

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

DIGITAL COLONIALISM THROUGH AI IN HIGHER EDUCATION: A GLOBAL SOUTH PERSPECTIVE ON DATA SOVEREIGNTY AND ALGORITHMIC GOVERNANCE

AUTHORED BY - TUSHAR SUBRAT

Abstract

The governance of artificial intelligence (AI) in higher education presents one of the most significant regulatory challenges of the digital age, particularly for institutions situated within the Global South. Existing policy and legal debates have predominantly framed AI governance through concerns of privacy, security, and ethical compliance, often overlooking the structural power asymmetries embedded within global digital ecosystems. This paper addresses that gap by examining the deployment of AI in higher education through the lens of digital colonialism, with particular attention to issues of data sovereignty, platform dependency, and algorithmic governance.

Employing a doctrinal and comparative legal methodology, the study analyses international AI governance instruments, data protection frameworks, and emerging regulatory approaches, alongside selected case studies concerning educational technology platforms, AI-enabled surveillance, cloud infrastructure dependence, and cross-border data governance. It argues that the growing reliance of universities on foreign-owned digital infrastructures and AI systems creates new forms of technological dependency that extend beyond conventional privacy concerns. These dependencies facilitate the extraction and external control of educational data, concentrate algorithmic authority within a limited number of transnational technology corporations, and risk reinforcing epistemic hierarchies that marginalize local, indigenous, and non-Western knowledge systems.

The analysis demonstrates that prevailing legal and policy frameworks, including data protection regimes and AI ethics instruments, provide only partial responses to these challenges because they primarily regulate the use of data rather than the underlying structures of technological power. While examining India's emerging regulatory landscape—including the Digital Personal Data Protection Act, 2023, the National Education Policy, 2020, and recent AI governance initiatives—the paper identifies both the opportunities and limitations of existing approaches to safeguarding educational autonomy in an increasingly platformized environment.

The paper contends that effective AI governance in higher education must be reconceptualized as a question of data sovereignty, platform sovereignty, and educational self-determination. It proposes a decolonial governance framework centred on sovereign digital infrastructure, algorithmic accountability, public-interest AI development, localized data governance, and enhanced Global South participation in international norm-making. By situating AI governance within broader debates on postcolonial power, knowledge production, and technological dependence, this study contributes to the emerging scholarship on digital colonialism and offers a Global South-centred framework for regulating AI in higher education.

Keywords:

Artificial Intelligence; Higher Education; Digital Colonialism; Data Sovereignty; Algorithmic Governance; Global South; India; Educational Technology; Decoloniality; AI Regulation.

1. Introduction

The increasing integration of Artificial Intelligence (AI) into higher education has been widely celebrated as a transformative development capable of enhancing pedagogical efficiency, personalizing learning experiences, expanding educational access, and improving institutional governance. Universities across the world are rapidly adopting AI-enabled technologies, including learning management systems, predictive analytics, automated assessment tools, generative AI platforms, and digital administrative infrastructures. In policy discourse, particularly within developing economies, these technologies are frequently portrayed as instruments of innovation capable of accelerating educational modernization and bridging longstanding developmental gaps.

However, the deployment of AI in higher education raises critical questions that extend beyond technological advancement and regulatory compliance. The concentration of AI development, computational infrastructure, and data-processing capabilities within a small number of multinational technology corporations has generated new forms of dependency that disproportionately affect institutions in the Global South. Educational institutions increasingly rely on digital platforms, cloud infrastructures, and algorithmic systems designed, owned, and governed by actors located outside their jurisdictions. Consequently, the adoption of AI in higher education is not merely a question of efficiency or innovation, but also one of power, control, and sovereignty.

This paper situates the governance of AI in higher education within the broader theoretical frameworks of neo-colonialism, digital colonialism, and data colonialism. While classical

colonialism relied upon territorial occupation and direct political domination, contemporary forms of control increasingly operate through technological infrastructures, data extraction mechanisms, and knowledge-production systems. The expansion of AI-driven educational technologies has created conditions in which student data, institutional resources, and academic practices become embedded within transnational digital ecosystems controlled by external actors. Such developments raise concerns regarding **data sovereignty, algorithmic accountability, privacy, academic freedom, and the preservation of local knowledge systems.**

Particular attention must be paid to the Global South, where historical experiences of colonial domination continue to shape contemporary technological and economic relationships. AI systems are predominantly trained on datasets, linguistic frameworks, and epistemological assumptions originating in the Global North. As a result, algorithmic decision-making processes often reproduce existing structural inequalities while marginalizing indigenous, local, and non-Western forms of knowledge. The growing dependence of universities on foreign technological infrastructures therefore risks creating new forms of epistemic subordination and institutional dependency, thereby reproducing colonial patterns in digital form.

