

Ethical Governance of Virtual Learning and Student Privacy in Foreign Cloud-Hosted Learning Environments in Rwanda: A Systematic Review.

Albert Rugaba

Bishop Stuart University, Kakoba Campus, Mbarara, Uganda

Page | 1

ABSTRACT

Background:

The recent development of cloud computing and Learning Management Systems has dramatically changed teaching and learning processes in higher education institutions throughout the world. This systematic review aims at synthesizing and critically evaluating existing evidence on ethical governance mechanisms and student privacy protections in foreign cloud-hosted learning environments in higher education, particularly in Rwanda.

Methods:

Peer-reviewed literature published between 2005 and 2025 was systematically searched in relevant databases. Studies dealing with ethical governance, student privacy, cloud computing, Learning Management Systems, digital sovereignty, and higher education were considered in the current review. The systematic review covered studies involving higher education institutions, students, faculty members, institutional governance mechanisms, and foreign cloud-hosted learning platforms.

Results:

A systematic review methodology was used to find, screen, appraise, and synthesize evidence in 38 articles. The systematic review was guided by the concepts of Digital Sovereignty Theory, Institutional Theory, and Technology-Organization-Environment (TOE) Framework. It was found that inadequate data center infrastructure, poor governance mechanisms at institutions, and low digital literacy of students and faculty members are the main barriers to the proper protection of students' data and compliance with Law No. 058/2021 on personal data and privacy in Rwanda. Furthermore, institutional pressures make universities adopt foreign cloud services in order to achieve legitimacy and efficiency, regardless of privacy and data sovereignty issues. However, the use of cloud computing technologies brings many advantages, such as accessibility, scalability, collaboration, and learning analytics.

Conclusion:

In order to ensure strong ethical governance and data sovereignty in Rwanda, it is necessary to invest in local digital infrastructure, develop robust institutional governance frameworks, enforce data protection policies, perform regular Data Protection Impact Assessments, and build digital ethics and cybersecurity capacity.

Future research:

Future research is required to explore the consequences of the dependence on foreign cloud hosting in higher education in Rwanda.

Keywords: Ethical governance; student privacy; cloud computing; Learning Management Systems; Rwanda higher education

Submitted: May 20, 2026 **Accepted:** June 21, 2026 **Published:** July 13, 2026

Corresponding Author: Albert Rugaba

Email: rugabaalbert7@gmail.com

Bishop Stuart University, Kakoba Campus, Mbarara, Uganda

INTRODUCTION

The fast growth of digital education technologies has brought about fundamental changes in higher education systems around the globe, and cloud computing and Learning Management Systems have become the core of teaching and learning processes. Foreign cloud-based educational systems are used by universities and schools as a means to promote learning and make it more accessible, scalable, collaborative, and resourceful. While cloud-based technologies provide many flexible options for learners, they raise several problems regarding data storage and

processing, cross-border data flows, and data governance (Armbrust et al., 2010; Sultan, 2010). At the same time, an intensive use of technology-based systems leads to the misuse of personal information, violations of the privacy of students, and unethical use of personal data in the digital environment (Acquisti et al., 2015; Zuboff, 2019).

From an ethical governance perspective, data governance in foreign cloud-hosted learning environments poses several questions as to institutional responsibility, regulatory compliance, accountability, transparency, and digital sovereignty. The key characteristics of the ethical

governance framework include accountability, transparency, fairness, and protection of people's rights (Floridi, 2013; Floridi & Taddeo, 2016). Yet, cloud computing complicates governance since the data used in the educational process can be processed and stored outside national borders, and hence traditional regulatory frameworks cannot be effectively applied (Mueller, 2017). The concept of digital sovereignty represents the tension between the globally distributed digital environment and a country's right to govern, protect, and control its data resources (Couture & Toupin, 2019; Pohle & Thiel, 2020). Besides, various institutional issues play a vital role in cloud computing governance as institutions usually tend to adopt similar technologies out of pressure, which can be coercive, normative, or mimetic in nature, and despite the lack of institutional preparedness (DiMaggio & Powell, 1983; North, 1990; Scott, 2014).

Privacy is among the most serious problems in foreign cloud-hosted learning environments, as there is an increased reliance on learning analytics and data-intensive technologies that support teaching and learning processes and decision-making at institutions. Privacy goes beyond data protection, implying the issue of contextual integrity according to which personal data should be collected, processed, and used in appropriate ways and contexts (Nissenbaum, 2010; Solove, 2006). The use of learning analytics as a component of LMS systems raises the ethical problem of informed consent, surveillance, profiling, and constant monitoring of students' performance (Slade & Prinsloo, 2013; Pardo & Siemens, 2014). Also, cloud computing systems face security risks in the form of unauthorized access, data breaches, cyberattacks, and loss of institutional control over personal data (Hashizume et al., 2013; Subashini & Kavitha, 2011). All these issues demonstrate the necessity of the creation of ethical governance frameworks that would protect students' privacy and promote responsible use of digital technologies in higher education.

