The Impact of AI on Privacy and Security of Data in Universities in Zimbabwe: A Literature Review

Reason Gobvu[1], Never Katsamudanga[2] and Godfrey Tsvuura[1]

[1]Zimbabwe Open University
https://orcid.org/0009-0000-4596-4629
Corresponding Author's email: gobvur@zou.ac.zw
[2] Harare Polytechnic
https://orcid.org/0009-0004-8053-3196
[1]Zimbabwe Open University
https://orcid.org/0000-0002-0317-0916

Abstract

In this empirical paper we discussed the impact of AI on data privacy and security in universities in Zimbabwe. The integration of how artificial intelligence (AI) in universities has transformed various aspects of educational systems offering enhanced efficiencies and personalised learning experiences were discussed. This technological advancement raises significant concerns regarding data privacy and security. As universities increasingly rely on AI systems that process vast amounts of sensitive information, the risk of data breaches and unauthorised access escalates. With a focus on Zimbabwe, this research offers a systematic literature analysis of the effects of AI on data security and privacy in higher education. The study explores topics such as application of AI in universities, data privacy and security concerns, ethical and legal gaps in the application of AI and prospects for AI adoption in a responsible manner, drawing on both worldwide and regional studies. The paper is couched in Information Security Theory which evolved in the 1970s–1980s within the field of computer security as government, military and corporate institutions began formulating formal information assurance standards (Bishop, 2003). Information Security Theory model became widely recognised through the U.S Department of Defense publication and the early academic security literature. The findings suggest that AI increases efficiency and personalisation in universities, it also puts universities at risk for algorithmic bias, data breaches and poor information governance. In Zimbabwean universities, these risks are worse due to inadequate infrastructure, poor implementation of data privacy laws and regulations and insufficient knowledge. The study ends by suggesting that strong legislative policies, cybersecurity frameworks and effective digital literacy programmes should be implemented to ensure responsible AI use.

Keywords: Artificial Intelligence, privacy, data security, universities, Zimbabwe, cybersecurity

Introduction

Higher education institutions around the world according to Zawacki-Richter *et al*., (2019) are progressively implementing artificial intelligence (AI) to improve administration, research and learning. Application of AI in higher education includes chatbots for administrative assistance, facial recognition for campus security, plagiarism detection and student performance prediction (Luckin et al., 2016). These advances increase productivity by gathering and handling large amounts of data, which raises privacy and security issues. The way universities function around the world is changing because of the increasing use of artificial intelligence (AI) in higher education. Teaching, learning and research environments are incorporating AI applications including facial recognition, predictive analytics, intelligent tutoring systems and automated administrative tools, Zawacki-Richter et al., (2019). AI is being used more by Zimbabwean universities to improve operations, especially in digital libraries and online

learning management systems, Chikomba & Mutsagondo, (2022). However, these changes bring serious issues with data security and privacy. A huge volume of records of financial, academic and personal data is processed by AI systems; if not handled properly, these data might be compromised and misused. According to Benaich & Hogarth, (2021) Cyberattacks targeting private student and employee data have occurred in institutions around the world, igniting concerns about monitoring, profiling and illegal access. These issues are intensified in Zimbabwe by the lack of suitable policies, lack of cybersecurity competence and limited technology infrastructure. This study scrutinises the potential and risks associated with artificial intelligence as it relates to data security and privacy in Zimbabwean universities.

Materials and Methods

Global teaching, learning and administrative procedures have been revolutionised by the quick spread of artificial intelligence (AI) in higher education. AI technologies are being used increasingly globally for smart campus management, plagiarism detection, predictive analytics and adaptive learning platforms, Zawacki-Richter et al., (2019). These developments present issues with data privacy, security and ethical governance while also providing chances to improve efficiency and personalised learning. The General Data Protection Regulation (GDPR) of the European Union and UNESCO's AI ethics guidelines are two examples of the strict international data protection frameworks that universities around the world must adhere to while simultaneously embracing technological innovation (Floridi & Cowls, 2019).