Against this backdrop, this paper critically examines the implications of AI-driven higher education through the interconnected lenses of data sovereignty and algorithmic governance. It argues that the governance of AI in higher education cannot be understood solely as a matter of technological regulation; rather, it constitutes a broader struggle over control of data, digital infrastructure, knowledge production, and educational autonomy. Through a doctrinal and comparative analysis of international and domestic legal frameworks, including India's emerging AI and data governance regime, the paper evaluates the adequacy of existing regulatory responses to these challenges.

2. Methodology

The paper proceeds in five parts. First, it establishes the conceptual foundations of digital colonialism and its relevance to contemporary AI governance. Second, it analyses the manifestations of digital colonialism within higher education through selected case studies from the Global South. Third, it examines the implications of AI adoption from a rights-based perspective, focusing on privacy, equality, cultural rights, academic freedom, and cognitive liberty. Fourth, it evaluates the legal and policy frameworks governing AI, data protection, and educational technology at both national and international levels, with particular emphasis on

India. Finally, it proposes a set of legal, institutional, and policy recommendations aimed at strengthening data sovereignty, promoting algorithmic accountability, and advancing a more equitable and decolonized model of AI governance in higher education.

By interrogating the relationship between artificial intelligence, educational governance, and postcolonial power structures, this paper seeks to contribute to the emerging scholarship on digital colonialism and to advance a Global South perspective on the future regulation of AI in higher education.

3. Conceptual Framework.

It is necessary to place current technology advancements within larger historical power systems in order to comprehend the implications of artificial intelligence (AI) in higher education. Critical research increasingly contends that AI's design, implementation, and governance reflect long-standing disparities between technologically dominant and dependent civilisations, despite the technology's frequent portrayal as a neutral and revolutionary instrument.

Kwame Nkrumah¹ was the most well-known proponent of neo-colonialism, arguing that formal political independence did not always mean the end of colonial connections. Rather than using direct territorial domination, control was increasingly exercised through institutional, cultural, and economic channels. Therefore, the term "neo-colonialism" describes a situation in which formally independent states continue to rely on outside forces for governance, finance, technology, and knowledge production.

Through the concept of coloniality, postcolonial theorists expanded on this understanding. Aníbal Quijano² defines coloniality as persistent systems of knowledge, authority, and social structure that endure after colonial governments have ended. Alternative types of knowledge are marginalised by these frameworks, which nonetheless favour Western epistemologies. In a similar vein, decolonial researchers contend that colonialism and modernity are historically entwined, making technological advancement inextricably linked to issues of dominance and power. The persistence of these inequalities is especially evident in educational institutions, which have traditionally served as vehicles for the spread of colonial languages, values, and methods of knowledge production. These days, instructional tools powered by AI run the risk of digitally replicating comparable patterns.

Decolonisation, according to decolonial theorist like Walter Dignolo³, is an epistemic endeavour that aims to undermine systems that favour a single universal idea of knowledge rather than just a political process. As a result, any evaluation of AI in higher education must

look at whose knowledge systems are represented, validated, and amplified in addition to who controls technology infrastructures.

Neo-colonial theory is translated into the field of ICTs via the paradigm of digital colonialism. It describes a system in which less technologically proficient regions' digital infrastructures, software ecosystems, online platforms, and data streams are controlled by powerful nation-states and multinational technology conglomerates.

According to Michael Kwet⁴, these companies systematically take economic and social value from the Global South while ensnaring countries in a condition of structural technological dependence by controlling operating systems, cloud networks, and data ecosystems.

Higher education institutions in poor nations rely on cloud-based learning management systems, generative AI applications, and AI tools created and hosted elsewhere. Local universities are reduced to passive consumers of technical frameworks whose basic design and governance procedures remain outside their control as a result of this structural dependency, which creates profoundly unbalanced relationships.

Given that algorithms are trained on historically biased datasets and created within particular cultural contexts, critical AI scholars have shown that they typically replicate current socioeconomic disparities.

The issues in higher education go beyond fairness to include epistemic injustice. The idea, which was developed by philosopher Miranda Fricker⁵, describes the deliberate exclusion of some groups as knowledgeable people. Since generative AI models are mostly trained on datasets from Western, English-language sources, they under-represent indigenous, local, and non-Western epistemologies while favouring specific types of knowledge. According to recent research, generative AI may exacerbate information asymmetries, hermeneutical exclusion, and testimonial injustice.