The increasing use of cloud-hosted educational systems in African countries, including Rwanda, takes place against the backdrop of the countries' and their higher education institutions' digital transformation and integration of educational technologies. However, regulatory and institutional frameworks are still emerging due to the difficulties of addressing the challenges of cross-border data governance, privacy protection, and ethical management of digital education. Regional policy instruments such as the Malabo Convention and the African Union Data Policy Framework outline the basic principles of data protection, cybersecurity, and digital governance on the continent (African Union, 2014, 2022). In terms of national legislation, Law No. 058/2021 on the protection of personal data and privacy serves as the legal framework for protecting personal information in Rwanda (Republic of Rwanda, 2021). Nevertheless, the existing body of literature contains few studies on the topic of ethical governance and student privacy in foreign cloud-hosted learning

environments in higher education in Rwanda. Most existing studies focus either on cloud computing adoption, digital transformation, or data protection and do not consider the interplay between ethical governance, institutional issues, and student privacy in foreign cloud-hosted learning environments.

This paper is aimed at synthesizing and critically analyzing the available evidence on the ethical governance mechanisms and student privacy protections in foreign cloud-hosted learning environments in higher education, particularly in Rwanda.

Theoretical Framework

This study is based on three interrelated theoretical frameworks, namely, Digital Sovereignty Theory, Institutional Theory, and the Technology-Organization-Environment (TOE) Framework. Altogether, these frameworks provide a multidimensional view of the issues of ethical governance and student privacy in foreign cloud-hosted learning environments in Rwanda. Digital Sovereignty Theory explains jurisdictional control over data in cross-border cloud systems, Institutional Theory highlights organizational isomorphic pressures in technology adoption, while the TOE Framework describes the role of technological, organizational, and environmental factors in institutional decision-making. Overall, these theories form the theoretical basis for analyzing the issues of cloud-based learning in the context of the emerging data protection regime in Rwanda (Pohle & Thiel, 2020; Scott, 2014; Mell & Grance, 2011).

Digital Sovereignty Theory

Digital Sovereignty Theory, proposed by such scholars as Pohle and Thiel (2020) and Couture and Toupin (2019), suggests that control over digital data is increasingly concerned with jurisdictional questions, regulatory power, and national authorities in the global digital ecosystem. According to the theory, data generated in a territory belongs to the legal and political jurisdiction of this territory, regardless of its location and the cloud computing technologies used for data processing and storage. In the case of cross-border data flow enabled by cloud computing technologies, the question of governance and accountability becomes even more complicated (Armbrust et al., 2010; Mueller, 2017).

Digital Sovereignty Theory is extremely relevant for the analysis of higher education because of the extensive collection of student information, including academic records, personal identifiers, and learning analytics generated in the process of working with Learning Management Systems (Coates et al., 2005; Williamson, 2017). If this data is stored in foreign cloud-based platforms, the jurisdictional issues, enforceability of privacy rights, and legal aspects of compliance with the national laws become even more relevant. Such a situation becomes especially problematic due to the global nature of cloud computing technologies, according to which data can be distributed

among international servers (Armbrust et al., 2010; Sultan, 2010).

In the case of Rwanda, Digital Sovereignty Theory fits very well with Law No. 058/2021 on the protection of personal data and privacy, which establishes clear conditions for lawful processing of personal data and its transfer to another state. The theory forms a conceptual framework for the evaluation of the ways Higher Learning Institutions comply with national legislation while using foreign cloud platforms. Moreover, it highlights the importance of regulatory institutions in ensuring that the data processing is in accordance with national sovereignty and data protection rules (Republic of Rwanda, 2021; African Union, 2014, 2022).

Overall, Digital Sovereignty Theory provides a lens to analyze the tensions between global digital infrastructure and national sovereignty. The theory emphasizes the importance of balancing technological efficiency with regulatory control, data protection, and institutional accountability in the cloud-based education systems (Couture & Toupin, 2019; Pohle & Thiel, 2020).

Institutional Theory

Institutional Theory, formulated by DiMaggio and Powell (1983) and developed by Scott (2014), suggests that organizational behavior is determined not by purely technical and economic factors, but by institutional factors. These factors include coercive, normative, and mimetic institutional pressures, which compel organizations to adopt certain structural and procedural practices for gaining legitimacy, stability, and recognition within the organizational environment.

In higher education, Institutional Theory helps to understand the adoption of cloud-based Learning Management Systems by universities as a response to global academic standards, technological tendencies, and competition pressures (Selwyn, 2016; Williamson, 2017). Universities tend to adopt foreign cloud-based digital platforms in order to conform to the best practices, to gain reputation and competitiveness within the globally integrated education market (Coates et al., 2005). This process can be considered as the case of mimetic isomorphism, as organizations try to imitate their peers that are recognized as more advanced or successful (DiMaggio & Powell, 1983).

However, Institutional Theory reveals the governance problem at the same time – adoption of foreign cloud systems tends to be much faster than the creation of institutional data governance practices that can handle such risks as data breaches, unauthorized access, and surveillance issues (Slade & Prinsloo, 2013; Zuboff, 2019).