AI-driven educational technologies, especially in the areas of online learning platforms, administrative data processing and research analytics have been gradually adopted at the national level in Zimbabwe. According to Mutsagondo (2019), the legal and policy framework for data security and privacy is still in its infancy when compared to international norms. Though its application in the higher education sector has been patchy, the Cybersecurity and Data Protection Act of 2021 provide a legal basis for data governance. Comprehensive data protection rules, secure infrastructures and skilled staff that can handle the dangers involved in implementing AI are lacking in many institutions (Chigada & Madzinga, 2021). Scholars have emphasised the necessity of all-encompassing policy frameworks to facilitate the responsible incorporation of AI in Zimbabwean academic institutions. A well-organised policy framework is necessary to guarantee that the adoption of AI is in line with both the Sustainable Development Goals (SDGs) and national education objectives. AI can also improve learning results and streamline administrative procedures at higher education institutions, according to studies. Addressing the dangers and difficulties of integrating AI, such as financial constraints and data privacy issues, is essential (Chatikobo & Pasipamire, 2024).

The literature on AI ethics, privacy and data protection is expanding internationally, but there are still significant gaps when it comes to the setting of higher education in Zimbabwe. The convergence of AI, data privacy and security in academic institutions has not received enough attention in the literature, which mostly focuses on infrastructure issues in digitisation (Mutsagondo, 2019; Chigada & Madzinga, 2021). Furthermore, there is a dearth of empirical data regarding how universities in poor nations are modifying international frameworks to fit local realities characterised by a lack of resources, lax enforcement and rapidly advancing technical capabilities.

Therefore, using a literature review lens, this study sets itself up to critically analyse how AI affects data security and privacy in Zimbabwean universities. Through the synthesis of knowledge on national policies, local practices and international norms, it helps close the scholarly divide. Secondly, protecting data privacy and security is essential in upholding

student rights, institutional trust and compliance with national laws and international best practices. The study is justified on two grounds: First, the growing use of AI tools in higher education calls for a context-sensitive understanding of the risks involved. By tackling this neglected field, the study provides pertinent information that can help stakeholders, legislators and academic institutions ensure the ethical and responsible integration of AI in Zimbabwean higher education.

Objectives of the study are to:

- examine the application of AI in universities
- assess the data privacy and security concerns
- analyse the ethical and legal gaps in the application of AI
- evaluate the prospects for AI adoption in a responsible manner

The study is based on the Information Security Theory, specifically the Parkerian Hexad, developed by Donn B. Parker in 2002. This paradigm was put forth as an expansion of the conventional CIA triad, which has long been the foundation of information security models and consists of confidentiality, integrity and availability (Parker, 2002). Despite offering a solid basis, Parker contended that the CIA trinity was insufficiently all-encompassing to handle the increasing complexity of information systems in the digital age. Parker (1998) developed the Parkerian Hexad, a six-element model that was later refined by Hintzbergen, et al. (2010), who added three more dimensions which are, possession or control, authenticity and utility.

According to McDermott and Fox (2004), the goal of this theory was to offer a more comprehensive approach to information security by guaranteeing that data is not only accurate, accessible and secret, but also legally controlled, verifiable and usable for its intended purposes. By broadening the spectrum of protection, the Parkerian Hexad acknowledged that illegal possession of data, information falsification and technical manipulations that made data unusable could all pose a threat to data security in addition to confidentiality violations or system outages (Hintzbergen et al 2010).

The Parkerian Hexad offers a strong lens used to examine the effects of artificial intelligence on data security and privacy in Zimbabwean universities, which is relevant to the current study. For example, the factor of confidentiality directly addresses safeguarding the private information of employees and students from unapproved access in AI-powered systems. Integrity guarantees that information utilised by AI systems to make decisions like admissions or grades is correct and unaltered. The requirement for dependable access to university systems is addressed by availability, which is essential in digital learning settings. The Parkerian Hexad thus directly supports the study's objectives, which are to investigate how AI technologies impact the security, privacy and governance of institutional and personal data in Zimbabwean universities. This is done by evaluating whether data is not only protected in a narrow sense, but also remains controlled, authentic and functionally useful thus key considerations in the responsible adoption of AI.

Devineni (2024) examined how AI affects data security and privacy. His research focused mostly on the moral uses of AI in the banking and healthcare industries. He concluded by emphasising the importance of AI as a vital tool in the never-ending fight against cyberattacks and urging more study and advancement. Based on medical records, Jose and Barbosa (2023) debated digital privacy and data security, guaranteeing patient privacy through effective cryptographic methods. Wengi and Ling's (2025) study, "AI on Trustworthy Distributed AI Systems," is another noteworthy study. The three main pillars of their research were governance, privacy and robustness. They concluded with a discussion on open challenges and

future research directions towards trustworthy distributed AI, such as the need for trustworthy AI policy guidelines. The researchers suggested that governments and regulatory agencies implement laws that require ethical AI use, data governance accountability and privacy principles to close these gaps. Along with establishing precise rules for data handling and breach reporting, these policies ought to promote openness in AI decision-making processes, Floridi et al., (2018).