Algorithmic homogenisation is an imminent danger to universities in the Global South. AI-generated educational materials may favour Western conceptual frameworks over regional intellectual traditions over time.

Taken together, neo-colonialism, digital colonialism, data colonialism, and critical AI theory reveal that AI governance in higher education cannot be understood solely as a technical or regulatory issue. Instead, it involves struggles over infrastructure, data, knowledge, and power. The central concern is not merely who uses AI, but who designs it, who controls its underlying data, whose values are embedded within its algorithms, and who benefits from its deployment. This paper therefore adopts a multidimensional framework that views AI-driven higher education through four interconnected layers: **infrastructural control**, **data extraction**,

algorithmic governance, and **epistemic domination**. These dimensions collectively illuminate how contemporary AI systems may reproduce colonial patterns of dependency and exclusion while simultaneously creating new challenges for data sovereignty and democratic governance in the Global South. This framework will guide the subsequent analysis of AI-enabled educational platforms, cross-border data flows, regulatory responses, and pathways toward a more equitable and decolonized digital future.

4. Digital Colonialism in Higher Education

The rapid integration of Artificial Intelligence (AI) into higher education has been celebrated as a transformative force capable of democratizing knowledge, personalizing learning, improving institutional efficiency, and expanding educational access.

However, beneath this narrative of technological progress lies a deeper question: **who controls the digital infrastructure through which education is increasingly delivered?**

Universities across the Global South increasingly rely upon cloud computing services, learning management systems, plagiarism-detection software, videoconferencing platforms, AI tutors, and generative AI applications developed and hosted primarily in the United States and Europe. India's educational policies mirror a worldwide wave of technological optimism regarding AI. The National Education Policy (NEP) 2020 champions this shift by leveraging digital tools, AI-driven personalized learning, and expanded tech access to revolutionize classrooms. Backed by government efforts, educational institutions are actively building their digital infrastructure and promoting AI literacy (CIET). This enthusiasm is clearly reflected in recent updates: AI is now embedded in standard curricula, the UGC is adding AI disciplines to higher education, and the AICTE has officially dubbed 2025 the "Year of Artificial Intelligence" (AICTE).

However, this rapid push for AI lacks crucial regulatory safeguards. Current policies prioritize adopting new tech over protecting data sovereignty, ensuring algorithmic transparency, or maintaining institutional independence. As UNESCO warns, embracing AI in classrooms requires strict protections against bias, privacy breaches, and digital divides (UNESCO). Compounding these risks, Michael Kwet⁴ warns of "digital colonialism." By relying heavily on foreign software and platform monopolies, educational institutions cede control, allowing outside entities to dictate tech design and reap the economic benefits without the need for physical occupation.

This reliance on outside technology has deepened with the surge of generative AI tools like ChatGPT, Gemini, Claude, and Copilot. Universities are eagerly embedding these platforms

into their academic and administrative routines, despite having no say in how the algorithms are trained or governed. Consequently, educational independence is sacrificed to the profit-driven goals of tech companies. Furthermore, as Virginia Eubanks⁶ highlights in *Automating Inequality*, such automated systems often disguise systemic biases as objective efficiency. While her work focused on welfare, the warning applies perfectly to higher education: algorithms may look neutral, but they frequently hardwire existing social and economic inequalities into institutional decision-making.

Recent debates over AI-detection tools highlight these exact risks. While universities widely use these programs to catch academic dishonesty, the software frequently misfires, disproportionately penalizing non-native English speakers (The Guardian). Similarly, the large language models themselves are trained primarily on English data from the Global North. As a result, they echo Western ideas while sidelining indigenous and local knowledge. This creates what is known as "epistemic injustice"—systematically silencing non-Western voices and trapping students in a narrow intellectual bubble. Ruha Benjamin's⁷ concept of "coded inequality" perfectly describes this phenomenon: technology often masks historical discrimination as objective innovation. In universities, this means AI can quietly reinforce old biases, even when it is promoted as a tool for inclusion.

Ultimately, digital colonialism in academia is about much more than just adopting new tools. It represents a massive shift where educational infrastructure, institutional data, and knowledge itself are swallowed up by global networks controlled by a handful of tech giants. The real question, then, isn't whether universities should use AI, but rather who sets the rules, who benefits, and who actually holds the reins.

5. Case Studies

This paper illustrates the analysis with several case studies of AI integration in Global South higher education contexts. These examples, while not exhaustive, highlight concrete tensions.