Within the context of Rwanda, Institutional Theory can help to understand why Higher Learning Institutions tend to adopt foreign cloud-based platforms regardless of the risks of the loss of data sovereignty and non-compliance with Law No. 058/2021. Various institutional pressures related to globalization, funding agencies, and international partnerships tend to shape the decision-making process of

higher education institutions (Republic of Rwanda, 2021; Scott, 2014).

Technology-Organization-Environment (TOE) Framework

The Technology-Organization-Environment (TOE) Framework, developed by Tornatzky and Fleischer and widely applied in technology adoption studies, explains organizational adoption of technology through three contextual factors, namely, technological, organizational, and environmental factors (Mell & Grance, 2011; Sultan, 2010).

In terms of technological aspects, Rwandan higher education institutions tend to use foreign cloud infrastructure due to the absence of local data center infrastructure and advanced technological capabilities of the foreign cloud services, such as scalability, accessibility, and interoperability (Armbrust et al., 2010; Subashini & Kavitha, 2011). These advantages make cloud computing systems attractive for handling large volumes of educational data.

In terms of organizational aspects, the factors such as lack of financial resources, poor ICT skills of university staff, and absence of institutional data governance structure play a role in the adoption of foreign cloud platforms (Sackey & Bahl, 2020). Universities lack the necessary technological capability to develop or maintain local secure infrastructure, which makes foreign cloud services the practical choice.

Environmental factors such as regulatory framework, cybersecurity policies, and national digital transformation strategy also play a role in technology adoption. In the case of Rwanda, institutions operate within the scope of the requirements of Law No. 058/2021, data governance frameworks of the African Union, and international data protection principles (African Union, 2014, 2022; UNCTAD, 2021).

Overall, the TOE Framework explains the ongoing adoption of foreign cloud-hosted learning environments in Rwanda. It proves that technology adoption is affected not only by innovations, but also by the interactions of organizational capability, technological infrastructure, and the environment (Mell & Grance, 2011; Sultan, 2010).

Research Questions

The present study is based on the theoretical concepts of Digital Sovereignty Theory, Institutional Theory, Technology-Organization-Environment (TOE) Framework, and data ethics perspectives that together explain the ways of student data governance in foreign cloud-hosted learning environments. These theories involve jurisdictional control over data, institutional pressures in the adoption of the technology, technological, organizational, and environmental factors affecting implementation, and the ethical importance of balancing innovation and accountability in cloud computing and LMS. While global and regional frameworks exist, there are still challenges in

terms of effective ethical governance of student data within higher education institutions in Rwanda when using foreign digital platforms. That is why the study is guided by the following research questions: *How does digital sovereignty affect the ethical governance of student data in foreign cloud-hosted learning environments in Rwanda? How do institutional pressures affect the adoption of foreign cloud-based learning systems in Rwandan higher education institutions? How do technological, organizational, and environmental factors affect the implementation of cloud-hosted learning platforms? What student privacy risks are associated with cloud computing and Learning Management Systems in higher education? How effective is the legal and policy framework of Rwanda in ensuring the ethical governance of student data in foreign cloud-hosted systems?*

RESEARCH METHODOLOGY

Research Design

For the current synthesis, an SLR design based on the PRISMA 2020 framework was applied to evaluate the evidence on ethical governance and privacy of students in the cloud-hosted learning environment abroad. As opposed to other review designs, SLRs provide a systematic and reproducible synthesis that helps mitigate bias and enhance transparency (Williamson, 2017; Zuboff, 2019). The theoretical bases of this systematic literature review are Digital Sovereignty Theory, Institutional Theory, and Technology-Organization-Environment (TOE) Framework, which reveal the aspects of governance structures, institutional adoption, and regulations of cloud educational systems in various countries (Couture & Toupin, 2019; DiMaggio & Powell, 1983; Mell & Grance, 2011). The three above-mentioned theories will assist in the interpretation of evidence concerning cloud governance, institutional pressures, and privacy issues in the higher education systems (Armbrust et al., 2010; Pohle & Thiel, 2020), while the literature base covers the time period of 2005-2025 and addresses cloud computing, learning analytics, and digital governance (Coates et al., 2005; Slade & Prinsloo, 2013).

Eligibility Criteria

To be included in the present SLR, studies were peer-reviewed journal articles, scholarly books, conference papers with a robust methodology, and official policy documents published during 2005-2025 and focusing on such topics as cloud computing, Learning Management Systems, ethical governance, student privacy, digital