Nearly 70% of companies in developing nations have implemented AI in some form to gain a competitive edge and improve operational efficiency, according to a 2020 McKinsey & Company report. Most of the research on AI ethics comes from developed nations like China, the US, and the UK (Tlili et al., 2024). When it comes to integrating AI into business processes, the developed world is leading the way. However, issues like algorithmic bias, transparency and data privacy taint this quick adoption (Maddula, 2018; Sheikh, 2020; Schiff et al., 2020). Such discussions in literature serve as the impetus for this study because researchers are still attempting to understand the fundamentals of artificial intelligence and how it affects data security and privacy.

My study is unique in that it makes the case for data privacy and security in universities. While some studies have contributed to the study of data privacy and security in relation to the use of AI, few of the studies have concentrated more on the impact of AI on data privacy and security in universities. Considering this, the study's goal is to talk about the use of AI in higher education, privacy concerns and monitoring, data security concerns, ethical regulation gaps and opportunities for responsible AI adoption.

AI applications in higher education include student data analytics, adaptive learning systems and administrative automation. Globally, these solutions enhance institutional effectiveness and student performance (Zawacki-Richter et al., 2019). AI is used in Zimbabwe's online learning platforms, digital libraries and testing systems (Chikomba & Mutsagondo, 2022). Benefits like adaptive learning, predictive analytics and administrative automation have been brought about by the global integration of artificial intelligence (AI) in higher education (Zawacki-Richter et al., 2019). However, issues with data privacy, surveillance and the moral management of student information are brought up by the expanding use of AI (Huang, 2023; Fu et al., 2024). Globally, the application of artificial intelligence (AI) in higher education has increased. Intelligent tutoring systems, adaptive learning platforms, automated grading, predictive analytics, administrative automation and chatbots for student support are among the tools that African universities have been implementing (Maluleke, 2025; Modiba, Van den Berg, & Mago, 2024). According to Maluleke's systematic review of 113 papers published between 2020 and 2024, the main advantages of implementing AI in higher education in Africa were improved teaching and learning, increased administrative effectiveness, digital transformation and increased access and inclusion.

Mukwerete and Chikusvura (2024) investigated how college students use AI tools for academic writing and discovered that assignments' grammar, structure and coherence had improved. However, the use is typically personal rather than institutional, and it frequently lacks official guidelines or widespread institutional backing. Another study by Tsekea and Mandoga, (2025) on university libraries in Zimbabwe indicated that, libraries are utilising AI for anti-plagiarism detection tools and chatbots or virtual assistants to answer common questions. However, a lot of libraries stated that they were still in the "adoption stage" as opposed to being fully operational; policy and infrastructure readiness is still lacking. AI-powered student writing tools, libraries, admissions and student support systems in Zimbabwe may collect academic,

personal and occasionally biometric data. Concerns regarding student work ownership and academic integrity are raised by instances in which library systems employ anti-plagiarism tools (Mandoga & Tsekea, 2025).

A legal framework for protecting personal data was established in Zimbabwe by the Cyber and Data Protection Act (2021). Despite this, research indicates that institutional practices frequently fall behind policy frameworks, with universities lacking robust privacy-by-design and data governance mechanisms (Chikomba & Mutsagondo, 2022; Mutsagondo, 2022). Learning management systems (LMS), digital libraries and online platforms are increasingly integrating AI-based tools. However, little is known about whether these implementations adhere to privacy standards or put students at risk for activities like surveillance, unauthorised profiling, or third-party data exploitation.

Despite Zimbabwe's official data protection laws, there are still gaps between policy and practice in higher education institutions. Without proper safeguards, AI-based educational technologies may gather, store and process private student information. Empirical evidence is lacking regarding the following topics: whether vendor contracts comply with Zimbabwe's Data Protection Act; how universities implement data protection in AI-enabled systems; and staff and student awareness of privacy rights.