5.1 Data Colonialism: BYJU'S and the Commodification of Educational Data

BYJU's is one of India's dominant ed-tech companies, with AI-driven personalized learning apps. A recent case study notes BYJU's rapid growth via "advanced tools and constant marketing," but it raises concerns about transparency and governance. Critics highlight issues in data use, employee treatment, and lack of clarity on how student data fuel algorithms. For instance, 2025 reports mention BYJU's intense data collection (screen time, quiz responses) to optimize content, yet parents and regulators question data privacy and bias. As a Global South

company, BYJU's sits in a complex position: it aims to serve Indian learners, but also partners with (and is influenced by) global investors and technologies. If its AI models rely on Western technology or datasets, Indian students may experience pedagogical misalignment. This case exemplifies "neocolonial corporate dynamics" – a local firm harnessing global AI, where profit motives can overshadow equitable educational goals. BYJU's case underscores the ethical dilemmas when EdTech corporations control learning data.

5.2 Surveillance Colonialism: AI Proctoring and Educational Monitoring

In Johannesburg, a private network "Vumacam" installed over 5,000 CCTV cameras with AI analytics in residential areas. Although aimed at crime reduction, academics warn this "turns CCTV into a tool of everyday surveillance," disproportionately affecting poor and historically oppressed communities. Activists draw explicit links to apartheid-era policing. Within universities, remote proctoring is also on the rise – for example, South African universities trialing AI monitoring of exams (eye-tracking, ambient noise analysis) have sparked privacy debates. The Vumacam example is outside campus walls, but it highlights "racialized bias in AI surveillance": algorithms trained on certain populations often misidentify or flag minority-group behavior. In education, similar biases can emerge if, say, proctoring software misreads gestures or accent in student voices. This case underscores that digital colonialism includes surveillance: external providers (often Western tech) supply monitoring tools that may entrench old social hierarchies.

5.3 Infrastructure Colonialism: Cloud Integration and Systemic Platform Reliance

Universities across the Global South exhibit a growing reliance on the core digital architectures built and managed by multinational technology monopolies. Academic institutions routinely outsource the hosting of their research repositories, learning management systems, and artificial intelligence frameworks to foreign cloud platforms operated by giants like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.

This systemic integration characterizes the phenomenon known as "infrastructure colonialism." For example, the adoption of software suites like Microsoft Teams and Google Workspace by universities in Africa, South Asia, and Southeast Asia escalated dramatically during the COVID-19 pandemic to preserve academic continuity. While these tools provided crucial remote learning support, they simultaneously locked autonomous educational institutions into proprietary, corporate-controlled technical environments. This dynamic significantly undermines technological self-determination and creates acute vendor lock-in, generating

severe financial and technical friction that prevents universities from migrating to domestic or open-source alternatives.

5.4 Labor Colonialism: Digital Subcontracting and the Global South Workforce

The operational viability of artificial intelligence relies on a vast infrastructure of human labor. Before machine learning models can accurately execute image classification, natural language processing, or speech recognition, they require massive volumes of meticulously categorized datasets—a labor-intensive prerequisite that global technology firms routinely outsource to developing economies.

Kenya has emerged as a primary hub for this digital subcontracting. Investigative findings reveal that outsourcing agencies employ thousands of Kenyan workers to moderate explicit content, filter toxic material, and sanitize datasets for elite AI developers, including organizations like OpenAI. These workers frequently endure substandard wages while suffering acute psychological distress from prolonged exposure to harmful material. A parallel dynamic is evident in India, which hosts a substantial segment of the invisible workforce executing the data labeling, content moderation, and algorithmic optimization that underpins contemporary AI systems.

Scholars classify this unequal distribution of work as "labor colonialism" because it systematically replicates historical imperial divisions of labor. Under this framework, high-value, high-margin activities—such as foundational AI research, intellectual property ownership, and primary profit extraction—remain concentrated within dominant, technologically advanced economies. Conversely, the highly repetitive, poorly compensated, and hazardous tasks are exported to the Global South.

While universities globally pressure students to acquire AI-centric competencies, the architecture of the international digital economy routinely channels labor from developing nations into the lowest tiers of the global value chain. Consequently, superficial integration into the global AI ecosystem fails to catalyze genuine technological empowerment or structural equity.

These cases (admissions, learning, surveillance, language) are summarized in Table 1. They reveal recurring patterns: external actors (tech companies or governments) set AI agendas; local communities have limited input; and historical inequalities are mirrored in the data and algorithms. In each example, data flows outward and decisions flow inward.