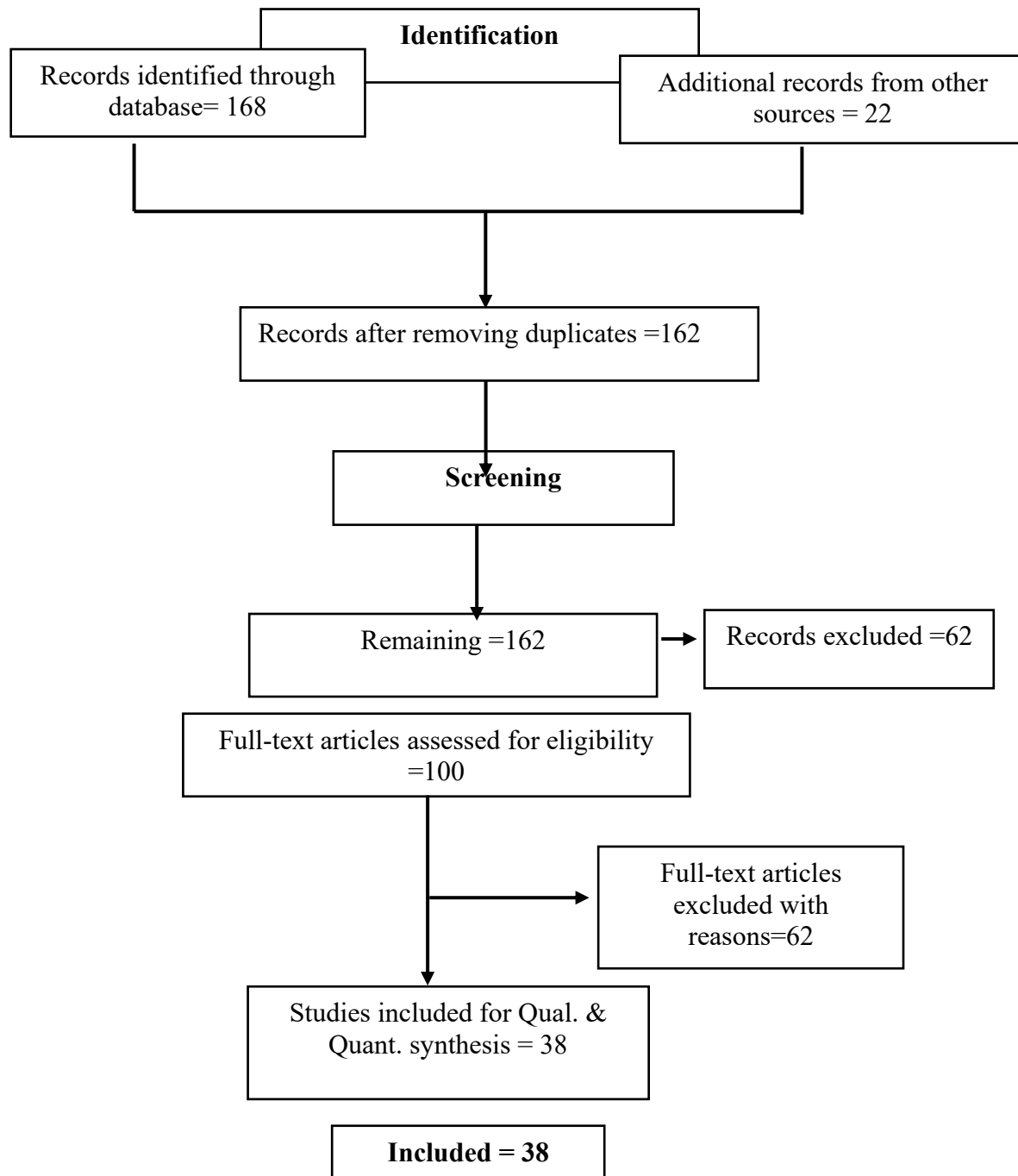
sovereignty, learning analytics, and cross-border data governance within higher education settings (Coates et al., 2005; Slade & Prinsloo, 2013; Zuboff, 2019). In addition, studies with non-educational cloud applications, lack of theoretical and empirical foundations, non-higher-education focus, opinion pieces, or those that have not been translated into English were excluded (Williamson, 2017; OECD, 2013). According to Couture and Toupin (2019) and Pohle and Thiel (2020), the studies selected were grouped into four thematic categories: ethical governance mechanisms, student privacy and data protection, institutional adoption of cloud-hosted learning environments abroad, and digital sovereignty with cross-border data governance.

Information Sources and Search Strategy

To obtain literature for the review, Google Scholar was used as a primary source supplemented by backward and forward citation tracking to find more literature on cloud computing and governance in higher education institutions (Armbrust et al., 2010; Sultan, 2010). Policy documents by UNESCO, OECD, the African Union, and the Government of Rwanda were used to conduct a detailed analysis of data protection and digital governance frameworks (African Union, 2014; African Union, 2022; Republic of Rwanda, 2021; OECD, 2013). The search strategy involved the use of keywords and Boolean operators ("AND" / "OR"): "cloud-hosted learning environments," "Learning Management Systems," "student data privacy," "ethical governance," "digital sovereignty," "cross-border data governance." The search was performed within English-language publications in the time period of 2005-June 2025 (Williamson, 2017; OECD, 2013; Zuboff, 2019).

Selection Process

The identified publications were exported to the review database, and duplicate records were removed before the actual screening (Williamson, 2017). Titles and abstracts of all records were screened according to eligibility criteria, followed by the evaluation of full texts of relevant studies regarding cloud computing and student privacy in higher education systems (Slade & Prinsloo, 2013). Two reviewers conducted the screening independently to ensure rigor and reduce potential bias. If disagreement occurred, further discussion led to reaching an agreement (DiMaggio & Powell, 1983). Automation tools were not used in the process, and a PRISMA 2020 flow diagram was made (Zuboff, 2019).