Large volumes of data are routinely collected by AI-driven systems, which presents privacy and surveillance concerns. Risks include student profiling, unauthorised data use and online activity monitoring (Smuha, 2021). Such actions may jeopardise academic freedom and individual rights, particularly when control is weak. According to Zhao et al. (2021), human decision autonomy, privacy protection, social equity, security responsibility attribution and ecology are the main ethical concerns surrounding AI now. According to their research, the extensive use of AI technology in education is inevitably compromising student privacy while progressively growing the volume of student data. They concluded that to establish effective data protection, governments, educational institutions and AI actors must collaborate. Struppek et al. (2023) in another study found that AI systems are vulnerable to backdoor attacks and data poisoning, among other cyberthreats. By adding malicious data, these attacks could alter AI models and possibly jeopardise educational institutions' decision-making procedures. According to their findings, using AI for crucial tasks raises the risk of these vulnerabilities, necessitating the use of strong cybersecurity measures. Taddeo and Floridi (2018) assert that because universities store enormous volumes of scientific and personal data, they are particularly vulnerable to cyberattacks. By anticipating threats, AI can enhance cybersecurity, but malicious actors can also exploit it. Vulnerabilities are increased in Zimbabwe by inadequate funding and cybersecurity infrastructure, Mhlanga (2020).

The application of artificial intelligence (AI) in African higher education systems is still largely unregulated and subject to serious ethical blind spots. Inadequate ethical frameworks and a lack of public discourse on AI technologies are the main causes of issues like algorithmic bias, data exploitation and lack of transparency, according to Cisse et al. (2020). These concerns are exacerbated by the region's generally low levels of digital literacy and regulatory enforcement capacity.

A significant step was taken in 2021 when Zimbabwe passed the Cybersecurity and Data Protection Act, but problems persist with its actual application, especially in universities (Mhlanga & Moloi, 2022). These organisations are vulnerable to breaches and the misuse of

sensitive data because they usually lack the administrative and technical capacity to enforce data privacy and security standards.

Furthermore, ethical standards specific to the use of AI in education have not yet been developed in many African countries. Implementing Global North frameworks without adapting them to local socio-cultural contexts may lead to AI applications that are ineffective or even harmful (Ndung'u and Signé, 2020). This "regulatory borrowing" often ignores the special needs, vulnerabilities and values of African academic communities.

Despite ethical and legal concerns, AI has a huge potential to improve educational outcomes in Africa. When paired with a strong ethical basis, AI systems can improve student engagement, automate administrative tasks and enable personalised learning (Benaich & Hogarth, 2021). However, the responsible use of AI requires the development of moral oversight processes and inclusive governance models. Investing in private and secure technologies is crucial. According to UNESCO (2021), universities should prioritise algorithmic accountability, data protection and fairness in AI applications. This means establishing transparent data governance frameworks and ensuring that AI systems are auditable and explicable.

Increasing capacity is yet another crucial element. As suggested by Akinyemi and Adepoju (2023), raising the digital and ethical literacy of administrators, staff members and students will empower them to critically assess and manage AI tools. This might mean holding regular training sessions, encouraging interdisciplinary research on the effects of AI, and integrating AI ethics into the curriculum. Co-creating ethical standards suitable for African contexts can also be facilitated by collaboration between governments, universities and the private sector. These collaborations can also help establish regulatory sandboxes that allow safe testing of AI technology before it is widely used (Kraemer-Mbula et al., 2021).

The impact of artificial intelligence (AI) on data security and privacy was investigated in this study using a Systematic Literature Review (SLR). The SLR technique was employed to guarantee comprehensive coverage and reduce bias due to its methodical and repeatable approach to locating, evaluating and synthesising literature (Kitchenham & Charters, 2007; Dewey & Drahota, 2016). Relevant literature was found using five major academic databases: Google Scholar, Scopus, Web of Science, ProQuest, Emerald, ResearchGate DOAJ-ZOU Library and ScienceDirect. In a Boolean search, terms like "Artificial Intelligence," "Privacy," and "Security" were combined. The search was limited to peer-reviewed publications published between 2014 and 2024.

To deal with the large number of results, a purposive sampling strategy guided by the PRISMA framework was employed (Moher et al., 2009). Peer-reviewed studies that examined the impact of AI on data security or privacy, published in English between 2014 and 2024 were accepted. 54 research projects were selected for additional consideration based on methodological rigour and relevance after 196 full texts were reviewed after an initial screening of 1,245 publications. Important information was extracted using a standardised form, including the study's goals, AI techniques and privacy/security findings. To identify recurrent themes, challenges and insights in the selected research, a thematic analysis was conducted (Braun & Clarke, 2006). The SLR technique provided a comprehensive and empirically supported synthesis of current knowledge to identify research gaps and direct future investigations.

