https://doi.org/10.48047/AFJBS.6.Si2.2024.5360-5367

AFJBS African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

PERSONAL DATA SECURITY IN AI-POWERED EDUCATIONAL TOOLS: AN INTERNATIONAL OVERVIEW

Kadirova Laylo Imomaliyevna,

Yusupova Zamira Zaripovna

Salixova Muhayyo Shakirovna,

Azamova Saodat Fayzullayevna

Teachers, TUIT

Article history

Volume 6 issue si2 2024

Received:18Apr2024

Accepted:20Jun2024

doi:10.48047/AFJBS.6.Si2.2024.5360-5367

ABSTRACT

The rapid integration of AI in education offers transformative opportunities but raises crucial concerns about the security and privacy of student data. This paper examines the international landscape of personal data security in AI-powered educational tools, highlighting key challenges and emerging solutions. We analyze the current regulatory frameworks and policies in major regions like the EU, US, China, Canada, and India, highlighting both strengths and limitations. The paper then delves into emerging solutions including data minimization techniques, enhanced transparency and control, ethical guidelines, education and awareness campaigns, and international cooperation. By addressing the identified challenges through a multi-faceted approach, we can foster the ethical and responsible use of AI in education, ensuring student data privacy and fostering a more equitable learning environment.

Keywords: AI in education, personal data security, privacy, data protection, regulations, international overview, ethical guidelines, transparency, accountability, data minimization, emerging solutions, challenges, opportunities.

INTRODUCTION

The rapid adoption of Artificial Intelligence (AI) in education presents numerous benefits, but also raises concerns regarding the security and privacy of personal data. This paper provides an international overview of the current landscape of personal data security in AI-powered educational tools, highlighting key challenges and emerging solutions.

AI systems to respect, safeguard, and advance human rights, fundamental freedoms, and dignity at all stages of their development. 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 re-frail 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.

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 ad-here 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.

MATERIALS AND METHODS

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 pro-vide sufficient encouragement for students who are less academically resil-ient 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 ad-dress such concerns within legal and ethical paradigms to ensure the sustain-able advancement of educational AI. Studies have examined AI ethics from a variety of perspectives. Re-garding risks of AI, Zhao et al. (2021) asserted that current AI ethical con-cerns are primarily over issues such as undermined human decision-making autonomy, privacy protection, social equity, security responsibility attribu-tion, 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, the judicial fairness of intelligent justice, the “information cocoon” effect in information push ser-vices, and the dignity of elderly individuals under robot care. 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. 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 proposed that the government should establish agile governance-based frameworks for the development and supervision of AI and other emerging industries; Jia and Jiang mentioned that the AI era’s effective public policy making de-pends on improved algorithms and data governance frameworks, social governance mechanisms, and global governance systems.

Challenges:

- Data Collection & Usage: AI-powered educational tools often collect vast amounts of personal data, including student performance, learning styles, demographics, and online behavior. The transparency and purpose of data collection can be unclear, raising concerns about misuse and exploitation.
- Data Security & Privacy: Ensuring the security and privacy of this sensitive data is paramount. Weak security measures, data breaches, and unauthorized access can compromise student privacy and lead to identity theft or discrimination.
- Algorithmic Bias & Fairness: AI algorithms trained on biased datasets can perpetuate existing inequalities and disadvantage certain student groups. This requires careful monitoring and ethical considerations to ensure fairness and equity in education.
- Lack of International Standards & Regulations: The lack of clear, internationally harmonized regulations and standards for data security in AI-powered education creates a fragmented regulatory landscape, making it difficult for stakeholders to ensure compliance.
- Lack of Awareness & Education: Educators, parents, and students may not be sufficiently aware of the potential risks associated with AI-powered tools, hindering their ability to protect their data and make informed choices.

International Perspectives:

- European Union (EU): The General Data Protection Regulation (GDPR) provides a strong framework for data protection, requiring clear consent, transparency, and data minimization.
- United States (US): The US lacks a comprehensive federal privacy law, relying on a patchwork of state laws. California's Consumer Privacy Act (CCPA) and the Children's Online Privacy Protection Act (COPPA) provide some protection, but gaps remain.

- China: China's Personal Information Protection Law (PIPL) emphasizes data localization and restricts data transfer outside the country, impacting the use of AI tools developed in other regions.
- Canada: Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) offers a strong foundation for data protection, but its application to AI remains under development.
- India: The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, address data security, but updates are needed to address the challenges posed by AI.