Data Collection Process

In parallel with the screening, data extraction took place independently by two reviewers who used a standardized matrix including authorship, year, context, methodology, theoretical basis, governance dimensions, technologies

used, ethical issues, privacy concerns, findings, and policy implications (Williamson, 2017; Slade & Prinsloo, 2013). The collected data were compared, and discrepancies were discussed to verify the data obtained against the original literature sources (Coates et al., 2005). The missing or

unclear information was found in additional parts of the same studies, without

Data Items and Missing Information

The following items of outcomes were extracted from the literature sources: ethical governance mechanisms, institutional governance frameworks, student privacy protections, digital sovereignty, cross-border data governance, governance of Learning Management Systems, adoption of cloud computing, learning analytics, and regulation (Slade & Prinsloo, 2013; Pohle & Thiel, 2020). The findings obtained from the sources were only explicitly reported; no imputation or assumption was made regarding missing data (Coates et al., 2005; Williamson, 2017).

Risk of Bias Assessment and Quality Appraisal

In order to assess methodological quality and risk of bias, two reviewers appraised studies independently according to the Joanna Briggs Institute (JBI) Critical Appraisal Checklists for different designs of each particular study (Williamson, 2017). The appraisal considered such elements as methodological rigor, sampling procedures, analytical quality, reporting, and relevance to ethical governance and student privacy in a cloud environment (Slade & Prinsloo, 2013). Disagreements were solved through discussions, with priority given to peer-reviewed journal articles and books in cloud computing and digital governance (Armbrust et al., 2010; Hashizume et al., 2013; Pardo & Siemens, 2014).

Data Preparation and Synthesis

The collected data were standardized to ensure consistency of the terminology connected to ethical governance, cloud computing, privacy, and digital sovereignty while preserving their initial meaning (Couture & Toupin, 2019; Pohle & Thiel, 2020). Due to heterogeneity, a qualitative thematic synthesis was chosen, and it entailed the processes of open coding and grouping of findings into four thematic categories: ethical governance mechanisms, student privacy and data protection, institutional adoption of cloud-hosted learning environments, and digital sovereignty with cross-border data governance (Slade & Prinsloo, 2013; Williamson, 2017).

Effect Measures, Bias, and Certainty of Evidence

There were no quantitative measures and meta-analyses due to qualitative synthesis of the literature (Slade & Prinsloo, 2013). The statistical heterogeneity was not assessed due to the heterogeneity of study designs and contexts, but the conceptual heterogeneity was discussed (Couture & Toupin, 2019). No sensitivity analysis and publication bias assessment were done because the bias was already

mitigated by including peer-reviewed and policy literature (OECD, 2013; African Union, 2022). The GRADE assessment was not conducted because it concerns intervention studies, not the synthesis of conceptual and qualitative evidence (Zuboff, 2019).

Presentation of Results and Ethical Considerations

Results will be presented qualitatively in terms of thematic synthesis with the use of evidence tables, thematic matrices, and the PRISMA 2020 flow diagram. Appendix A presents excluded literature and reasons for exclusion (Williamson, 2017; Slade & Prinsloo, 2013). No ethical approval was required as secondary literature was used in the review, but academic integrity was kept via precise citations and avoidance of plagiarism (Solove, 2006; Nissenbaum, 2010; Zuboff, 2019). Throughout the research process, ethical considerations regarding privacy, data governance, and proper use of educational data were taken into account (Florida & Taddeo, 2016; OECD, 2019).

The systematic search and screening process identified studies relevant to ethical governance and student privacy in foreign cloud-hosted learning environments in higher education. After removal of duplicates and screening against eligibility criteria, 38 studies were included in the final synthesis. The selection process followed PRISMA 2020 guidelines, involving sequential stages of identification, screening, eligibility assessment, and inclusion. Full-text screening led to the exclusion of studies that were not focused on higher education, lacked methodological grounding, or were non-empirical or non-policy relevant. A detailed PRISMA flow diagram summarizing identification, screening, eligibility, and inclusion is presented in Figure 1, while excluded studies and reasons for exclusion are provided in Appendix A (Williamson, 2017; OECD, 2013). Registration Number: J26/BSU/PHD-EPMA/0248

RESULTS

Description of Included Studies and Study Features

This systematic review covered 38 articles published from 2005 to 2025, including conceptual/theoretical and empirical literature about cloud computing in education, LMS governance, student privacy, and digital sovereignty. Generally, theoretical and conceptual studies prevailed within the literature corpus, while the number of empirical pieces validating institutional practice and student data governance was rather low. Three main theoretical frameworks used within this literature were Institutional Theory, Digital Sovereignty Theory, and Technology-Organization-Environment (TOE) Framework (DiMaggio & Powell, 1983; Couture & Toupin, 2019; Mell & Grance, 2011).