We examined empirical studies that addressed artificial intelligence in higher education. Additionally, we used the Boolean operators "OR" to combine various search terms that are used interchangeably, such as AI or Machine Intelligence. The "AND" function was also used to further refine the research topic, which included AI, data security and privacy. Articles written in English and released between 2014 and 2024 were selected. We looked at each publication's titles, abstracts and methods sections to see if the findings and scope matched the review's goals. A total of fifteen items were judged suitable for achieving the review's goals.

Results

Zimbabwean universities are gradually implementing AI technologies, particularly in the following domains: online learning platforms, automated testing systems, digital libraries and student data analytics for performance forecasting. This is in line with worldwide trends in the adoption of AI, even though it occurs in an environment with limited resources and gaps in infrastructure.

AI systems collect vast amounts of private data, including biometric data, academic transcripts and patterns of online behaviours. The lack of formal data privacy policies at many Zimbabwean universities exposes them to misuse and unauthorised access. Furthermore, data collection and utilisation are opaque, and informed consent is inadequate. This knowledge gap increases the risk of inadvertent data leaks and keeps organisations from cultivating a security-conscious culture.

Most Zimbabwean universities, according to the literature, lack specialised cybersecurity personnel and are ill-prepared to manage emerging risks specific to artificial intelligence, like model manipulation, data poisoning and adversarial attacks. Institutional data is therefore more susceptible to manipulation, ransomware attacks and breaches. The Cybersecurity and Data Protection Act (2021) has been put into effect in Zimbabwe; however, there are still ethical problems that need to be addressed, such as algorithmic bias, a lack of accountability and opaque decision-making. Additionally, there are not enough internal compliance mechanisms in place, and stakeholders are not well-informed about their legal responsibilities.

According to the study, administrators, educators and students frequently lack the training necessary to recognise AI systems, adopt safe data practice and identify privacy vulnerabilities. Despite the risks, artificial intelligence presents opportunities for progress. These include personalised learning environments, efficient data management and cybersecurity monitoring through AI-powered intrusion detection systems. However, these benefits are only available if they are implemented properly and backed by monetary investments in secure infrastructure and ethical principles.

Most of the literature currently published on artificial intelligence and data security in education comes from Western or Asian contexts, with little focus on Africa or Zimbabwe. Local research focuses on digitisation problems rather than AI-specific risks and solutions. This highlights the necessity for Zimbabwean academic institutions to carry out more empirical studies and create context-specific policies.

Summary of the Findings

Theme	Key Insights
AI Use in Universities	Growing but uneven across institutions
Privacy Risks	High due to opaque data practices and weak policies
Cybersecurity Preparedness	Low — outdated systems and skills shortages
Legal and Ethical Gaps	Present — lack of enforcement and weak ethical oversight
Digital Literacy	Insufficient — training needed for safe AI adoption
AI Potential	High — for personalisation and threat detection, if implemented responsibly
Research Gap	Lack of localised studies on AI privacy/security in African higher education

Discussion

This study conducted a systematic review of recent literature on the effects of artificial intelligence (AI) on data security and privacy, with a focus on digital environments and higher education. The results show that concerns about privacy issues like data collection, surveillance and lack of consent, as well as security issues like cybersecurity vulnerabilities, data breaches and regulatory compliance, are growing.

Some researchers, such as Bareq et al. (2024) and Mooradian et al. (2025), draw attention to the increasing complexity of managing personal data in AI-powered systems. Some, like Usman et al. (2023), raise ethical questions, arguing that the application of AI might infringe upon fundamental rights like privacy and non-discrimination. They highlight the need for a comprehensive legal and ethical framework to ensure that technological advancements do not compromise basic human rights.

ProQuest produced 96 initial results despite searching several databases; all of these were eliminated during screening, and no relevant articles were discovered. Eleven articles in total were selected after a comprehensive review, as shown in Table 1.