Case	Region & Context	AI Application	Digital Colonialism Issues
Data Colonialism (BYJU'S)	India / Global South; commercial EdTech backed by global capital.	AI-driven learning apps tracking screen time, quiz responses, and behavior.	Corporate monetization and extraction of student data without transparent local consent.
Surveillance Colonialism (AI Proctoring)	Johannesburg, South Africa; urban centers and universities.	Remote exam proctoring (eye-tracking) and city-wide facial recognition.	Entrenchment of historical biases and social hierarchies through invasive algorithmic monitoring.
Infrastructure Colonialism (Cloud Integration)	Global South universities; post-COVID-19 digital pivot.	Cloud platforms and LMS (AWS, Azure, Google Workspace, Teams).	Loss of technological sovereignty due to severe corporate vendor lock-in to external infrastructure.
Labor Colonialism (Digital Subcontracting)	Kenya and India; backend workforce for Western tech.	Data annotation, content moderation, and dataset sanitization.	Exploitative outsourcing that traps local workforces at the lowest tier of the global value chain.

Table 1: Examples of AI use in Global South higher education and related digital colonialism concerns

6. Rights-Based Analysis

While the integration of Artificial Intelligence (AI) into higher education is typically championed for driving efficiency, customized learning, and technological advancement, evaluating this trend through a human rights lens exposes a deeper reality. Rather than acting

as neutral instruments, AI systems function as administrative frameworks that actively shape fundamental liberties. The systemic harvesting of student data, reliance on automated decision-making, dependence on foreign platforms, and transnational data extraction pose serious risks to privacy, academic freedom, equity, and cultural sovereignty.

6.1 Right to Privacy and Informational Self-Determination

The foremost rights issue introduced by educational artificial intelligence is the threat to privacy and informational self-determination. As affirmed by the Supreme Court of India in *Justice K.S. Puttaswamy v. Union of India* (2017)⁸, privacy is not merely about concealment; it fundamentally involves the ability to exercise meaningful control over one's personal data to preserve human dignity.

AI-integrated learning platforms systematically harvest an extensive array of student data, spanning academic metrics, biometric markers, emotional responses, and predictive behavioral analytics. Instruments such as remote proctoring software, eye-tracking algorithms, and facial recognition effectively convert modern educational spaces into environments of pervasive, continuous surveillance.

While India's Digital Personal Data Protection (DPDP) Act of 2023⁹ mandates informed consent and purpose limitation, the inherent power imbalance in academic settings complicates these protections. Because students are practically compelled to accept the technological terms set by their institutions to access their education, "consent" is often reduced to a mandatory procedural formality rather than a genuine, autonomous choice.

Global regulatory frameworks—such as the GDPR¹⁰, the EU AI Act¹¹, and UNESCO's Recommendation on the Ethics of AI¹²—mirror these exact concerns. They advocate for strict transparency, proportionality, and human oversight, recognizing that educational data is exceptionally sensitive because it maps a student's cognitive development, behavioral habits, and future potential.

Viewed through the lens of digital colonialism, these AI systems reduce students to heavily monitored subjects whose personal information is continuously extracted, analyzed, and commodified across transnational digital networks. Consequently, personal informational autonomy is usurped by algorithmic surveillance. This widespread deployment of behavioral profiling and cross-border data extraction jeopardizes cognitive privacy, ultimately treating learners less as students and more as raw data sources fueling the global AI economy

6.2 The Right to Equality and Protection from Algorithmic Discrimination

The integration of artificial intelligence into academic settings poses substantial risks to the principles of equality and non-discrimination. Foundational legal frameworks—including Articles 14 and 15 of the Indian Constitution, alongside global human rights treaties like the ICCPR¹³ and ICESCR¹⁴—strictly forbid discriminatory practices and mandate equitable access to educational opportunities.

Despite the prevailing narrative that frames AI as an impartial and objective tool, critical scholarship reveals that algorithmic systems routinely institutionalize and exacerbate existing social disparities. Prominent researchers, such as Safiya Umoja Noble¹⁸, Ruha Benjamin⁷, and Virginia Eubanks⁶, have extensively documented how these technologies inherit the structural biases, cultural assumptions, and skewed datasets of their creators.

Within higher education, this algorithmic bias materializes through several distinct vectors:

- **Linguistic Marginalization:** English-dominant large language models (LLMs) inherently disadvantage students whose primary language is not English.
- **Biased Surveillance:** Facial recognition and remote proctoring tools frequently exhibit reduced accuracy for individuals with darker skin tones, significantly increasing the risk of misidentification and unjust exclusion.
- **Cultural Standardization:** Automated grading and assessment algorithms often reward writing styles, linguistic conventions, and cultural references that align strictly with Western academic traditions.

