Received: 6 December 2021 | Accepted: 13 April 2022

DOI: 10.1111/bjet.13226

ORIGINAL ARTICLE

British Journal of Educational Technology BERA

Data privacy on the African continent: Opportunities, challenges and implications for learning analytics

Paul Prinsloo[1] | **Rogers Kaliisa**[2]

[1]Department of Business Management, University of South Africa (Unisa), Pretoria, South Africa

[2]Department of Education, Faculty of Educational Sciences, University of Oslo, Oslo, Norway

Correspondence
Paul Prinsloo, Department of Business Management, University of South Africa (Unisa), Pretoria, South Africa.
Email: prinsp@unisa.ac.za

Funding information
None

Abstract

Whilst learning analytics is still nascent in most African higher education institutions, many African higher education institutions use learning platforms and analytic services from providers *outside* of the African continent. A critical consideration of the protection of data privacy on the African continent and its implications for learning analytics in African higher education is therefore needed. In this paper, we map the current state of legal and regulatory environments and frameworks on privacy to establish their implications for learning analytics. This scoping review of privacy regulations in 32 African countries, complemented by 15 scholarly papers, revealed that there are numerous national and regional legislation and regulatory frameworks, providing clear pointers pertaining to (student) data privacy to governments, higher education institutions and researchers. As such, the findings of this research have implications for African higher education to ensure not only legal compliance but also to oversee and safeguard student data privacy as part of their fiduciary duty. This research provides crucial insights regarding the importance of context for thinking about the expansion and institutional adoption of learning analytics.

KEYWORDS
Africa, data protection, higher education, learning analytics, legislation, privacy

Practitioner notes

What is already known about this topic
- Personal data have become commodified and are regarded as a valuable commercial asset.
- The commercial value of data relies on the collection and analysis of increasing volumes, granularity, variety and velocity of personal data (both identifiable and aggregated).
- Africa and African higher education are regarded as new data frontiers to be exploited.

What this paper adds
- This paper, for the first time, makes an attempt to map privacy legislation and academic research on (student) data privacy in the African continent.
- Maps key implications for African higher educations to consider in collecting, analysing, using and sharing student data.
- It provides pointers for a research agenda pertaining to student data privacy on the African continent.

Implications for practice and/or policy
- African higher education institutions should consider student data privacy when entering into service level agreements with educational technology and platform providers.
- African governments should develop common data sharing frameworks to facilitate cross-border data transfer.
- Current African data privacy legislation provides important implications for the adoption and institutionalisation of learning analytics.
- African higher education also has to consider the ethical aspects of learning analytics.

INTRODUCTION

Higher education is becoming increasingly digitised and datafied, and evidence suggests that as institutions responded to the disruption caused by COVID-19, the digitisation and datafication of teaching and learning has intensified (García-Morales et al., 2021; Williamson et al., 2020; Williamson & Hogan, 2020). Though there is uncertainty to the extent to which African higher education is digitised and datafied (Prinsloo & Rogers, in press), evidence shows to what extent the pandemic has increased the digitisation and datafication of teaching, learning and the various administrative processes supporting them (Egielewa et al., 2021; Tamrat & Teferra, 2020; Van Schalkwyk, 2021). Irrespective of the context, increased digitisation and datafication also resulted in various stakeholders raising concerns about *student data privacy* (Khalil et al., 2022; Prinsloo et al., 2021).

Since its emergence as a research focus and practice in 2011, learning analytics (LA) has matured with many institutions in the Global North institutionalising LA (Axelsen et al., 2020). Whilst scholarship and the institutionalisation of LA continue to expand and deepen (Prinsloo

& Kaliisa, in press), the absence of case studies and research in LA—and student data privacy, in particular—on the African continent is noteworthy. Recent research by Kaliisa et al. (2022) point to several challenges in the adoption of LA and many of the challenges such as, difficulties integrating technical and pedagogical expertise in LA' use; (2) lack of connection between LA and educational theories or pedagogies; (3) failure to align LA with teachers' practice; and (4) *ethical and privacy concerns*. As student data privacy is central to published concerns pertaining to the implementation of LA, this paper proceeds from the assumption that the protection of student data privacy on the African continent warrants research. Student data privacy is furthermore central to concerns arising from the increasing influence of online program management (OPM) providers and the commodification and assetisation of education provision (Komljenovic, 2020; Williamson, 2021). African HEIs are particularly vulnerable to exploitation as a result of these trends, necessitating an enquiry regarding to student data privacy protection on the African continent (Prinsloo & Kaliisa, in press; Prinsloo, 2018, 2020).

The digitalisation and datafication of African HEIs are in many respects, inevitable (Mugimu, 2021; Prinsloo, 2020). Africa will also not escape the impact of the Fourth Industrial Revolution (4IR) (Ayentimi & Burgess, 2019; Naude, 2017), and, as Africa is the world's most populous continent (World Population Review, n.d.), with estimations that its population will double by 2050 (The Economist, 2020), and with 19 out of the world's 20 youngest countries (Myers, 2019) being on the African continent, Africa is seen as *terra nullis*, a new data frontier to conquer (Prinsloo, 2020). In the light of the foreseen massification of higher education and the need to provide educational opportunities at scale (eg, Lebeau & Oanda, 2020), African HEIs will have to consider the implications of agreements with OPM providers, many of whom will be located in the Global North. Amid the broader concerns of the implications of the commodification and subsequent assetisation of higher education (Birch, 2020; Komljenovic, 2020; Williamson, 2021), concerns about Africa being re-colonised and its data exported and capitalised may be legitimate (Prinsloo, 2020).

There are 54 sovereign states on the African continent and there is no, as far as can be established, a central database on existing legislation covering the whole continent, or publicly available resources (per country or region) for education institutions, educators and students providing guidance and resources to support the protection of student data privacy. Recent research by Abdulrauf (2021) found that only “about” (p. 96) 23 African states have data privacy legislation in place. Through this scoping review, this paper draws on the available information (internet sources and scholarly, peer-reviewed literature) pertaining to data protection regulations on the African continent to provide an answer to the following question: *What is known about the protection of personal data on the African continent?* Based on the findings, we identify examples and highlight some of the opportunities and challenges that higher education institutions and researchers seeking to protect student data privacy when institutionalising learning analytics could face. We conclude this paper with a set of possible practices that higher education institutions, governments and individual researchers may consider to protect student data privacy in the context of LA.

SOME BRIEF NOTES ON THE CONTEXT

As student data privacy on the African continent is closely linked to the digitisation of higher education, it is important to provide a brief overview of what we currently know about the state of digitisation and datafication on the African continent, before contextualising student data privacy in LA in international HEIs in the context of current national and international privacy legislation and regulatory frameworks.

THE CURRENT STATE OF DIGITALISATION AND DATAFICATION OF AFRICAN HEIS

The number of individuals on the African continent using the internet has increased from 81 million in 2010, to 294 million in 2019 (State of Broadband Report, 2020). There has been a 12.98% growth in internet use from 2000–2021, and currently 43% of Africa's population has access to the internet (Statista, 2022). By 2030, the growth in internet access will see 75% of Africa's population having access (Allen, 2021), and Forbes forecasts that "Africa is the next frontier for the internet" (Tuerk, 2020). Despite increasing access to the internet, Ischebeck (2020, referring to findings from the U.N Broadband Commission) reports that several countries in Sub-Saharan, such as, but not limited to, Somalia, Nigeria and South Sudan, have an internet penetration of less than 2%.