Table 1: Summary of reviewed literature on AI, Privacy and Security

Author(s) and Year	Title of Study	Article Type	Source Database	Addresses Privacy/Security
Bareq et al. (2024)	The role of AI in shaping data privacy	Journal	Emerald Insight	Yes – Focus on data privacy
Mooradian et al. (2025)	The impact of AI on data privacy: A risk management perspective	Journal	Emerald Insight	Yes – Privacy and risk management
Ahmed et al. (2024)	The role of AI in higher education: Benefits and challenges	Journal	Emerald Insight	No – General AI in education

Modiba (2023)	Adoption of AI to enhance records management practices	Journal	Emerald	Partially – Records management and security
Rahmati (2025)	Federated learning for privacy-preserving AI in human-robot collaboration	Journal	Emerald	Yes – Privacy-preserving techniques
Paul (2024)	Privacy and data security concerns in AI	Journal	ResearchGate	Yes – Privacy and security concerns
Deveneni (2024)	AI in data privacy and security	Journal	ResearchGate	Yes – Comprehensive discussion on both
Bonovic et al. (2025)	Privacy, personal data protection and the digital age	Journal	DOAJ-ZOU Library	Yes – Focus on data privacy
Xinyu et al. (2025)	Discussion on AI safety and ethical issues	Journal	DOAJ-ZOU Library	Partially – Ethical implications of AI
Sarikakis et al. (2025)	AI and privacy: The urgent need for children's literacy	Journal	DOAJ-ZOU Library	Yes – Privacy concerns for children
Usman et al. (2023)	AI and fundamental rights: A legal perspective	Journal	Manual Search	Yes – Human rights, privacy, and legal frameworks

Table 2: Database search summary

Database	Articles Screened	Articles Included
Emerald Insight	58	5
ResearchGate	40	2
DOAJ-ZOU Library	30	3
ProQuest	96	0
Manual Search	12	1

Research shows that AI still presents both opportunities and risks when it comes to handling sensitive data. The evolution of privacy-preserving techniques such as federated learning has not been reflected in the legal and ethical frameworks (Rahmati, 2025). Technologists, lawmakers and educators must collaborate to bridge this divide and ensure moral AI use that upholds human rights (Usman et al., 2023).

According to the study, artificial intelligence (AI) has two implications for higher education: it boosts productivity and creativity, but it also poses privacy and security issues. Zimbabwe's issues are made worse by inadequate infrastructure and lax enforcement of data privacy laws. These results are consistent with international research that highlights the necessity of adopting AI in a balanced manner (Luckin et al., 2016; Smuha, 2021). Furthermore, it is essential to

foster an environment of transparency and ethical AI use to lessen prejudices and ensure that everyone in the university ecosystem is treated equally. According to recent research, proactive data privacy and security management in the context of AI is morally necessary to maintain faculty and student trust in addition to being a matter of regulatory compliance (Shadbolt et al., 2020). Finding a balance between innovation and stringent privacy regulations will be crucial to utilising AI in higher education to its full potential while protecting the security and rights of all stakeholders.

Therefore, universities should think about the wider implications for rights, ethics and governance rather than just implementing AI for efficiency. According to Voigt and Von dem Bussche (2017), institutional initiatives should incorporate privacy-by-design principles and conform to international standards like the General Data Protection Regulation (GDPR) of the European Union.

Conclusion

The literature shows that while Zimbabwean universities are using AI, particularly in academic writing, libraries and some administrative or learning-enhancement contexts, adoption is uneven, mostly on a small scale, and hampered by gaps in technology, law, ethics and governance. Data privacy and security are ongoing concerns because institutions are often not fully prepared in terms of policy, infrastructure, staff, or vendor contracts. Even though they are recognised, ethical concerns like bias, intellectual property, academic integrity and transparency are still not sufficiently addressed by formal institutional mechanisms. AI significantly affects university data security and privacy, bringing with it both opportunities and challenges. As educational institutions use AI technologies to enhance student learning and operational effectiveness, the risks of data breaches and ethical concerns pertaining to privacy are becoming more urgent. To lower these risks, universities must implement robust security measures, effective data governance and staff training on AI-driven systems.

References

Abdulrahman, M., Al-Zahrani, T.M. & Talal, M.A. (2024). Exploring the impact of AI on higher education: The dynamics of ethical, social, and educational implications. *Humanities and Social Sciences Communications*, *11*(1), 1-12.