Table 1. Characteristics of Included Studies

Type of study	Topic of study	Methodological approach	Key theories/frameworks	Main contribution
Conceptual studies	Ethics and governance	Theoretical analysis	Floridi (2013); Nissenbaum (2010)	Foundations of data governance ethics
Empirical studies	LMS and learning analytics	Qualitative/mixed methods	Slade & Prinsloo (2013)	Evidence on student privacy risks
Policy documents	Data protection regulation	Policy/legal analysis	OECD (2013); AU (2022)	Frameworks for governance and compliance
Technical studies	Cloud infrastructure	Conceptual/technical review	Armbrust et al. (2010)	Insights into cloud system architecture

Overall, the institutional adoption process was heavily influenced by efficiency considerations, technology dependence, and regulatory ambiguity, with surveillance learning analytics increasingly integrated into educational platforms (Zuboff, 2019; Williamson, 2017).

Bias within Included Studies

Generally, the methodological quality of included studies differed depending on their design. Conceptual pieces were characterized by a moderate to high interpretive bias caused

by a low level of empirical validation. Empirical studies, in turn, were methodologically rigorous but contextually non-generalizable beyond particular institutions or countries. Finally, policy documents were authoritative and policy-relevant but had no features characteristic of scholarly research, such as methodological transparency. As a result, the overall risk of bias within this evidence base can be considered as moderate due to its heterogeneity, inconsistency in reporting, and lack of analytical depth (Hashizume et al., 2013; OECD, 2013).

Table 2. Risk of Bias Assessment

Type of study	Risk of bias	Methodological rigor	Transparency
Conceptual studies	Moderate-High	Moderate	Moderate
Empirical studies	Low	High	High
Policy documents	Moderate	Moderate	High

Theme 1: Ethical Governance and Stakeholder Involvement

The first theme revealed by this synthesis is a multidimensional concept of ethical governance, which includes regulatory compliance, institutional legitimacy, and data protection ethics. According to the majority of studies, ethical governance represents a tool to ensure accountability, transparency, and legal processing of student data in a digital learning environment (Floridi, 2013; Solove, 2006; Nissenbaum, 2010). However, cloud-hosted

platforms add to the complexity of the governance process due to cross-border data flows and jurisdictional fragmentation. Institutions are usually driven by coercive and normative pressures focusing on technological adoption and efficiency instead of participatory governance structures (DiMaggio & Powell, 1983; Scott, 2014). On the other hand, contemporary policy frameworks emphasize the importance of stakeholder involvement in governance processes, especially concerning LMS platforms and learning analytics systems (OECD, 2013; UNESCO, 2021).

Table 3. Conceptualizations of Ethical Governance

Dimension of governance	Number of studies	Key focus area	Supporting literature
Regulatory compliance	34 studies	Legal/policy adherence	Republic of Rwanda (2021); African Union (2022); UNCTAD (2021)
Institutional legitimacy	29 studies	Adoption pressures	DiMaggio & Powell (1983); Scott (2014)
Data protection ethics	31 studies	Privacy and consent	Floridi (2013); Nissenbaum (2010)
Cross-border governance	27 studies	Data sovereignty	Couture & Toupin (2019); Pohle & Thiel (2020)

Theme 2: Structural Barriers

This theme encompasses persistent structural barriers to ethical governance within cloud-hosted learning environments. One of the most common barriers is institutions' reliance on foreign cloud infrastructure due to a lack of national data centre capacity, which reduces institutional control over learning data and exposes it to foreign jurisdiction (Armbrust et al., 2010; Subashini & Kavitha, 2011). Other structural barriers include a lack of institutional capacity to conduct such actions as Data Protection Impact Assessment (DPIA), to implement cybersecurity measures, and monitor compliance (Hashizume et al., 2013; Sackey & Bahl, 2020). Communication barriers between technical staff, administrators, and policy makers hinder the implementation process, and the digital literacy gap reduces the effectiveness of data protection compliance (Slade & Prinsloo, 2013; Williamson, 2017).

Theme 3: Benefits of Cloud-Hosted Learning Systems

Despite the existence of ethical issues, this body of literature emphasizes several important advantages of cloud-hosted learning environments. First of all, one of the main advantages of cloud-based systems is increased access and scalability of digital learning without substantial investments in infrastructure (Armbrust et al., 2010; Sultan, 2010). Secondly, cloud infrastructure makes institutions more efficient due to improved data management and decreased burden of ICT infrastructure (Coates et al., 2005). Thirdly, learning analytics tools available in LMS platforms enable data-driven decision making, although they create ethical issues related to surveillance and invasion of privacy (Slade & Prinsloo, 2013; Williamson, 2017). Lastly, cloud technology adoption is also associated with institutional modernization and competitiveness in higher education systems (Selwyn, 2016; UNESCO, 2021).

