications (pp. 85-100). CRC Press.

Christoforaki, M., & Beyan, O. (2021). AI Ethics—A Bird's Eye View. Applied Sciences, 12(9), 4130. https://doi.org/10.3390/app12094130

Dabis, A., & Csáki, C. (2024). AI and ethics: Investigating the first policy responses of higher education institutions to the challenge of generative AI. Humanities and Social Sciences Communications, 11(1), 1-13. https://doi.org/10.1057/s41599-024-03526-z

Dey, V. (2023). The Role of Artificial Intelligence in Physical Education and Sports: A Review of Current Applications and Future Potential, Journal Global Values, Vol. XIV, Special Issue, No. 2023, 9-14. https://doi.org/10.31995/jgv.2023.v14iS3.003

Donnell, F. O., Porter, M., & Fitzgerald, S. The Role of Artificial Intelligence in Higher Education: Higher Education Students use of AI in Academic Assignments. Irish Journal of Technology Enhanced Learning, 8(1). https://doi.org/10.22554/szwjfy54

Drozdz, A. (2020). Protection of Natural Persons with Regard to Automated Individual Decision-Making in the GDPR. Kluwer Law International B.V. http://digital.casalini.it/9789403520537

El Khatib, M., Al Sharif, M., & Mohamad, H. (2023). Impact of AI TRiSM on Knowledge and Decision Making for Business Executives in the Education Industry. International Journal of Theory of Organization and Practice (IJTOP), 3(2), 1-15. https://doi.org/10.54489/ijtop.v3i2.290

Farahani, M. S., & Ghasmi, G. (2024). Artificial Intelligence in education: A comprehensive study. Forum for Education Studies, 2(3), 1379. https://doi.org/10.59400/fes.v2i3.1379

Feng, T., & Li, Q. (2024). Artificial Intelligence in Education Management: Opportunities, Challenges, and Solutions. Frontiers in Business, Economics and Management, 16(3), 49-54. https://doi.org/10.54097/raxsbp45

Garcia, J. L. C., Udechukwu, I. P., Ibrahim, I. B., Chukwu, I. J., Dağ, H., Dimitrova, V., & Mollakuqe, E. (2024). Securing AI Systems: A Comprehensive Overview of Cryptographic Techniques for Enhanced Confidentiality and Integrity. In 2024 13th Mediterranean Conference on Embedded Computing (MECO) (pp. 1-8). IEEE. https://doi.org/10.1109/MECO62516.2024.10577883

Geller, L. (2010). Data Management in Academic Settings: An Intellectual Property Perspective. Science and Engineering Ethics, 16, 769-775. https://doi.org/10.1007/s11948-010-9240-4

Gupta, M., & Shah, U. N. (2023). Navigating the Data Security Landscape: Challenges and Solutions in Financial Markets amid Digitalization and Artificial Intelligence. International Journal of Multidisciplinary Research and Analysis, 10. https://doi.org/10.47191/ijmra/v6-i12-77

Hallinan, D., Leenes, R., & De Hert, P. (Eds.). (2021). Data Protection and Privacy, Volume 13: Data Protection and Artificial Intelligence (Vol. 13). Bloomsbury Publishing.

Hoel, T., & Chen, W. (2018). Privacy and data protection in learning analytics should be motivated by an educational maxim—Towards a proposal. Research and Practice in Technology Enhanced Learning, 13(1), 1-14. https://doi.org/10.1186/s41039-018-0086-8

Holmes, W., & Porayska-Pomsta, K. (2023). The ethics of artificial intelligence in education. Routledge Taylor.

Howard, S. K., Swist, T., Gasevic, D., Bartimote, K., Knight, S., Gulson, K., Apps, T., Peloche, J., Hutchinson, N., & Selwyn, N. (2021). Educational data journeys: Where are we going, what are we taking and making for AI? Computers and Education: Artificial Intelligence, 3, 100073. https://doi.org/10.1016/j.caeai.2022.100073

Ino, T., Yoshida, K., Matsutani, H., & Fujino, T. (2023). Data Poisoning Attack against Neural Network-Based On-Device Learning Anomaly Detector by Physical Attacks on Sensors. Sensors, 24(19), 6416. https://doi.org/10.3390/s24196416