Even in the absence of explicit malicious intent, these dynamics result in disparate impact and indirect discrimination. The core issue is not a matter of isolated software glitches, but rather deeply structural flaws embedded within the algorithmic architecture itself. Consequently, students from marginalized socio-economic, cultural, and linguistic backgrounds face systematic disadvantages when their academic evaluations are mediated by AI.

6.3 The Right to Education and Substantive Learning

The right to education serves as the fundamental normative benchmark for assessing the integration of AI in higher education. Anchored in Article 21A of the Indian Constitution, Article 13 of the ICESCR¹⁴, UNESCO's Sustainable Development Goal 4 (SDG 4), and General Comment No. 13 of the Committee on Economic, Social and Cultural Rights¹⁵, education is universally recognized as an essential human right.

Unquestionably, artificial intelligence has the capacity to democratize academic access, tailor learning experiences, and bridge geographic divides. Innovations such as adaptive learning

environments, automated translation, and intelligent tutoring systems hold immense potential to broaden participation—a vision enthusiastically echoed in frameworks like India’s National Education Policy (NEP) 2020.

Nevertheless, a human rights perspective demands scrutiny of not just educational accessibility, but the intrinsic quality and purpose of learning. As outlined in General Comment No. 13, education is a holistic process meant to cultivate human dignity, personality, and active societal participation. It must not be reduced to the mere automated and efficient transfer of data.

An overreliance on proprietary AI architectures threatens to forge new paradigms of educational dependency. As universities increasingly outsource their digital infrastructure to private tech conglomerates, public academic priorities risk being subsumed by corporate motives. Furthermore, algorithmically driven content threatens to homogenize curricula, elevating dominant global perspectives while actively sidelining and marginalizing localized knowledge systems.

6.4 Cultural and Linguistic Rights

The colonial underpinnings of artificial intelligence are highly pronounced when analyzed through the lens of cultural and linguistic rights. International legal instruments—such as the 2005 UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions and the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP)¹⁷—explicitly mandate the protection of linguistic diversity and cultural self-determination.

However, generative AI models are overwhelmingly trained on English-centric datasets and epistemological repositories anchored in the Global North. This asymmetry systematically elevates dominant Western languages and cultural paradigms while marginalizing languages with limited digital footprints, which frequently suffer from poor performance, systemic inaccuracies, and reduced accessibility.

This imbalance introduces severe risks of digital homogenization and epistemic erasure:

- **Marginalization of Local Knowledge:** Indigenous histories, traditional pedagogies, and non-Western intellectual traditions are increasingly rendered invisible within AI-mediated educational platforms.
- **Reinforcement of Hierarchies:** Students who rely predominantly on AI-generated content are exposed to a restricted spectrum of perspectives that implicitly legitimize global knowledge hierarchies.

This dynamic is uniquely damaging to postcolonial societies, where educational institutions

historically functioned as primary tools for cultural subjugation. Digital colonialism replicates these legacy power structures through algorithmic mechanisms rather than physical imperial administrations. Modern hegemony operates by outsourcing control to technological frameworks that unilaterally dictate which forms of information are recognized as visible, credible, and authoritative.

6.6 Emerging Rights: Cognitive Liberty

An emerging domain of critical scholarship advocates for the recognition of **cognitive liberty**—the fundamental right of individuals to maintain sovereignty over their own mental faculties and psychological development. Although it has not yet been formally codified within most domestic or international statutory legal systems, cognitive liberty has become a central pillar in contemporary discourses surrounding neuro-rights and artificial intelligence ethics.

AI-driven educational ecosystems do not merely act as passive collectors of information; they actively manipulate learning trajectories, direct cognitive focus, curate content delivery, and scaffold intellectual engagement. Through proprietary recommendation algorithms and predictive analytics, these systems systematically dictate the specific knowledge architectures students encounter, thereby shaping their academic choices and long-term opportunities.

Within this framework, digital colonialism transcends the expropriation of data and infrastructure, encroaching upon human cognition itself. When the algorithmic architectures that govern how students think, learn, and interpret knowledge are engineered exclusively by external corporate actors, the foundational principles of intellectual self-determination and cognitive autonomy are fundamentally compromised.