The impacts of the relative low levels of access to the internet, as well as vast differences between African countries, on the digitisation of higher education have not yet been researched. There is, however, evidence that points to the relationship between the digitalisation of education to "huge levels of local and foreign investment, as well as above-average internet access and connectivity" (Ischebeck, 2020). In research on educators' knowledge and interest to use an institutional LMS in six Sub-Saharan countries—Ghana, Nigeria, Tanzania, Uganda, Zimbabwe and South Africa—Bervell and Umar (2017) report that most African educators have little knowledge and interest in the use of LMSs. Moodle is, by far, not only the most popular LMS on the African continent (with 78% market share) but also the fastest growing LMS (having had 53% market share in 2008, to its current 78% plus market share) (Phil Hill, personal communication, 2021). In a report by Business Market Insights (2020), the report states that the "education and LA market in Middle East and Africa (MEA) is expected to grow from US$ 307.3 million in 2019 to US$ 1490.0 million by 2027; it is estimated to grow at a compound annual growth (CAGR) rate of 22.4% from 2020 to 2027." There is evidence that points to a relationship between the digitalisation of education to "huge levels of local and foreign investment, as well as above-average internet access and connectivity" (Ischebeck, 2020).

Whilst everything points to the internet penetration to continue to increase, and that African HEIs will increasingly embrace the digitalisation of teaching and learning, the sharing, collection and commodification of (personal) data will also expand, with implications for personal data privacy (Abdulrauf, 2021), and specifically, LA. In the light of several incidents (eg, Facebook, Cambridge Analytica, refs), it is clear that "the lack of adequate regulations for the collection and processing of personal information can have significant ramifications" (Data Protection Africa—Trends, n.d.).

DATA PRIVACY AND LEGISLATION ON THE AFRICAN CONTINENT IN A BROADER CONTEXT: A BRIEF INTRODUCTION

Privacy is very difficult, if not impossible to define, "because it is exasperatingly vague and evanescent" (Solove, 2008, p. 1088 referring to Miller). Despite the difficulty to define privacy, context-dependent understandings of the notion of privacy are found in most, if not all cultures (eg, Newell, 1998; Vis, Dunbar & Jahnke, 2011). Dominant current legal understandings and definitions of privacy are informed by, inter alia, Roman-Dutch law and world-views and values from the Global North (Campbell, 2020). Research into different cultural understandings of privacy (eg, Krasnova et al., 2012; Neswell, 1998) often refer to the contrasts between cultures that value *individualism* versus the more *collectivist* cultures from the Global South. For example, in Africa group interests outweigh individual interests due to the culture of collectivism; hence claims for individual privacy are less common (Makulilo, 2016a, 2016b).

This has, however, been disproved by scholars (Abdulrauf, 2021), and the protection of data privacy is as important on the African continent, as elsewhere in the world.

It is also important to recognise that "Although data privacy is no longer new to Africa, compliance with data privacy norms has been significantly lower compared to other jurisdictions" (Abdulrauf, 2021, p. 87). Whilst international privacy legislation such as the GDPR has become a global standard of a particular understanding and protection of individual privacy, there are also views that the global acceptance of the GDPR as *normative* can be seen as imperialistic with a disregard for contextual understandings of privacy (Gstrein & Zwitter, 2021; Mannion, 2020), in particular from the Global South (Makulilo, 2016a, 2016b). Considering the lasting legacy of colonialism in the Global South, and in particular on the African continent, it should not come as a surprise that there are scholars and institutions in the Global South that are pushing back against the EU as 'normative power' (Berge, 2021) to the exclusion of local and regional understandings of, for example, privacy. Whilst the GDPR deals with the protection of personal information, its impact is wide-ranging. "Due to the strengthened third-party obligations in the GDPR for data export to non-European Union countries and fear of loss of foreign investment if such countries fail to provide adequate protection of personal data, the GDPR exerts profound influence on data privacy law reform and practice outside Europe" (Makulilo, 2021, p. 117).

We therefore need to understand privacy legislation on the African continent against the increasing importance of global e-Commerce, with the protection of data and trust foundational to the new economy. "Undoubtedly this has been the paramount motivation for the adoption of data privacy legislation in Africa" (Makulilo, 2015, p. 79).

There is also increasing evidence of "pervasive surveillance programmes and data mining activities" on the African continent with African governments requesting users' information from companies such as Google, Facebook and Twitter, "obviously in violation of data privacy norms (Abdulrauf, 2021, p. 88). The issue is not the absence of regulation, but the "quality of implementation and enforcement by law" (Abdulrauf, 2021, p. 88). Whilst several African states do have data privacy legislation, "the jurisprudence based on case law and the decisions/recommendation of DPAs [Data Protection Authorities] is highly underdeveloped" (Abdulrauf, 2021, p. 93). The African Union Data Protection Convention, envisaged to become a common standard for data privacy on the African continent, will only enter into force when 15 states of the African Union has ratified the convention, and at the time of the writing of this paper, this has not been achieved. There is furthermore no "binding regional-wide normative framework on data privacy" in place (Abdulrauf, 2021, p. 94). [See Abdulrauf (2021) and Makulilo (2015) for a discussion of the initiatives of various sub-regional bodies].

In the light of the increasing levels of digitisation and datafication on the African continent, and specifically in African higher education, we have to seriously consider the ever-increasing and ever-pervasive 'data gaze' (Beer, 2019), and its impact on student data privacy (Prinsloo, 2020). As African higher education becomes increasingly digitised and datafied, African higher education has to consider not only current national and extra-national data privacy legislation but also develop internal policies and regulatory frameworks to ensure not only compliance, but move towards the ethical collection, analysis and use of student data.

As a way to establish what is currently known about data privacy on the African continent, the next section provides details on our choice of following a scoping review methodology.

METHODOLOGY

The methodological framework of undertaking a scoping review by Munn et al. (2018) and used in previous scoping reviews (eg, Kaliisa et al., 2021) underpinned this review. Scoping reviews are guided by an a priori protocol; a systematic approach of searching for information;

clear and transparent processes resulting in reproducible research; designed and executed to increase reliability and reduce error and (using multiple reviewers); and extract and present data in a structured way (Munn et al., 2018, p. 5). To increase the rigour of this scoping review we used the checklist by Cooper et al. (2021) and implemented the PRISMA (PRISM-ScR) guidelines for scoping reviews (Tricco et al., 2018). The review followed five stages: (i) identifying the research questions (ii) identifying relevant studies; (iii) study selection; (iv) charting data; and (v) collating, summarizing and reporting results. These stages are further described below, highlighting how they were executed in this study.

Identifying the research questions

As it is the case with most scoping reviews, we came up with a general question, as the focus of the current study is to summarize the breadth of evidence regarding the legal frameworks on data protection, on the African continent and later discuss their implications for LA research. Thus, we formulated two research questions:

- How are the currently existing legal frameworks approaching personal data protection in Africa?
- What are the implications of the current state of legal frameworks/data protection policies towards protecting student (data) privacy in learning analytics?

Cooper et al. (2021), in their criteria for quality scoping reviews, indicated that the rationale for using a scoping review should be clear, more than one researcher needs to be involved and that the questions would guide the inquiry.