Ismail, I. A. & Aloshi, J. M. (2025). Data Privacy in AI-Driven Education: An In-Depth Exploration into the Data Privacy Concerns and Potential Solutions. In K. Keeley (Ed.), AI Applications and Strategies in Teacher Education (pp. 223-252). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-5443-8.ch008

Johanes, P. and Thille, C. (2019). The heart of educational data infrastructures = Conscious humanity and scientific responsibility, not infinite data and limitless experimentation. British Journal of Educational Technology (BJET), 50, 2959-2973. https://doi.org/10.1111/bjet.12862

Jones, K. M. (2019). Learning analytics and higher education: A proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. International Journal of Educational Technology in Higher Education, 16(1), 1-22. https://doi.org/10.1186/s41239-019-0155-0

Jose, D. (2024). Data Privacy and Security Concerns in AI-Integrated Educational Platforms, Recent Trends in Management and Commerce 5(2), 87-91. https://doi.org/10.46632/rmc/5/2/19

Joshi, M., Krag, S.S. (2010). Issues in Data Management. Science and Engineering Ethics 16, 743–748. https://doi.org/10.1007/s11948-010-9223-5

Kaddouri, M., Mhamdi, K., Chniete, I., Marhraoui, M., Khaldi, M., & Jmad, S. (2025). Adopting AI in Education: Technical Challenges and Ethical Constraints. In M. Sanmugam, B. Edwards, N. Mohd Barkhaya, & Z. Khlaif (Eds.), Fostering Inclusive Education with AI and Emerging Technologies (pp. 25-72). IGI Global Scientific Publishing.

https://doi.org/10.4018/979-8-3693-7255-5.ch002

Kaswan, K. S., Dhatterwal, J. S., & Ojha, R. P. (2024). AI in personalized learning. In Advances in Technological Innovations in Higher Education (103-117). CRC Press.

Kay, J., & Kummerfeld, B. (2019). From data to personal user models for life-long, life-wide learners. British Journal of Educational Technology, 50(6), 2871-2884. https://doi.org/10.1111/bjet.12878

Konstantinidis, K., & Apostolakis, I. (2025). The Added Value of Real-World Data in the Digital Health Ecosystem: Challenges in the Greek Context. In Convergence of Population Health Management, Pharmacogenomics, and Patient-Centered Care (pp. 91-118). IGI Global.

Kujundziski, A. P. & Bojadjiev, J. (2025). Artificial Intelligence in Education: Transforming Learning Landscapes. In M. Stevkovska, M. Klemenchich, & N. Kavaklı Ulutaş (Eds.), Reimagining Intelligent Computer-Assisted Language Education (pp. 1-54). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-4310-4.ch001

Kumi-Yeboah, A., Kim, Y., Yankson, B., Aikins, S., & Dadson, Y. A. (2023). Diverse students' perspectives on privacy and technology integration in higher education. British Journal of Educational Technology, 54(6), 1671-1692. https://doi.org/10.1111/bjet.13386

Li, L. (2006). Digital Storytelling: Self-Efficacy and Digital Literacy. In T. Reeves & S. Yamashita (Eds.), Proceedings of E-Learn 2006--World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education (pp. 2159-2164). Honolulu, Hawaii, USA: Association for the Advancement of Computing in Education (AACE). Retrieved from https://www.learntechlib.org/primary/p/24031/.

Lin, M. P., Liu, A. L., Poitras, E., Chang, M., & Chang, D. H. (2023). An Exploratory Study on the Efficacy and Inclusivity of AI Technologies in Diverse Learning Environments. Sustainability, 16(20), 8992. https://doi.org/10.3390/su16208992

Mappisabbi, A. F., & Amirullah, N., Batti, S. (2024). Leveraging Data and Artificial Intelligence for Innovative Educational Management Practices. International Journal of Management Research and Economics, 2(2), 182-192. https://doi.org/10.54066/ijmre-itb.v2i2.1788

Maraj, D., Vuković, M., & Hotovec, P. (2024). A Survey on User Profiling, Data Collection, and Privacy Issues of Internet Services. Telecom, 5(4), 961-976. https://doi.org/10.3390/telecom5040048

Meroto, M. B. das N., Moreira, A. C. e S., Braz Sobrinho, B., Ferraz, D. de O., Scarpati, E. das V., do Carmo, J. P. G., Mendes, K. A. P., & de Oliveira, R. O. M. (2024). Integrating emerging technologies into classrooms: a multimedia perspective. CONTRIBUCIONES A LAS CIENCIAS SOCIALES, 17(2), e5180. https://doi.org/10.55905/revconv.17n.2-145

Miao, F., Holmes, W., Huang, R., & Zhang, H. (2021). AI and education: A guidance for policymakers. Unesco Publishing.