Although still an evolving paradigm, the concept of cognitive liberty underscores a critical shift in the future of educational governance

A rights-based perspective demonstrates that digital colonialism within higher education extends far beyond simple economic disparities or technological reliance. Instead, it directly compromises a comprehensive spectrum of fundamental liberties—encompassing privacy, equity, the right to learning, cultural self-determination, academic freedom, and the evolving concept of cognitive liberty.

7. Data Sovereignty and Cross-border Data Flow

7.1. Data Sovereignty

Rather than merely utilizing digital tools, contemporary universities are being systematically integrated into comprehensive AI ecosystems that dictate data governance and institutional

administration. These AI infrastructures function by consuming expansive student-generated datasets, including academic submissions, behavioral telemetry, grading histories, metadata, and biometric markers. Moving this material to external systems shifts the core ethical dilemma beyond data privacy toward critical questions of structural ownership and systemic control.

This institutional absorption is underscored by massive corporate initiatives, such as OpenAI's partnership with California State University deploying ChatGPT Edu to roughly 500,000 users across 23 campuses, alongside Google's \$1 billion higher-education initiative providing financial incentives, cloud credits, and Gemini access to over 100 launching universities¹⁹. These agreements illustrate how higher education is being structurally bound to rely on external providers for foundational academic operations.

This state of dependency is highly consequential because this dynamic induces a "data-commons" contradiction: the university serves as the primary engine of value generation, yet the infrastructural conglomerate monopolizes the data pipelines.

7.2. Platform Power

Digital sovereignty is inextricably linked to platform power—specifically, the authority to establish system defaults, control user interfaces, and dictate the operational parameters under which academic institutions must function. The defining trend in modern higher education is vendor lock-in, driven by a highly concentrated oligopoly of technology conglomerates. A small handful of corporations—specifically Google, Microsoft, OpenAI, and Amazon—increasingly monopolize the integrated AI assistants, cloud infrastructures, productivity suites, and administrative ecosystems that anchor university operations. These aggressive corporate expansions signify that universities are not simply procuring detached software utilities; they are entering enduring, structural platform dependencies that systematically restrict institutional autonomy and dictate internal governance frameworks.

This dynamic illustrates how platform capitalism directly mutates into an administrative governance challenge. Once a university deeply embeds its communication networks, pedagogical content delivery, and student assessment mechanisms within a proprietary architecture, migrating to alternative frameworks becomes economically, technically, and politically prohibitive. Consequently, routine commercial procurement choices inherently dictate the structural design of pedagogy. For nations in the Global South, this creates a dual vulnerability: severe economic reliance paired with profound epistemic dependence, as curriculum design, student support mechanisms, and evaluative standards become mediated by algorithmic models trained and optimized on foreign datasets. Ultimately, the authority to

define baseline academic standards—such as educational "efficiency," "safety," or "innovation"—is outsourced from traditional academic bodies to corporate software engineering teams, presenting a direct challenge to educational self-determination.

7.3. Platform Sovereignty

Digital sovereignty fundamentally intersects with the challenge of platform dependency, as academic institutions increasingly consolidate their reliance on a narrow oligopoly of technology conglomerates—specifically OpenAI, Google, Microsoft, Amazon, and Anthropic—for foundational AI utilities, cloud networks, and digital communication suites. This high concentration of market power engenders severe institutional dependency, diminishes educational self-determination, and creates acute risks of vendor lock-in.

The mechanics of platform capitalism function by deeply embedding users within closed, proprietary architectures where the financial, technical, and operational costs of exit are prohibitively high. Within higher education, this structural capture is evidenced by the ubiquitous implementation of enterprise tools such as Microsoft Teams, Google Workspace, Google Classroom²⁰, and Amazon Web Services (AWS). Once a university embeds its primary administrative operations, grading frameworks, learning management systems, and research workflows into a specific ecosystem, migrating to an alternative infrastructure becomes structurally and economically impractical.

This profound reliance severely compromises platform sovereignty. While universities may nominally retain their formal academic independence, they become structurally subordinate to infrastructural architectures dictated by private interests. Consequently, crucial decisions regarding algorithmic parameters, user interface design, data governance, and content moderation are systematically transferred from educational authorities to corporate boards.

7.4. Global South Digital Colonialism

These ethical and structural challenges are significantly magnified in the Global South, where AI integration unfolds against a backdrop of deep infrastructural, economic, and technological asymmetries. Academic institutions in developing nations typically deploy imported AI architectures that are trained on external datasets and regulated by frameworks engineered for vastly different socio-cultural contexts.