Ahmad, H., Han, M.M., Alam, M.K., Rehmat, M., Irshad, M., Arraño-Muñoz, A. & Ariza-Montes, A. (2023). Impact of artificial intelligence on human loss in decision-making, laziness, and safety in education. *Humanities and Social Sciences Communications, 10*(1), Article 1787. https://doi.org/10.1057/s41599-023-01787-8

Ahmed, A.M., Hassan, H.S. & Abdelkader, M. (2024). *The role of AI in higher education designing higher education courses: Benefits and challenges*. Emerald Insight.

Anjum, N. (2024). AI in education: Striking a balance between innovation and privacy. *AI and Education Review*, *11*(1), 45–60.

Baker, R.S. & Inventado, P.S. (2014). Educational data mining: An overview of the state of the art. *International Journal of Artificial Intelligence in Education, 24*(2), 139–150.

Bareq, L., Smith, J. & Al-Mutairi, H. (2024). The role of AI in shaping data privacy. *Journal of Information Privacy and Ethics, 19*(1), 33–47.

Benaich, I. & Hogarth, I. (2021). *State of AI report 2021*. Air Street Capital. https://www.stateof.ai.

Bishop, M. (2003). *Computer security: Art and science*. Addison-Wesley.

Banović, J.M. & Radisavljević, I.M. (2025). Privacy, personal data protection and the digital age: A (criminal) law" omnibus". *Sociološki pregled*, *59*(1), 36-56.

Braun, V. & Clarke, V. (2006). *Thematic analysis in psychology*. Qualitative Research in Psychology, *3*(2), 77–101.

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

Charles Sturt University Library. (2025). *Library guide: Literature review/systematic literature reviews*. https://libguides.csu.edu.au/litreview.

Chatikobo, M.V. & Pasipamire, N. (2024). *Readiness to embrace artificial intelligence in information literacy instruction at a Zimbabwean University*.

Chigada, J. & Madzinga, R. (2021). Cybersecurity and data protection in Zimbabwe: Opportunities and challenges. *African Journal of Information Systems, 13*(1), 45–62.

Chikomba, T. & Mutsagondo, S. (2022). Digital transformation in Zimbabwean universities: Opportunities and challenges. *Zimbabwe Journal of Educational Technology, 5*(2), 35–48.

Cisse, M., Hope, A. & Moyo, M. (2020). Artificial intelligence in Africa: Policy perspectives and regulatory challenges. *African Journal of Information and Communication, 26*(1), 1–15. https://doi.org/10.23962/10539/30324.

Creswell, J.W. (2014). *Research design: Qualitative, quantitative and mixed methods approaches* (4th ed.). Sage Publications.

Daniel, J.S. (2025). *Artificial intelligence and privacy: Navigating the ethical frontier*. Cambridge University Press.

Deveneni, K.S. (2024). *AI in data privacy and security*. ResearchGate.

Devineni, S.K. (2024). Artificial intelligence in data privacy and security. *Journal of Cybersecurity and Ethics, 12*(3), 45–62.

Dewey, A. & Drahota, A. (2016). *Introduction to systematic reviews*. JRSM, 109(4), 148–152. Kitchenham, B., & Charters, S. (2007). *Guidelines for performing SLRs in Software Engineering*.

Floridi, L. & Cowls, J. (2019). A unified framework of five principles for AI in society. *Harvard Data Science Review, 1*(1). https://doi.org/10.1162/99608f92.8cd550d1.

Fu, Y. & Weng, Z. (2024). Navigating the ethical terrain of AI in education: A systematic review on framing responsible human-centred AI practices. *Computers and Education: Artificial Intelligence*, *7*, 100306.

Harris, J. (2020). The cybersecurity landscape in higher education: Challenges and solutions. *Journal of Higher Education Policy and Management, 42*(3), 267–279.

Hintzbergen, J., Hintzbergen, K., Baars, H. & Smulders, A. (2010). *Foundations of information security based on ISO27001 and ISO27002*. Van Haren Publishing. ISBN 978-90-8753-568-1.

Holmes, W., Bialik, M. & Fadel, C. (2019). *Artificial intelligence in education: Promises and implications for teaching and learning*. Centre for Curriculum Redesign.

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. https://doi.org/10.1080/13600834.2019.1573507

Huang, L. (2023). Ethics of artificial intelligence in education: Student privacy and data protection. *Science Insights Education Frontiers, 16*(2), 1201–1213.

Luckin, R., Holmes, W., Griffiths, M. & Forcier, L. B. (2016). *Intelligence unleashed: An argument for AI in education*. Pearson.