Emerging Solutions:

- Data Minimization & Privacy-Preserving Technologies: Implementing techniques like differential privacy and federated learning to reduce data collection and enhance privacy.
- Enhanced Transparency & Control: Providing clear information about data collection, usage, and user rights. Allowing users to control their data and opt out of certain data collection practices.
- Ethical Guidelines & Standards: Developing internationally recognized ethical guidelines for the design, development, and deployment of AI in education.
- Education & Awareness Campaigns: Raising awareness among educators, parents, and students about the risks and benefits of AI-powered tools and empowering them to make informed decisions.
- International Cooperation: Fostering collaboration between governments, researchers, and technology companies to develop a harmonized global framework for data security in AI-powered education.

Option 1: Focusing on the Need for Action

The rise of AI-powered educational tools presents a double-edged sword. While offering potential to personalize learning and improve outcomes, it also poses significant risks to student data privacy. This paper analyzes the current state of data security in AI-powered education across various global regions, revealing a fragmented regulatory landscape and potential vulnerabilities. It calls for urgent action, including the development of international standards, robust data protection measures, and public education initiatives, to safeguard student data and ensure responsible AI implementation in education.

Option 2: Emphasizing the Ethical Dimension

The integration of AI in education raises significant ethical concerns around data privacy, algorithmic bias, and the potential for inequitable outcomes. This paper provides an international overview of the challenges and opportunities associated with personal data security in AI-powered educational tools. It examines current regulations, explores emerging solutions, and argues for a collaborative approach involving policymakers, educators, researchers, and technology developers to ensure the ethical and responsible use of AI in education.

Option 3: Focusing on the Benefits of AI while Emphasizing Responsibility

The potential of AI to personalize education and enhance student learning is undeniable. However, realizing this potential requires a commitment to data security and ethical considerations. This paper examines the global landscape of personal data protection in AI-powered educational tools, analyzing existing regulations, identifying gaps, and highlighting emerging solutions. It emphasizes the need for a proactive and collaborative approach to ensure that AI advancements in education are ethically sound, transparent, and prioritize student well-being.

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 pro-vide 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 ad-dress such concerns within legal and ethical paradigms to ensure the sustain-able advancement of educational AI. Studies have examined AI ethics from a variety of perspectives. Re-grading risks of AI, Zhao et al asserted that current AI ethical con-corns are primarily over issues such as undermined human decision-making autonomy, privacy protection, social equity, security responsibility attribution, and ecology, whereas Tan and Yang 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, the judicial fairness of intelligent justice, the "information cocoon" effect in information push ser-vices, and the dignity of elderly individuals under robot care. 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 Goo. 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 proposed that the government should establish agile governance-based frameworks for the development and supervision of AI and other emerging industries; Jia and Jiang mentioned that the AI era's effective public policy making de-pends on improved algorithms and data governance frameworks, social governance mechanisms, and global governance systems.

CONCLUSION:

Ensuring the responsible use of AI-powered tools in education requires a collaborative effort from all stakeholders. Addressing the challenges outlined above through a combination of regulator y frameworks, technological advancements, ethical guidelines, and public awareness will be crucial to maximizing the benefits of AI while protecting student data and privacy. A global approach that emphasizes transparency, accountability, and individual control will be essential for building trust and ensuring the ethical and responsible use of AI in education.

REFERENCES

1. Z. Zhang and Z. Zhang, A Review on Face Detection and Recognition Techniques. (Artificial Intelligence Review, 47(3), 2016), pp. 346-364.

1. Y. Taigman, M. Yang, M. Ranzato and L. Wolf, DeepFace: Closing the gap to human-level performance in face verification. (In Proceedings of the IEEE conference on computer vision and pattern recognition, 2014), pp. 1701-1708.

2. F. Schroff, D. Kalenichenko and J. Philbin, FaceNet: A unified embedding for face recognition and clustering. (In Proceedings of the IEEE conference on computer vision and pattern recognition, 2015), pp. 815-823.

3. O. M. Parkhi, A. Vedaldi, and A. Zisserman, Deep face recognition. (In Proceedings of the British Machine Vision Conference, 2015), pp. 41.1-41.12.

4. J. Deng, J. Guo and S. Zafeiriou, ArcFace: Additive angular margin loss for deep face recognition. (In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019), pp. 4690-4699.