Theme 4: Student Privacy Risks and Challenges in Data Governance

Another key finding of the literature synthesis is the ongoing risks of student privacy violation within foreign cloud-hosted learning environments. LMS platforms gather substantial amounts of behavioral and academic data, such as logins, engagement, and assessment data, often without full awareness of students (Coates et al., 2005; Williamson, 2017). Cross-border data storage raises the question of jurisdiction and limits national data protection law enforcement (Mueller, 2017; Republic of Rwanda, 2021). In addition, the literature pays attention to the development of surveillance capitalism in education, when data extraction and behavior tracking are prioritized over privacy protection (Zuboff, 2019). It causes ethical questions regarding informed consent, transparency, and student autonomy in a digital learning environment (Nissenbaum, 2010; Solove, 2006). Weakness of governance framework and a lack of

technical safeguards increase vulnerability to data breaches and unauthorized access (Hashizume et al., 2013; Subashini & Kavitha, 2011).

Meta-analysis, Heterogeneity, and Evidence Synthesis

No meta-analysis was performed due to the qualitative and heterogeneous nature of the included studies. The variability in theoretical frameworks, methodologies, institutional context, and governance definitions did not allow for statistical analysis. Consequently, findings were synthesized thematically, with heterogeneity being conceptual/disciplinary, not statistical in nature (Williamson, 2017).

DISCUSSION OF FINDINGS

This review highlights how ethical governance and student privacy in foreign cloud-based learning environments are influenced by a variety of factors, including technological dependency, institutionality, and fragmented regulations. It becomes clear from the TOE model that limited national infrastructure forces higher education institutions to turn to foreign cloud services and thus decreases local control over educational data while increasing cross-border risks related to governance (Armbrust et al., 2010; Mell & Grance, 2011). Moreover, Institutional Theory argues that universities tend to use cloud technologies because of coercion and isomorphic pressures associated with attempts to maintain organizational legitimacy despite poor or undeveloped governance frameworks (DiMaggio & Powell, 1983; Scott, 2014).

Comparison with Previous Studies

It must be noted that the findings obtained during this research coincide with previous findings on how cloud adoption in education is usually based on efficiency and isomorphism, but not on regulatory preparedness (Sultan, 2010; Williamson, 2017). Similarly, other researchers argue that learning analytics systems increase surveillance risks and threaten established privacy norms in education (Slade & Prinsloo, 2013; Zuboff, 2019). Moreover, the found gaps in governance correspond to the global problem of digital sovereignty and jurisdictional issues in cloud-based infrastructure (Couture & Toupin, 2019).

Explanation of Findings

Persistence of privacy risks is possible due to insufficient governance capacity of the institution, a lack of technical skills needed to conduct a DPIA, and dependence on foreign service providers. Normalization of data-intensive educational systems leads to acceptance of surveillance-based analytics, which is performed without sufficient ethical assessment (Nissenbaum, 2010; Solove, 2006).

Generalizability

The findings can be generalized to higher education systems of developing countries with a similar level of dependence on foreign cloud infrastructure. However, regional differences in terms of regulatory maturity and infrastructure make it difficult to generalize to advanced digital ecosystems (OECD, 2013; UNCTAD, 2021).

CONCLUSION

Issues of ethical governance and student privacy in cloud-hosted learning environments abroad are considerably influenced by the factors of infrastructural dependence, weak governance capacity, and low levels of digital literacy. Infrastructural dependence makes institutions lose control over data and increases their vulnerability to cross-border governance issues (Armbrust et al., 2010; Mueller, 2017). Institutional adoption of foreign clouds is mostly based on legitimacy considerations rather than on the ability to govern, which results in fragmented governance and poor compliance with the national data protection regulations (DiMaggio & Powell, 1983; Republic of Rwanda, 2021). Insufficient awareness of the rules of data protection makes institutions more vulnerable to surveillance and data misuse (Nissenbaum, 2010; Williamson, 2017).

Improvement of ethical governance requires a comprehensive approach that should combine infrastructure development, institutional reforms, and human resource development. The development of national cloud infrastructure, DPIA compliance, and integration of digital ethics training into curricula are important for the sustainability of data sovereignty and privacy governance in higher education (Couture & Toupin, 2019; UNESCO, 2021). The future research could be directed towards the empirical analysis of the effectiveness of governance of foreign clouds in higher education systems of Africa.

Limitations of Included Studies and Review

The included studies suffer from heterogeneity of methodologies, dominance of conceptual works over empirical ones, and lack of African-specific sources. As for the review, its limitations include language limitations and the use of only public databases (Williamson, 2017).

Recommendations

It is recommended to improve the national digital infrastructure, especially focusing on the establishment of secure data centers, and thus increasing data sovereignty. Universities need to perform obligatory DPIAs and strengthen governance mechanisms in relation to cloud-based systems. Moreover, regular training in the sphere of digital ethics, cybersecurity, and privacy is essential for staff and students (UNESCO, 2021; Republic of Rwanda, 2021).

Author's Biography

Albert Rugaba is a high school teacher in Rwanda who specializes in teaching Geography and History subjects in high school. He holds a Bachelor's Degree in Geography and

History with Education, a Master's of Science degree in Educational Planning and Administration from Mount Kenya University, and a Post Graduate Diploma in Theology and Religion from East African Christian University. Currently, he is enrolled for his Doctor of Philosophy (PhD) in Educational Planning, Management, and Administration at Bishop Stuart University, Uganda. His areas of research include educational planning, management, and digitalization of education with a specific focus on governance and policy in a technology-enhanced learning environment.