Identifying and selecting relevant studies

Cooper et al. (2021) state that the identification of relevant literature is a crucial second step following consensus on the guiding questions. We developed inclusion and exclusion criteria, search queries, performed literature searches and later screened analysed and summarised the findings. The primary source of data for this paper is from non-scholarly legal documents (eg, data regulatory policies and frameworks). 15 scholarly papers on data privacy on the African continent complemented this data. In this regard, the search process entailed two but simultaneous searches and selections. The search string used to find relevant papers and legal documents included variations and different combinations of the following search terms, which were applied through Boolean logic: “Africa” AND “privacy” AND “legal”; “data protection” AND “Africa” AND/OR “Education* higher education*”. For the purpose of this research two databases were identified namely Scopus and Web of Science. In addition, since some of the target sources of data (policy documents) are rarely published in scholarly journals and databases, we conducted general searches on Google to find relevant documents related to data legislations in different African countries. The searches were conducted to include relevant papers published up to and including the 30th of October 2021. In particular, the search for regulatory frameworks was limited to 1 January 2016 to 16 August 2021. The GDPR was adopted in 2016 and was assumed to indicate a major turning point for international privacy legislation. As this search included newspaper papers, law firms offering services, scholarly papers, the two researchers engaged with each entry on the first ten pages to look for databases regarding legislation for the protection of data privacy on the African continent. The six websites that formed part of the final web corpus are reported in Table 1 (below).

Of these six websites, Data Protection Africa (n.d.) provided the most comprehensive overview of privacy legislation of 32 African countries resulting in the researchers using this website as the basis of their analysis supplementing the findings with information found on the other web pages in the web corpus. It is important to note that there is conflicting information between Data Protection Africa (n.d.) and UNCTAD (n.d.) as illustrated in the fact that UNCTAD (n.d.) lists Senegal as not having legislation in place whilst Data Protection Africa (n.d.) indicates that Senegal not only has legislation but also enforces it. As it falls outside the scope of this paper to scrutinise evidence provided on legislation in all 54 African states, the researchers opted to use the database on Data Protection Africa (n.d.) as the information on the 32 selected African countries is updated regularly. (Also see Privacy International, 2017).

TABLE 1 List of websites used to retrieve data privacy regulatory frameworks

Website name and address	Description
Data Protection Africa https://dataprotection.africa	"Data Protection Africa is an online open-access portal that provides information on data protection laws and access to data protection authorities in 32 African countries. Data Protection Africa is an ALT Advisory special project"
Research ICT Africa https://researchictafrica.net	"Research ICT Africa (RIA) is an African think tank that has operated for over a decade to fill a strategic gap in the development of a sustainable information society and digital economy. It has done so by building the multidisciplinary research capacity needed to inform evidence-based policy and effective regulation Africa. RIA's dynamic and evolving research agenda examines the uneven distribution of the benefits and harms of the intensifying global processes of digitalisation and datafication"
Africa ICT Policy Database https://www.ictpolicy.org	"The Africa ICT Policy Database (AIPD) is designed as an open and free resource for information technology across Africa especially on policies and laws. It is a project of The Centre for Intellectual Property and Information Technology Law (CIPIT) based at The Strathmore Law School in Nairobi, Kenya. CIPIT's mission is to study, create, and share knowledge on the development of intellectual property and information technology, especially as they contribute to African Law and Human Rights. From our experience working on ICT policies across countries and regions in Africa, we have encountered two main challenges on Information technology policy making processes; scare official policy documents and limited opportunities for governments to involve the public(s) in making new ones"
Privacy International https://privacyinternational.org/	"Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why PI is here: To protect democracy, defend people's dignity, and demand accountability from institutions who breach public trust"
iapp—Privacy Perspective https://iapp.org/news/privacy-perspectives/	"The IAPP is the largest and most comprehensive global information privacy community and resource. Founded in 2000, the IAPP is a not-for-profit organization that helps define, promote and improve the privacy profession globally"
United Nations Conference on Trade and Development (UNCTAD) https://unctad.org/page/data-protection-and-privacy-legislation-worldwide	"The UNCTAD Global Cyberlaw Tracker is the first ever global mapping of cyberlaws. It tracks the state of e-commerce legislation in the field of e-transactions, consumer protection, data protection/privacy and cybercrime adoption in the 194 UNCTAD member states. It indicates whether or not a given country has adopted legislation, or has a draft law pending adoption. In some instances where information about a country's legislation adoption was not readily available, 'no data' is indicated"

The screening was based on titles, abstracts and full-text skimming, and began on 10th August until 30 October 2021. It is important to note that this process was iterative, with frequent discussions between the two researchers to avoid potential ambiguity with a broad research question and to ensure that abstracts selected are relevant for full paper review. Following these procedures, the final dataset included data from 32 African countries. In addition, 15 empirical studies (see Appendix A) focussing on issues of data privacy in Africa were analysed and used to complement the main findings (eg, data regulation frameworks), based on the following inclusion criteria:

- The study reports on the legal understanding of and/or the protection of personal data and/or privacy issues in the context of Africa.
- The study is published in a peer-reviewed journal or conference proceedings or published by an official government department.
- Study or report is published in English and available for public use.

Charting the data

Following Cooper et al. (2021) guidelines, a data-charting manual was jointly developed by the two researchers to determine, which variables to extract from the identified studies. The two researchers used sifting and sorting of data as well as Excel spreadsheets including abstracts, comments from the full text and an analysis of the identified variables. Guided by the research questions, the coding for the privacy legislations included the following variables: fast facts; (2) Data privacy legislation; (3) personal data; (4) collection and processing; (5) cross-border transfer; and (6) security and breach protocol. Moreover, the coding for scholarly papers included the following variables: Authors; the title of research; country, outline of the data protection framework/privacy/ ethical framework; and the context of application (eg, higher education and business). The coding was performed through several stages. Initially, two coders took a grounded approach and reviewed 2 studies for training purposes and to gain familiarity with the literature. In this case, initial codes were formed based on the descriptions and contextual information provided in the papers and of relevance to the research questions. Next, each of the coders independently coded a further 4 papers and then discussed coding challenges to refine the coding scheme. We used social moderation where two researchers coded all the papers and then discussed all the areas where ratings differed until an agreement was reached. Finally, the coders split the papers and proceeded with coding the full sample following the revised codes.

The coding scheme included noting the authors and title of the paper, the country on which it reports, the field of application (eg, general, education, ethics, teaching and learning, general privacy and 'technical' privacy such as cyber security) and data privacy.

Collating, summarizing and reporting results

This stage involved a summary and analysis of results coded at the charting stage. First, we came up with a descriptive numerical summary of the results, which highlights the key characteristics of the included studies (eg, country background and nature of legislation). Since the scholarly, peer-reviewed dataset and the privacy regulations corpus was relatively small, this stage was completed manually without assistance from any software. We undertook a narrative analysis of the identified studies using privacy regulations from each country and individual scholarly papers as the unit of analysis. Cooper et al. (2021) suggest that the results should be presented in a descriptive or diagrammatic format,

that issues of bias would be discussed, and that implications for future research be put forward.