Maddula, S.S. (2018). The impact of AI and reciprocal symmetry on organisational culture and leadership in the digital economy. *Engineering International, 6*(2), 201–210.

McKinsey & Company. (2020). *The state of AI in 2020*. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/global-survey-the-state-of-ai-in-2020

Mhlanga, D. (2020). Artificial Intelligence in the fourth industrial revolution: The case of Africa. *Journal of African Studies and Development, 12*(2), 31–40. https://doi.org/10.5897/JASD2019.0561

Miller, J. (2021). Data privacy in higher education: Navigating the complexities. *Higher Education Review, 53*(1), 55–70.

Modiba, M. (2023). *Adoption of AI to enhance records management practices*. Emerald.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G. & TP Group. (2009). *PRISMA statement*. PLoS Med, *6*(7).

Mooradian, N., Franks, P.C. & Srivastav, A. (2025). *The impact of AI on data privacy: A risk management perspective*. Emerald Insight.

Moyo, A., Makota, J. & Gumbo, S. (2025). ChatGPT Experiences in Universities in Zimbabwe. *Oikos: The Zimbabwe Ezekiel Guti University Bulletin of Ecology, Science Technology, Agriculture, Food Systems Review and Advancement*, *3*(1 and 2), 72-92.

Mutsagondo, S. (2019). Challenges in the implementation of modern records management systems in Zimbabwe. *Journal of the South African Society of Archivists, 52*(1), 20–35.

Mutsagondo, S. (2022). Records and information management policy and the management of public sector records in Zimbabwe. *Information Development, 38*(4), 532–544.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.

Parker, D. B. (2002). *Toward a new framework for information security?* In J. H. P. Tipton & M. Krause (Eds.), *Computer Security Handbook* (4th ed.). John Wiley & Sons.

Paul, J. (2024). Privacy and data security concerns in AI. *Stanford University AI Policy Review*. https://www.researchgate.net/publication/385781993_Privacy_and_data_security_concerns_in_AI.

Rahmati, M. (2025). *Federated learning for privacy-preserving AI in human-robot collaboration*. Emerald.

Sarikakis, K. & Chatziefraimidou, A. (2025). *AI and privacy: The urgent need for children literacy*. *Revista Comunicando*, *14*(1), e025003-e025003.

Shadbolt, N., O'Hara, K. & Hall, W. (2020). The ethics of AI in education: A framework for understanding and addressing the challenges. *AI & Society, 35*(3), 577–590. https://doi.org/10.1007/s00146-019-00862-y.

Smuha, N.A. (2021). Beyond a human rights-based approach to AI governance: Promise, pitfalls, plea. *Philosophy and Technology, 34*(1), 91–113. https://doi.org/10.1007/s13347-019-00391-2.

Taddeo, M. & Floridi, L. (2018). How AI can be a force for good. *Science, 361*(6404), 751–752. https://doi.org/10.1126/science.aat5991.

Tarisayi, K. & Manhibi, R. (2025). Revolutionising Education in Zimbabwe: Stakeholder Perspectives on Strategic AI Integration. *Journal of Learning and Teaching in Digital Age*, *10*(1), 87-93.

Tlili, A., Denden, M., Abed, M. & Huang, R. (2024). Artificial intelligence ethics in services: Are we paying attention to that? *The Service Industries Journal*, *44*(15-16), 1093-1116.

Tranfield, D., Denyer, D. & Smart, P. (2003). Developing evidence-informed management knowledge. *British Journal of Management*, *14*(3), 207–222.

Usman, H., Nawaz, B. & Naseer, S. (2023). The future of state sovereignty in the age of artificial intelligence. *Journal of Law Social Studies*, *5*, 142-152.

Voigt, P. & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004.

Xinyu, C., Tianfang, H., Yanlin, L. & Haoyuan, Y. (2025). *Discussion on AI safety and ethical issues*. In *ITM Web of Conferences,* 70, 04031. EDP Sciences. https://doi.org/10.1051/itmconf/20257004031.

Zawacki-Richter, O., Marín, V.I., Bond, M. & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education – where are the educators? *International Journal of Educational Technology in Higher Education, 16*(1), 1–27. https://doi.org/10.1186/s41239-019-0171-0.

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. https://doi.org/10.3969/j.issn.1009-8097.2016.03.001.