Micheni, E., Machii, J., & Murumba, J. (2024). The role of artificial intelligence in education. Open Journal for Information Technology, 7(1), 1. https://doi.org/10.32591/coas.ojit.0701.04043m

Mironova, M.I. (2022). Data Gathering and the Problem of Data Privacy. In: Inozemtsev, M.I., Sidorenko, E.L., Khisamova, Z.I. (eds) In the Platform Economy. Palgrave Designing a Supranational Legal Framework, Singapore: Springer Nature Singapore, (pp. 365-378). https://doi.org/10.1007/978-981-19-3242-7_25

Mondal, S., Gharote, M. S., & Lodha, S. P. (2022). Privacy of Personal Information: Going incog in a goldfish bowl. Queue, 20(3), 41-87. https://doi.org/10.1145/3546934

Moussawi, S., Deng, X., & Joshi, K. D. (2024). AI and Discrimination: Sources of Algorithmic Biases. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 55(4), 6-11. https://doi.org/10.1145/3701613.3701615

Mumtaz, S., Carmichael, J., Weiss, M., & Nimon-Peters, A. (2024). Ethical use of artificial intelligence based tools in higher education: are future business leaders ready?. Education and Information Technologies, 1-27. https://doi.org/10.1007/s10639-024-13099-8

Ncube, M. M., & Ngulube, P. (2023). A Systematic Review of Postgraduate Programmes Concerning Ethical Imperatives of Data Privacy in Sustainable Educational Data Analytics. Sustainability, 16(15), 6377. https://doi.org/10.3390/su16156377

Nykonenko, A. (2023). THE IMPACT OF ARTIFICIAL INTELLIGENCE ON MODERN EDUCATION: PROSPECTS AND CHALLENGES, Artificial Intelligence, 2, 10-15. https://doi.org/10.15407/jai2023.02.010

Pangrazio, L., Auld, G., Lynch, J., Sawatzki, C., Duffy, G., Hannigan, S., & O'Mara, J. (2024). Data justice in education: Toward a research agenda. Educational Philosophy and Theory, 1-12. https://doi.org/10.1080/00131857.2024.2320196

Pavlenko, Z. (2021). LAW IN DIGITAL REALITY. The Bulletin of Yaroslav Mudryi National Law University Series Philosophy Philosophies of Law Political Science Sociology, 2(49). https://doi.org/10.21564/2663-5704.49.229779

Piñeiro-Martín, A., García Mateo, C., Docío Fernández, L., & López Pérez, M. D. C. (2022). Ethics guidelines for the development of virtual assistants for e-health. In Proc. Iber SPEECH 2022, 121-125. https://doi.org/10.21437/IberSPEECH.2022-25

Prinsloo, P., & Slade, S. (2015). Student privacy self-management: Implications for learning analytics. In Proceedings of the 5th International Conference on Learning Analytics and Knowledge (pp. 83-92). https://doi.org/10.1145/2723576.2723585

Prinsloo, P., Slade, S., & Khalil, M. (2022). The answer is (not only) technological: Considering student data privacy in learning analytics. British Journal of Educational Technology, 53(4), 876-893. https://doi.org/10.1111/bjet.13216

Pulivarthy, P. & Whig, P. (2025). Bias and Fairness Addressing Discrimination in AI Systems.

In P. Bhattacharya, A. Hassan, H. Liu, & B. Bhushan (Eds.), Ethical Dimensions of AI Development (pp. 103-126). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-4147-6.ch005

Radanliev, P., De Roure, D., Maple, C., Nurse, J. R., Nicolescu, R., & Ani, U. (2024). AI security and cyber risk in IoT systems. Frontiers in Big Data, 7, 1402745. https://doi.org/10.3389/fdata.2024.1402745

Ren, D. Q., & Liu, H. (2022). Privacy Computing Issues in Collecting and Using Customer Data of Mobile Devices. In 2022 7th International Conference on Signal and Image Processing (ICSIP) (pp. 382-389). IEEE. https://doi.org/10.1109/ICSIP55141.2022.9886951

Rohunen, A. & Markkula, J. (2018). Development of Personal Information Privacy Concerns Evaluation. In M. Khosrow-Pour, D.B.A. (Ed.), Encyclopedia of Information Science and Technology, Fourth Edition (pp. 4862-4871). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-5225-2255-3.ch421

Ross, E. A. S., & Baines, J. (2024). Treading water: new data on the impact of AI ethics information sessions in classics and ancient language pedagogy. Journal of Classics Teaching, 25(50), 181–190. https://doi.org/10.1017/S2058631024000412

Santos, O., & Radanliev, P. (2024). Beyond the Algorithm: AI, Security, Privacy, and Ethics. Addison-Wesley Professional.