ANALYSIS AND FINDINGS

The research question informing this scoping review was as follows: *How are the current existing legal frameworks approaching personal data protection in Africa?*

The analysis and findings are structured as follows:

First, the analysis and findings from the web corpus are presented using the structure of data on Data Protection Africa (Data Protection Africa, n.d.), namely, (1) fast facts; (2) Data privacy legislation; (3) personal data; (4) collection and processing; (5) cross-border transfer; and (6) security and breach protocol. This layer of analysis is then supplemented with insights from the other websites in the web corpus as well as findings from the 15 scholarly, peer-reviewed corpus.

General overview: Fast facts

Data Protection Africa (n.d.) does not claim to provide a comprehensive overview of all African countries' legislation on data protection. UNCTAD (n.d.) does, however, provides a broad overview of all legislation on the African continent, *but with no detailed analysis*. According to UNCTAD (n.d.), of the 54 African countries, 28 states (52%) have legislation in place, 9 countries (17%) have draft legislation, and 13 countries (24%) have no legislation in place. The countries with no legislation in place are Libya, Egypt, Sudan, Ethiopia, Central African Republic, Cameroon, Liberia, Sierra Leone, Guinea Bissau, Burundi, Djibouti, Eritrea, and Senegal.

Of the 32 African countries on Data Protection Africa's database (Data Protection Africa, n.d.) (representing 60% of the 54 sovereign states), six countries do not currently have any legislation for the protection of data, four countries have legislation in place but there is no data on the legislation being enforced, eight countries have legislation but do not enforce the legislation and 13 (40%) of the African countries on this database have legislation in place as well as evidence that the legislation is enforced (see Table 2 below). The findings in this paper align with what Makulilo (2015) found in his analysis of African privacy laws and initiatives. The author found that existing policies are vague and coupled with a lack of national enforcement bodies.

Data privacy legislation

Mauritius was amongst the first countries to table legislation pertaining to data privacy and was the first African country to establish the Office of the Data Protection Commissioner and make it operational. As of January 2018, Mauritius regulates data protection under the Data Protection Act 2017 (Government of Mauritius, 2017), which repealed and replaced the former act, so as to align with the European Union General Data Protection Regulation 2016/679 (GDPR). In 2007, Burkina Faso became the first French-speaking country in sub-Saharan Africa with an operative data protection authority.

Of all the countries represented in this database, the Angolan law is the only African country that specifically mentions the cultural realities in the Angolan context (but does not provide more details pertaining to what exactly is referred to). Compared with the number of African countries that, in their legislation, specifically mention compliance with European

TABLE 2 An overview of privacy legislation of 32 African states

No legislation	Legislation but no data on enforcement	Legislation but not enforced	Legislation and enforced
Mozambique (privacy protected by the Constitution) Namibia (privacy protected by the Constitution, data protection law in process), Burundi, Ethiopia Tanzania, Egypt (currently under review by Parliament)	Malawi (partial legislation), Kenya, Togolese Republic, Rwanda (partial legislation)	Angola, Botswana, Lesotho, Madagascar, Zimbabwe, Niger, Seychelles, Uganda South Africa (The final sections of POPIA came into force on 1 July 2020, giving Responsible Parties one year within which to comply)	Mauritius, Zambia (partial enforcement), Gabon, Benin Burkino Faso, Cape Verde, Côte D'Ivoire (Ivory Coast), Ghana, Mali, Nigeria Senegal, Morocco Tunisia
Total: 6	**Total: 4**	**Total: 8**	**Total: 13**

standards (GDPR) (eg, but not limited to Lesotho, Madagascar and Mauritius), there is very little evidence of how African countries account for the specifics whether in culture, religion and/or context of the African continent. There is, however evidence of attempts to ensure regional compliance, eg, the South African Development Community (SADC) data protection standards (in the case of Lesotho), and Madagascar mentioning advice from other Francophone countries belonging to the *Association francophone des autorites de protection des donnes personnelles* (AFAPDP). The implications for student data privacy include, but are not limited to the vulnerability of African higher education institutions to fall prey to commercial expansion in the provision OPM providers (Komljenovic, 2020; Williamson, 2021) with very little regard for student data privacy and not protection provided to institutions and students.

PERSONAL DATA

Of the 32 countries in the Data Protection Africa (n.d.) database, 27 countries define 'personal information of which 14 countries distinguish between personal data and sensitive personal data, 6 of these countries have a category called 'special categories of personal data' (eg, Mauritius), or define it as 'special personal information' (South Africa) or just refer to specific categories of data, eg, 'racial or genetic origins' (eg, Tunisia), 4 countries don't define personal data, and 1 country does not define personal data but defines sensitive data (Togolese Republic).

Of interest is the case of Mozambique, which does not explicitly define 'personal data' but lists a number of data such as a person's political, philosophical or ideological beliefs, religious beliefs, political affiliation, trade union membership and particulars related to the person's privacy.

The collection and processing of personal data

Consent *prior* to the collection of personal data is specifically mentioned (eg, Angola, Lesotho, Zambia, South Africa) but Mauritius is the only African country acknowledging the right to withdraw consent at any time. South African legislation has 'openness' (implying

notification of collection) as principle—"The responsible party must keep documentation of all processing operations and notify the data subject when collecting personal information, barring certain exceptions" (Data Protection Africa, n.d.). General principles informing the collection and processing of personal data include transparency, legality, good faith, proportionality, truthfulness, respect to private life and legal and constitutional guarantees (eg, Angola). The principle of minimality is found in the case of Lesotho, Madagascar South Africa—referring to the processing of personal data that is required to be adequate, relevant and not excessive.

Considering the increasing influence of Artificial Intelligence (AI) in LA, it is important to note the prohibition of *automated data collection* and processing except under specific conditions provided in the respective legislation in the case of Gabon, Benin, Burkino Faso, Cape Verde, Cote d'Ivoire, Ghana, Niger, Senegal, Togolese Republic, Morocco, Lesotho and Mauritius.

The right to have access to collected data, to rectify personal data, to restrict or erase personal data or to register an objection regarding the processing of personal data is only found in the legislation of Mauritius.

Taking into account the nature of big data and collecting personal data from a range of sources and modalities, it is interesting to note that a number of African countries such as Niger, Benin, Gabon, Cape Verde, Cote D'Ivoire and Senegal specifically mention regulations pertaining to the "interconnection of personal data" (Data Protection Africa, n.d.). For example, legislation in Nigeria stipulates that the interconnection of personal data shall.

- not discriminate against or limit the fundamental rights, freedoms, and guarantees of data holders;
- ensure the use of appropriate safety measures; and
- take into account the principle of relevance.

From the above, it is clear that consent plays an important role, and this has implications for learning analytics, and educational technology in general. Though the collection, analysis and use of student data (eg, personal, demographic and behavioural) may fall under the social contract between higher education providers and students, consent cannot be assumed as learning analytics increasingly expands into collecting also multimodal data, using AI and interconnecting personal data.

Cross-border transfer of personal data

The majority of African countries allow the cross-border transfer of data. The cross-border transfer is allowed between countries with similar, or adequate levels of protection eg, legislation in Angola stipulates "Cross-border personal data transfers to countries without an adequate level of protection must be authorised" (Data Protection Africa, n.d.). A number of African states, however, have no regulation in place for the cross-border transfer of data such as Namibia, Burundi, Rwanda, Malawi, Seychelles and Tanzania.