Abbreviation Full Meaning

AU	African Union
DPIA	Data Protection Impact Assessment
HEC	Higher Education Council
HEIs	Higher Learning Institutions
ICT	Information and Communication Technology
LMS	Learning Management System
MINEDUC	Ministry of Education (Rwanda)
NCSA	National Cyber Security Authority
OECD	Organisation for Economic Co-operation and Development
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RISA	Rwanda Information Society Authority
SaaS	Software as a Service
TOE	Technology–Organization–Environment Framework
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific, and Cultural Organization

Registration, Protocol, and Competing Interests

The review was not registered in any systematic review registry. There was no protocol used in the process of research. There are no competing interests. Registration Number: J26/BSU/PHD-EPMA/0248

REFERENCES

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514. <https://doi.org/10.1126/science.aal465>
2. African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). African Union.
3. African Union. (2022). Data policy framework. African Union Commission.

4. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58. <https://doi.org/10.1145/1721654.1721672>
5. Coates, H., James, R., & Baldwin, G. (2005). A critical examination of the effects of learning management systems on university teaching and learning. *Tertiary Education and Management*, 11(1), 19-36. <https://doi.org/10.1080/13583883.2005.9967137>
6. Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, 21(10), 2305-2325. <https://doi.org/10.1177/1461444819865984>
7. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147- 160. <https://doi.org/10.2307/2095101>
8. Floridi, L. (2013). *The ethics of information*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199641321.001.0001>
<https://doi.org/10.1093/acprof:oso/9780199641321.003.0002>
9. Floridi, L. (2014). *The fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press.
10. Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A*, 374(2083), 20160360. <https://doi.org/10.1098/rsta.2016.0360>
11. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernández, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 5. <https://doi.org/10.1186/1869-0238-4-5>
12. Ifenthaler, D., & Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology Research and Development*, 64(5), 923-938. <https://doi.org/10.1007/s11423-016-9477-y>
13. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing (SP 800-145)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-145>
14. Mueller, M. (2017). *Will the internet fragment? Sovereignty, globalization, and cyberspace*. Polity Press.
15. Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press. <https://doi.org/10.1515/9780804772891>
16. North, D. C. (1990). *Institutions, institutional change, and economic performance*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511808678>
17. OECD. (2013). *The OECD privacy framework*. OECD Publishing.
18. OECD. (2019). *OECD principles on artificial intelligence*. OECD Publishing.
19. Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511807763>
20. Pardo, A., & Siemens, G. (2014). Ethical principles for learning analytics. *British Journal of Educational Technology*, 45(3), 438-450. <https://doi.org/10.1111/bjet.12152>
21. Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4), 1-19. <https://doi.org/10.14763/2020.4.1532>
22. Republic of Rwanda. (2021). Law No. 058/2021 of 15/10/2021 relating to the protection of personal data and privacy. Government of Rwanda.
23. Rhodes, R. A. W. (1996). *The new governance: Governing without government*. Political Studies, 44(4), 652-667. <https://doi.org/10.1111/j.1467-9248.1996.tb01747.x>
24. Sackey, E., & Bahl, M. (2020). Socio-technical system configurations for secure cloud computing in academic environments. *International Journal of Information Management*, 52, 102115.
25. Scott, W. R. (2014). *Institutions and organizations: Ideas, interests, and identities (4th ed.)*. SAGE Publications. <https://doi.org/10.3917/mana.172.0136>
26. Selwyn, N. (2016). *Education and technology: Key issues and debates*. Bloomsbury Academic. <https://doi.org/10.5040/9781474235952>
27. Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist*, 57(10), 1510-1529. <https://doi.org/10.1177/0002764213479366>
28. Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477-560. <https://doi.org/10.2307/40041279>
29. Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.
30. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11. <https://doi.org/10.1016/j.jnca.2010.07.006>
31. Sultan, N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management*, 30(2), 109-116. <https://doi.org/10.1016/j.ijinfomgt.2009.09.004>
32. UNCTAD. (2021). *Data protection and privacy legislation worldwide*. United Nations.
33. UNDP. (2022). *Digital strategy 2022-2025*. United Nations Development Programme.

35. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. UNESCO.
36. Westin, A. F. (1967). Privacy and freedom. Atheneum.
37. Williamson, B. (2017). Big data in education: The digital future of learning, policy and practice.

SAGE

Publications.

<https://doi.org/10.4135/9781529714920>

38. World Bank. (2021). World development report 2021: Data for better lives. World Bank.
39. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

Publisher Details:

SJC PUBLISHERS COMPANY LIMITED



Category: Non Government & Non profit Organisation

Contact: +256 775 434 261 (WhatsApp)

Email: info@sjpublisher.org or studentsjournal2020@gmail.com

Website: <https://sjpublisher.org>

Location: Scholar's Summit Nakigalala, P. O. Box 701432, Entebbe Uganda, East Africa