Sei, Y. (2024). Privacy-Preserving Data Collection and Analysis for Smart Cities. In: Murakami, Y., Kimura, K. (eds) Human-Centered Services Computing for Smart Cities, 157–212. Springer, Singapore. https://doi.org/10.1007/978-981-97-0779-9_5

Singh, G. & Thakur, A. (2024). AI in Education: Ethical Challenges and Opportunities. In R. Kumar, A. Joshi, H. Sharan, S. Peng, & C. Dudhagara (Eds.), The Ethical Frontier of AI and Data Analysis (18–38). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-2964-1.ch002

Singh, T. M., Reddy, C. K. K., Murthy, B. R., Nag, A., & Doss, S. (2025). Ai and education: Bridging the gap to personalized, efficient, and accessible learning. In M. Ouaissa, M. Ouaissa, H. Lamaazi, M. El Hamlaoui, & K. Reddy C. (Eds.), Internet of Behavior-Based Computational Intelligence for Smart Education Systems (pp. 131-160). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-8151-9.ch005

Slade, S., Prinsloo, P., & Khalil, M. (2019). Learning analytics at the intersections of student trust, disclosure and benefit. In Proceedings of the 9th International Conference on Learning Analytics & Knowledge (235-244).

Toyokawa, Y., Horikoshi, I., Majumdar, R., & Ogata, H. (2023). Challenges and opportunities of AI in inclusive education: A case study of data-enhanced active reading in Japan. Smart Learning Environments, 10(1), 1-19. https://doi.org/10.1186/s40561-023-00286-2

Vetter, M. A., Lucia, B., Jiang, J., & Othman, M. (2024). Towards a framework for local interrogation of AI ethics: A case study on text generators, academic integrity, and composing

with ChatGPT. Computers and Composition, 71, 102831. https://doi.org/10.1016/j.compcom.2024.102831

Xiong, Z., Li, H., Liu, Z., Chen, Z., Zhou, H., Rong, W., & Ouyang, Y. (2024). A Review of Data Mining in Personalized Education: Current Trends and Future Prospects, Frontiers of Digital Education, 1, 26–50 (2024). https://doi.org/10.1007/s44366-024-0019-6

Yılmaz, Ö. (2024). Personalised learning and artificial intelligence in science education: current state and future perspectives. Educational Technology Quarterly, 2024(3), 255-274. https://doi.org/10.55056/etq.744

Yu, D., Zhang, K., Tao, Y., Xu, W., Zou, Y., & Cheng, X. (2024). Correlation-Aware and Personalized Privacy-Preserving Data Collection. In 2024 International Conference on Computing, Networking and Communications (ICNC) (pp. 724-729). IEEE. https://doi.org/10.1109/ICNC59896.2024.10556247

Zaman, B. U. (2024). Leveraging Big Data and AI for Personalized Learning Opportunities, Challenges, and Ethical Considerations. Challenges and Ethical Considerations (July 16, 2024). http://dx.doi.org/10.2139/ssrn.4896086

Zhang, H., Zhao, Y., Yang, C., Farhan, A., & Johnston, F. Towards Secure and Private AI: A Framework for Decentralized Inference. In Workshop on Responsibly Building the Next Generation of Multimodal Foundational Models. https://doi.org/10.48550/arXiv.2407.19401

Zobeida, S., Xiao, K., & Oshima, J. (2021). Artificial Intelligence and New Technologies in Inclusive Education for Minority Students: A Systematic Review. Sustainability, 14(20), 13572. https://doi.org/10.3390/su142013572

Acknowledgments

Not Applicable.

Funding

Not Applicable.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Macrothink Institute.

The journal’s policies adhere to the Core Practices established by the Committee on

Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

Open access

Copyrights