Considering the reality that many Massive Open Online Course providers are offered from contexts other than the states from which students register, regulation pertaining to the cross-border transfer of data is crucial, not only for students but also for institutions who offer courses on such programmes and/or encourage students to supplement their curricula with a selection of MOOCs (Khalil et al., 2018a, 2018b).

It is clear that it is crucial that African states and regional networks need to improve regulations to protect and regulate the cross-border transfer of data. Failure to adopt such a

comprehensive legal framework can jeopardise trans-border data flows amongst regions (Taylor, 2020).

Security and breach control

Of the 32 African countries, 10 countries do not have any requirements for the notification of security and breaches (Namibia, Zambia, Gabon, Burkino Faso, Cape Verde, Mali, Niger, Malawi, Seychelles and Tunisia). Software-as-service and cloud computing raises several issues pertaining to personal (student) data privacy (Krueger & Moore, 2015; Luna, 2021; Varella, 2016). It is also interesting to note that even though countries such as Zimbabwe have extensive constitutional provisions for the protection of privacy, they lack a comprehensive data protection statute (Ncube, 2016). The same applies to Nigeria, which is reported as lagging behind in terms of protecting personal data with no serious form of control to check against abuse (Abdulrauf & Fombad, 2017). Constitutional provisions determine the formal structure of the state, defining the powers and jurisdictions of its various structures. This implies that in the cases of Zimbabwe and Nigeria, the constitutions provide for the protection of personal privacy as the responsibility of specific structures, but there is no coherent statute or legislation in place.

Sharing data with third parties

Sharing of personal data with third parties as prohibited is mentioned in 14 of the 32 countries—(Ghana, Lesotho, Cape Verde, Gabon, Zimbabwe, South Africa, Zambia, Niger, Rwanda, Angola, Rwanda, Madagascar, Nigeria and Benin). For example, Zambian legislation states "not disclose any personal information held by the data controller to a third party unless required or permitted by law or specifically authorized in writing by the data subject" (Data Protection Africa, n.d.).

DISCUSSION

In this section, we respond to the second research question, which seeks to draw implications from the current state of legal frameworks and data protection policies towards protecting student (data) privacy in learning analytics. The implications are discussed in the context of three actors (1) higher education institutions, (2) national governments and (3) researchers. This section is complimented by findings from the scholarly papers.

Implications for higher education institutions

It goes without noting that higher education institutions, irrespective of context or geopolitical location, have to adhere to national, regional and international conventions and regulations pertaining to the protection of personal (student) data. Even where there is no applicable national or regional regulatory frameworks in place, states should still be cognisant of, for example, Principles on Personal Data Protection and Privacy (UN System Chief Executives Board for Coordination (n.d.) (see Privacy International, 2017). To what extent these are enforceable by affected individuals is still to be proven. In addition to compliance to legislation and regulatory frameworks, higher education also has a fiduciary and moral duty of care to ensure student data privacy (Prinsloo & Slade, 2016, 2017).

Need for clear privacy and regulation frameworks

Given that existing national regulations are implicit about the use of student data, it is upon higher education institutions to devise strategies that support the use of students' data for research purposes. One possible approach is to seek consent at the time of registration and provide clear, easy-opt-in, and opt-out options for the students to consider. In particular, given the unequal power relationship between students and HE authorities (Slade & Prinsloo, 2013), there must be a level of privacy that (i) the data subject should be able to expect and (ii) which the data recipient publicly assures (Singh & Ramutsheli, 2016). The need for regulatory frameworks is further critical, given the increasing use of technologies (eg, learning management systems), which are mostly from technology companies in the Global North (Prinsloo, 2018, 2020). We propose that once clear regulatory frameworks are in place, the developers of LA technologies and tools will use them as a guide to develop tools that are sensitive and compliant to the needs of the different countries. In other words, since LA is tied to the use of technology, privacy concerns connected to LA should not only be perceived from a purely legal perspective but also from a technological point of view (eg, through the design process) (Steiner et al., 2016), and as a *social* phenomenon (Prinsloo, Slade & Khalil, under submission). Meanwhile, since companies cannot develop tools for only one specific country, it underscores the need for a unified data regulation framework on the African continent similar to the GDPR regulations in the European Union as proposed by the African Union's Data Protection Convention.

IMPLICATIONS FOR GOVERNMENTS

Develop common data sharing frameworks/agreements

The findings revealed that some African countries (eg, Ghana, Lesotho, Cape Verde, Gabon, Zimbabwe, South Africa, Zambia, Niger, Rwanda, Angola, Rwanda, Madagascar, Nigeria and Benin) prohibit the cross-border transfer of data. Whilst this could be a good move to ensure privacy, it is also a challenge for research collaboration, particularly in interdisciplinary fields such as LA. It is important that African governments and specifically data regulation bodies develop data privacy regulations that are friendly to international jurisdictions such as the European Union, Americas and Asia to facilitate data exchanges. Borena et al. (2015) advanced the same view and noted that privacy regulations cannot be advanced through isolated isolations but instead through regional and comprehensive regulatory schemes. This could especially be important for the LA field that relies on collecting data from learning management systems, with vendors mainly from the Global North.

Moreover, as also observed by Daigle (2021), in some cases, technology companies could withdraw business or change their business practices from regions where they face regulatory challenges that could resultant big economic losses. All this could affect the institutionalisation of LA on the African continent. African higher education institutions may be particularly vulnerable in the light of the fact that only 23 African states have privacy legislation in place, and concerns about enforcing legislation (Abdulrauf, 2021). Thus, whilst we recognise the possible challenges of a unified privacy framework given the differences in culture and economic backgrounds, it is crucial to come up with data protection models and authorities (Sutherland, 2018), which offer high protection for African data subjects without simultaneously creating rights that could be difficult to implement and scare away technology companies that could offer technologies to support learning analytics. There is a need for pan-African data protection and privacy regulatory framework so that companies providing educational technologies do not have to navigate regulations across different countries

(Daigle, 2021) (Also, see the concerns raised by Abdulrauf, 2021 regarding the role of the African Union in this regard). However, African countries should pay attention to the social, cultural and economic differences *within* the African context, since privacy as a relational and social concept should also be understood within the social and cultural context of a particular region (Dagbanja, 2016). Africa, and personal data protection on the African continent, cannot be isolated from broader, international developments in personal data protection, as found in, for example, the GDPR. The world is connected and whilst there are disparities in levels and quality of connections, everyone is affected (Castells, 2013). As Africa, and African higher education is increasingly connected, it is crucial that the interests of African students in terms of their data privacy are respected and protected.

IMPLICATIONS FOR STUDENT DATA PRIVACY AND LEARNING ANALYTICS

Need for empirical studies on data privacy in education

In this paper, overall, we found only 10 empirical studies (eg, Abebe et al., 2021; Daigle et al., 2021) focussing on privacy regulations on the African continent, yet five of them were conducted in South Africa. This finding aligns with a recent review by Hakimi et al. (2021) focussing on the ethics of using digital trace data in learning and education. The study reported that most studies were conceptual and mainly conducted in specific geographic areas (notably the United States, the United Kingdom, and Australia) with only four studies in Africa, yet they were all from South Africa. With this trend, we propose that it is hard to come up with policies to regulate data privacy and specifically for educational research and LA, in particular, if not based on empirical evidence. In this regard, it is critical that LA researchers and practitioners move towards research aimed at engaging HE stakeholders to develop ethical frameworks, resembling efforts in other regions such as the SHEILA framework. In particular, evidence for developing regulatory frameworks should be based on views from African experts since as Abebe et al. (2021) noted, conversations around Africa data and privacy are often dominated by non-African stakeholders.

Developing in-house LA tools

Given the current nature of personal data protection regulations, African LA researchers and practitioners, with support from higher educational institutions should develop LA systems that do not require reliance on external vendors. For example, Makerere University in Uganda has a local learning management system called' Makerere University E-learning Learning system. In such cases, it is possible for researchers to follow the local data privacy regulations as guided by ethical research committees without threatening student privacy.

Seek consent

In situations where policies about personal data sharing and analysis are not clear, we suggest that LA researchers and practitioners to follow the traditional norms of seeking for consent to avoid any breach of privacy regulations. Besides, LA researchers and practitioners should pay close attention to other privacy regulations in jurisdictions outside Africa (eg, GDPR), to ensure that whilst working through partnerships, all the necessary requirements are followed.

LIMITATIONS

This paper is based on evidence from websites that present information about the existing data regulations. However, we recognise the possibility of having missed some regulations, which are not yet published on the websites. In addition, the search was conducted to include studies and regulations published and available in English. However, since English is not as an official language in some African universities, it is possible that some important sources on student data privacy could have been missed. Moreover, this being a scoping review, we did not aim to include all available studies but only a sample of studies that we found relevant to answer the study's research questions. Meanwhile, despite these limitations, this study paper presents evidence from 32 countries that provide a strong basis to understand the current state of privacy legislation and their potential impact for LA research and practice. This work provides a great platform for LA researchers and practitioners who wish to advance their own research agenda on privacy in Africa.

CONCLUSION

This paper reports a scoping review of the current state of the art of legal and regulatory frameworks on privacy regulations on the African continent, where data from 32 African countries were the subject of analysis. We also complemented our analysis with 15 scholarly papers. The purpose of the review is to draw implications for the future of LA research and practice on the African continent. This paper has revealed a growing trend by African jurisdictions to adopt comprehensive data protection legislation even though few of these have been adopted into law. In particular, we identified differences between countries when it comes to policies such as cross-border data transfers. The paper also revealed that existing regulations are implicit about personal data particularly, with existing regulations and debates mainly centred on data protection in health, business and e-government services.

Based on the current privacy regulations, and some evidence from academic literature, this paper highlights implications for LA research and practice. In particular, we emphasise that as African higher education is increasingly becoming digitised and datafied, the expansion of the institutionalisation of LA in the Global South and other underserved regions particularly the African continent, necessitate understanding national and regional data and privacy regulations, and formulating context-appropriate policies and frameworks to protect student privacy. In particular, we have emphasised the need to harmonise data sharing regulations within Africa and make sure that regional and institutional regulations are developed to oversee and safeguard student data privacy as part of their fiduciary duty. As there is evidence that African higher education institutions are seen as a new data frontier, with commercial interests informing learning platform providers intending to capture the African market, this paper provides crucial insights regarding the importance of protecting (African) student data privacy on regional, national and institutional levels.

ACKNOWLEDGEMENTS

We express our appreciation for the reviewers for their helpful critique, comments and suggestions.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

ETHICS STATEMENT

As scoping review, no institutional ethical clearance process was required. In general, the authors acknowledge and adhered to the BERA Ethical Guidelines for educational research (fourth edition, 1998).

DATA AVAILABILITY STATEMENT

The document and data used in this paper are either publicly available on the internet or accessible through scholarly databases.

ORCID

Paul Prinsloo https://orcid.org/0000-0002-1838-540X

REFERENCES

Abdulrauf, L. A. (2021). Giving 'teeth' to the African Union towards advancing compliance with data privacy norms. *Information & Communications Technology Law*, *30*(2), 87–107. https://doi.org/10.1080/13600834.2021.1849953

Abdulrauf, L. A., & Fombad, C. M. (2016). The African Union's data protection Convention 2014: A possible cause for celebration of human rights in Africa? *Journal of Media Law*, *8*(1), 67–97. https://doi.org/10.1080/17577632.2016.1183283

Abdulrauf, L. A., & Fombad, C. M. (2017). Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms. *Liverpool Law Review*, *38*(2), 105–134. https://doi.org/10.1007/s10991-016-9189-8

Abebe, R., Aruleba, K., Birhane, A., Kingsley, S., Obaido, G., Remy, S. L., & Sadagopan, S. (2021, March). Narratives and counter narratives on data sharing in Africa. In M. C. Elish, W. Isaac, & R. Zemel (Eds.), *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 329–341). The Association for Computing Machinery.

Agbozo, E., Alhassan, D., & Spassov, K. (2018, November). Personal data and privacy barriers to e-Government adoption, implementation and development in Sub-Saharan Africa. In *International Conference on Electronic Governance and Open Society: Challenges in Eurasia* (pp. 82–91). Springer, Cham.

Allen, N. (2021, March 11). *The promise and perils of Africa's digital revolution*. Brookings TechStream. https://www.brookings.edu/techstream/the-promises-and-perils-of-africas-digital-revolution/

Alunge, R. (2019, May). The effect of Africa's adoption of the EU notion of personal data: The case of examination results. In *2019 IST-Africa Week Conference (IST-Africa)* (pp. 1–13). IEEE.

Axelsen, M., Redmond, P., Heinrich, E., & Henderson, M. (2020). The evolving field of learning analytics research in higher education. *Australasian Journal of Educational Technology*, *36*(2), 1–7. https://doi.org/10.14742/ajet.6266

Ayentimi, D. T., & Burgess, J. (2019). Is the fourth industrial revolution relevant to sub-Sahara Africa? *Technology Analysis & Strategic Management*, *31*(6), 641–652. https://doi.org/10.1080/09537325.2018.1542129

Beer, D. (2019). *The data gaze*. Sage.

Bervell, B., & Umar, I. N. (2017). A decade of LMS acceptance and adoption research in Sub-Sahara African higher education: A systematic review of models, methodologies, milestones and main challenges. *EURASIA Journal of Mathematics, Science and Technology Education*, *13*(11), 7269–7286. https://doi.org/10.12973/ejmste/79444

Berge, M. V. (2021). *The EU as a Normative Power in the field of artificial intelligence?: Challenges and concepts in the governance and regulation of digital technologies using the example of the EU and its human-centred approach to AI* (Master's thesis). University of Twente.

Birch, K. (2020). Technoscience rent: Toward a theory of rentiership for technoscientific capitalism. *Science, Technology, & Human Values*, *45*(1), 3–33.

Borena, B., Belanger, F., & Egigu, D. (2015, January). Information privacy protection practices in Africa: A review through the lens of critical social theory. In *2015 48th Hawaii International Conference on System Sciences* (pp. 3490–3497). IEEE.

Business Market Insights. (2020). *Middle East and Africa education and learning analytics market forecast to 2027*. https://www.businessmarketinsights.com/reports/middle-east-and-africa-education-and-learning-analytics-market

Campbell, J. (2020). The origins and development of the right to privacy. In A. Koltay & P. Wragg (Eds.), *Comparative privacy and defamation* (pp. 9–23). Edward Elgar Publishing.

Castells, M. (2013). *Communication power*. Oxford University Press.

Cooper, S., Cant, R., Kelly, M., Levett-Jones, T., McKenna, L., Seaton, P., & Bogossian, F. (2021). An evidence-based checklist for improving scoping review quality. *Clinical Nursing Research*, *30*(3), 230–240. https://doi.org/10.1177/1054773819846024

Dagbanja, D. N. (2016). The right to privacy and data protection in Ghana. In A. B. Makulilo (Ed.), *African data privacy laws* (pp. 229–248). Springer.

Daigle, B. (2021). Data protection laws in Africa: Pan-African survey and noted trends. *Journal of International Commerce & Economics*, 1–27. https://heinonline.org/HOL/P?h=hein.journals/jice2021&i=1

Data Protection Africa. (n.d). *Trends*. https://dataprotection.africa/trends/

Egielewa, P., Idogho, P. O., Iyalomhe, F. O., & Cirella, G. T. (2021). COVID-19 and digitized education: Analysis of online learning in Nigerian higher education. *E-Learning and Digital Media*, *19*, 20427530211022808.

García-Morales, V. J., Garrido-Moreno, A., & Martín-Rojas, R. (2021). The transformation of higher education after the COVID disruption: Emerging challenges in an online learning scenario. *Frontiers in Psychology*, *12*, 196. https://doi.org/10.3389/fpsyg.2021.616059

Government of Mauritius. (2017). *Data protection act*. https://dataprotection.govmu.org/Pages/The%20Law/Data-Protection-Act-2017.aspx

Gstrein, O. J., & Zwitter, A. J. (2021). Extraterritorial application of the GDPR: Promoting European values or power? *Internet Policy Review*, *10*(3), 1–30. https://doi.org/10.14763/2021.3.1576

Hakimi, L., Eynon, R., & Murphy, V. A. (2021). The ethics of using digital trace data in education: A thematic review of the research landscape. *Review of Educational Research*, *91*(5), 00346543211020116. https://doi.org/10.3102/00346543211020116

iapp. (n.d.) *Privacy perspective*. https://iapp.org/news/privacy-perspectives/

Ischebeck, J. (2020). *5 reasons for potential eLearning failure in Africa*. eLearning Industry. https://elearningindustry.com/reasons-for-potential-elearning-failure-in-sub-sahran-africa

Kaliisa, R., Kluge, A., & Mørch, A. I. (2021). Overcoming challenges to the adoption of learning analytics at the practitioner level: A critical analysis of 18 learning analytics frameworks. *Scandinavian Journal of Educational Research*, *66*(3), 367–381. https://doi.org/10.1080/00313831.2020.1869082

Khalil, M., Prinsloo, P., & Slade, S. (2018a). User consent in MOOCs–micro, meso, and macro perspectives. *International Review of Research in Open and Distributed Learning*, *19*(5). https://doi.org/10.19173/irrodl.v19i5.3908

Khalil, M., Prinsloo, P., & Slade, S. (2018b). The unbearable lightness of consent: Mapping MOOC providers' response to consent. In R. Luckin, S. Klewmmer, & K. Koedinger (Eds.), *Proceedings of the fifth annual ACM conference on learning at scale* (pp. 1–11). Association for Computing Machinery.

Khalil, M., Prinsloo, P., & Slade, S. (2022). Realising the potential of learning analytics: reflections from a pandemic. In J. Liebowitz (Ed.), *Online learning analytics* (pp. 79–94). Auerbach Publications.

Komljenovic, J. (2020). The future of value in digitalised higher education: Why data privacy should not be our biggest concern. *Higher Education*, 1–17.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering*, *4*(3), 127–135. https://doi.org/10.1007/s12599-012-0216-6

Krueger, K. R., & Moore, B. (2015). New technology "clouds" student data privacy. *Phi Delta Kappan*, *96*(5), 19–24. https://doi.org/10.1177/0031721715569464

Lebeau, Y., & Oanda, I. O. (2020). *Higher education expansion and social inequalities in Sub-Saharan Africa: Conceptual and empirical perspectives* (Working Paper 2020-10). United Nations Research Institute for Social Development (UNIRISD). https://ueaeprints.uea.ac.uk/id/eprint/77509/

Luna, R. (2021, February 7). *Stranger danger!: How hackers break into school databases to steal student data, and what legislatures should do about it. How hackers break into school databases to steal student data, and what legislatures should do about it*. https://doi.org/10.2139/ssrn.3781055

Makulilo, A. B. (2015). Myth and reality of harmonisation of data privacy policies in Africa. *Computer Law & Security Review*, *31*(1), 78–89. https://doi.org/10.1016/j.clsr.2014.11.005

Makulilo, A. B. (2016a). The context of data privacy in Africa. In *African data privacy laws* (pp. 3–23). Springer.

Makulilo, A. B. (2016b). A person is a person through other persons-a critical analysis of privacy and culture in Africa. *Beijing Law Review*, *7*, 192–204. https://doi.org/10.4236/blr.2016.73020

Makulilo, A. B. (2021). The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius. *The International Journal of Human Rights*, *25*(1), 117–146. https://doi.org/10.1080/13642987.2020.1783532

Mannion, C. (2020). Data imperialism: The GDPR's disastrous impact on Africa's E-commerce markets. *Vanderbilt Journal of Transnational Law*, *53*, 685–711.

Mugimu, C. B. (2021). *Higher Education Institutions (HEIs) in Africa embracing the "new normal" for knowledge production and innovation: Barriers, realities, and possibilities*. IntechOpen. https://www.intechopen.com/online-first/79255

Munn, Z., Peters, M. D., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Medical Research Methodology*, *18*(1), 1–7. https://doi.org/10.1186/s12874-018-0611-x

Myers, J. (2019, August 30). *19 of the world's 20 youngest countries are in Africa*. World Economic Forum. https://www.weforum.org/agenda/2019/08/youngest-populations-africa/

Naudé, W. (2017). *Entrepreneurship, education and the fourth industrial revolution in Africa*. Naudé, Wim, Entrepreneurship, Education and the Fourth Industrial Revolution in Africa. https://ssrn.com/abstract=2998964 or https://doi.org/10.2139/ssrn.2998964

Ncube, C. B. (2016). Data protection in Zimbabwe. In *African data privacy laws* (pp. 99–116). Springer, Cham.

Newell, P. B. (1998). A cross-cultural comparison of privacy definitions and functions: A systems approach. *Journal of Environmental Psychology*, *18*(4), 357–371. https://doi.org/10.1006/jevp.1998.0103

Prinsloo, P., & Slade, S. (2017). Student vulnerability and agency in networked, digital learning. European Journal of Open, Distance and E-Learning. http://www.eurodl.org/?p=special&sp=articles&inum=8

Prinsloo, P. (2018). *Include us all! Directions for the adoption of learning analytics in the Global South: An African perspective*. Digital Learning for Development (DL4D). http://dl4d.org/portfolio-items/learning-analytics-for-the-global-south/

Prinsloo, P. (2020). Data frontiers and frontiers of power in (higher) education: A view of/from the Global South. *Teaching in Higher Education*, *25*(4), 366–383. https://doi.org/10.1080/13562517.2020.1723537

Prinsloo, P., Khalil, M., & Slade, S. (2021, September). Learning analytics in a time of pandemics: Mapping the field. In *EDEN Conference Proceedings* (No. 1, pp. 59–70).

Prinsloo, P., & Slade, S. (2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. https://doi.org/10.18608/jla.2016.31.10

Privacy International. (2017). *101: Data protection*. https://privacyinternational.org/explainer/41/101-data-protection

Solove, D. J. (2008). *Understanding privacy*. GWU Legal Studies Research Paper No. 420, GWU Law School Public Law Research Paper No. 420. https://ssrn.com/abstract=1127888

Statista. (2022). *Internet penetration rate in Africa as of December 2020, compared to the global average*. https://www.statista.com/statistics/1176654/internet-penetration-rate-africa-compared-to-global-average/

State of Broadband Report. (2020). *The State of Broadband 2020: Tackling digital inequalities. A decade for action*. International Telecommunication Union and United Nations Educational, Scientific and Cultural Organisation.

Singh, D., & Ramutsheli, M. P. (2016). Student data protection in a South African ODL university context: Risks, challenges and lessons from comparative jurisdictions. *Distance Education*, *37*(2), 164–179. https://doi.org/10.1080/01587919.2016.1184397

Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist*, *57*(10), 1510–1529. https://doi.org/10.1177/0002764213479366

Steiner, C. M., Kickmeier-Rust, M. D., & Albert, D. (2016). LEA in private: A privacy and data protection framework for a learning analytics toolbox. *Journal of Learning Analytics*, *3*(1), 66–90. https://doi.org/10.18608/jla.2016.31.5

Sutherland, E. (2018, June 22). *Digital privacy in Africa: Cybersecurity, data protection & surveillance*. https://doi.org/10.2139/ssrn.3201310

Tamrat, W., & Teferra, D. (2020). COVID-19 Threat to higher education: Africa's challenges, responses, and apprehensions. *International Higher Education*, *102*, 28–30.

Taylor, R. D. (2020). "Data localisation": The internet in the balance. *Telecommunications Policy*, *44*(8), 102003.

The Economist. (2020, March 28). *Africa's population will double by 2050*. https://www.economist.com/special-report/2020/03/26/africas-population-will-double-by-2050

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., … Straus, S. E. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. *Annals of Internal Medicine*, *169*(7), 467–473. https://doi.org/10.7326/M18-0850

Tuerk, M. (2020, June 9). Africa is the next frontier for the internet. *Forbes*. https://www.forbes.com/sites/miriamtuerk/2020/06/09/africa-is-the-next-frontier-for-the-internet/?sh=7a3fe26f4900

UN System Chief Executives Board for Coordination. (n.d.). https://unsceb.org/privacy-principles

United Nations Conference on Trade and Development (UNCTAD). (n.d.) https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

van Schalkwyk, F. (2021). Reflections on the public university sector and the covid-19 pandemic in South Africa. *Studies in Higher Education*, *46*(1), 44–58. https://doi.org/10.1080/03075079.2020.1859682

Varella, L. (2016). When it rains, it pours: Protecting student data stored in the cloud. *42 Rutgers Computer & Tech. LJ*, *94*, 103.

Vis, M., Dunbar, J. W., & Jahnke, J. H. W. (2011). *Indigenous and community-based notions of privacy*. https://www.researchgate.net/profile/Jens_Weber6/publication/310482039_Indigenous_and_Community-based_Notions_of_Privacy/links/582f93e408ae138f1c03595c/Indigenous-and-Community-based-Notions-of-Privacy.pdf

Williamson, B. (2021). Making markets through digital platforms: Pearson, edu-business, and the (e) valuation of higher education. *Critical Studies in Education*, *62*(1), 50–66. https://doi.org/10.1080/17508487.2020.1737556

Williamson, B., Bayne, S., & Shay, S. (2020). The datafication of teaching in Higher Education: Critical issues and perspectives. *Teaching in Higher Education*, *25*(4), 351–365. https://doi.org/10.1080/13562517.2020.1748811

Williamson, B., & Hogan, A. (2020). *Commercialisation and privatisation in/of education in the context of Covid-19*.

World Population Review. (n.d.). *Continent and region populations 2021*. https://worldpopulationreview.com/continents

How to cite this article: Prinsloo, P., & Kaliisa, R. (2022). Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. *British Journal of Educational Technology*, *00*, 1–20. https://doi.org/10.1111/bjet.13226

APPENDIX A

PEER REVIEWED, SCHOLARLY PAPERS IN THIS SCOPING REVIEW

Author(s) and data	Paper title
Abdulrauf, L. A., and Fombad, C. M. (2016)	The African Union's data protection Convention 2014: A possible cause for celebration of human rights in Africa? *Journal of Media Law,* 8(1), 67–97
Abdulrauf, L. A., and Fombad, C. M. (2017)	Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms. *Liverpool Law Review*, 38(2), 105–134
Abebe, R., Aruleba, K., Birhane, A., Kingsley, S., Obaido, G., Remy, S. L., & Sadagopan, S (2021, March)	Narratives and counter narratives on data sharing in Africa. In Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (pp. 329–341)
Agbozo, E., Alhassan, D., & Spassov, K. (2018, November)	Personal data and privacy barriers to e-Government adoption, implementation and development in Sub-Saharan Africa. In *International Conference on Electronic Governance and Open Society: Challenges in Eurasia* (pp. 82–91). Springer, Cham
Alunge, R. (2019, May)	The Effect of Africa's Adoption of the EU Notion of Personal Data: The Case of Examination Results. In 2019 IST-Africa Week Conference (IST-Africa) (pp. 1–13). IEEE
Borena, B., Belanger, F., & Egigu, D (2015, January)	Information privacy protection practices in Africa: A review through the lens of critical social theory. In 2015 48th Hawaii International Conference on System Sciences (pp. 3490–3497). IEEE
Dagbanja, D. N. (2016)	The right to privacy and data protection in Ghana. In *African Data Privacy Laws* (pp. 229–248). Springer, Cham
Daigle, B. (2021)	Data Protection Laws in Africa: A Pan-African Survey and Noted Trends. Journal of International Commerce and Economics
Hakimi, L., Eynon, R., & Murphy, V. A. (2021)	The ethics of using digital trace data in education: A thematic review of the research landscape. *Review of Educational Research*, 00346543211020116
Makulilo, A. B. (2016a)	The context of data privacy in Africa. In *African Data Privacy Laws* (pp. 3–23). Springer, Cham

Author(s) and data	Paper title
Makulilo, A. B. (2016b)	A person is a person through other persons-a critical analysis of privacy and culture in Africa. Beijing L. Rev., 7, 192
Makulilo, A. B. (2021)	The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius. The International Journal of Human Rights, 25(1), 117–146
Ncube, C. B. (2016)	Data Protection in Zimbabwe. In *African Data Privacy Laws* (pp. 99–116). Springer, Cham
Singh, D., and Ramutsheli, M. P. (2016)	Student data protection in a South African ODL university context: Risks, challenges and lessons from comparative jurisdictions. *Distance Education*, 37(2), 164–179
Sutherland, E. (2018)	Digital privacy in Africa: Cybersecurity, data protection & surveillance. *Data Protection & Surveillance* (June 22, 2018)