This rapid, unregulated expansion is evidenced by a 2025 UNESCO survey²¹ indicating that nearly two-thirds of universities globally have either established or are actively drafting AI governance policies. While this indicates a rising awareness of the stakes, it simultaneously

highlights how the velocity of technological adoption is vastly outpacing institutional and regulatory preparedness.

Consequently, achieving genuine digital sovereignty in the Global South demands far more than basic data privacy legislation. It necessitates comprehensive digital self-determination—encompassing the cultivation of sovereign digital infrastructure, local AI ecosystems, public-interest data governance, and the institutional capability to build viable alternatives to foreign platforms. Failing to secure these foundational elements risks transforming higher education into a modern frontier of digital colonialism, where a concentrated oligopoly of transnational technology conglomerates permanently monopolizes the control of data, digital infrastructure, and global knowledge production.

8. India Legal Framework

8.1 Data Protection Framework

DPDP Act 2023: India's new Digital Personal Data Protection Act⁹ creates a consent-based regime. Personal data may be processed only for “lawful purposes” with free, specific consent (or under broadly defined “legitimate uses” that include government services and sovereignty/security). Individuals gain rights to access, correct, port or erase their data and to know which agencies hold or share it. Data fiduciaries (entities processing data) must implement security safeguards, appoint Data Protection Officers, notify breaches, and erase data when no longer needed. The Act also creates a category of “Significant Data Fiduciaries” (large processors) with extra duties (mandatory DPIAs, audits). Crucially, mandatory localization was relaxed: the government may simply *notify* restrictions on cross-border flows (for example on national security grounds).

- **Srikrishna Committee & Draft Bills²²:** The 2018 Justice B.N. Srikrishna Committee report (and the draft 2019 PDP Bill) had envisioned a GDPR-style framework: detailed obligations on **data fiduciaries**, classification of data as sensitive or critical, and an independent Data Protection Authority (DPA) with broad rule-making power. The Srikrishna draft mandated user consent, data audits, and data-localization for certain purposes. These recommendations directly informed later laws, although the final DPDP Act (2023) scaled back many requirements and centralized more discretion in government hands.
- **IT Act 2000 and SPDI Rules 2011²³:** Prior to dedicated privacy law, India's IT Act and its 2011 rules provided limited protection. Section 43A of the IT Act (as interpreted by the Sensitive Personal Data or Information – SPDI – Rules) imposed liability on

companies that negligently failed to protect “sensitive personal data” (e.g. passwords, financial, health or biometric data). The law required “reasonable security practices and procedures” – defined as safeguards to prevent unauthorized access or disclosure. However, this regime did not grant user rights (beyond compensation) or a regulatory authority; it merely allowed aggrieved individuals to sue for damages.

8.2 Educational Governance Framework

- **National Education Policy (NEP) 2020²⁴:** The NEP emphasizes leveraging technology in education while bridging the digital divide. It calls for creating “*open, interoperable, evolvable, public digital infrastructure*” in the education sector to support multiple learning platforms. Existing national e-learning platforms (like SWAYAM and DIKSHA) should be scaled up with richer assistive tools (two-way video/audio for virtual classes, analytics dashboards for teachers).. NEP also mandates digital content repositories (including AR/VR, gamified learning apps) and backup mechanisms for e-content dissemination. These initiatives aim to reach students wherever they are, in multiple Indian languages, especially during disruptions (e.g. pandemics).
- **UGC/AICTE Guidelines²⁵:** In 2020 the UGC liberalized online education: accredited universities (based on high NAAC/NIRF scores) may offer full-fledged online UG and PG programs. The All India Council for Technical Education (AICTE) issued parallel guidelines (2021) allowing approved institutes to run online professional courses (MBA, MCA) subject to NBA accreditation and other criteria. Both regulators strictly forbid online delivery for programs that require hands-on training or campus labs: for example, engineering (with lab courses), medical, architecture, agriculture, and any research degrees (M.Phil/Ph.D) remain off-limits. Online exams are allowed (with options for proctored home tests or exam centers), but practices like franchise recruitment or off-campus expansions are prohibited.
- **Academic Bank of Credits (ABC):** NEP 2020 envisioned a digital *Academic Bank of Credits* to record every student’s earned credits in one repository. Through the ABC, students can seamlessly transfer and redeem credits across institutions or programs, facilitating flexibility (e.g. multi-disciplinary learning) while preserving integrity and confidentiality of records. This virtual credit-banking infrastructure underpins new modular and cross-institutional degree structures.
- **National Digital (or Digital) University:** In the 2022 Union Budget, the government announced a *National Digital University* (sometimes called Digital University) to

provide “world-class quality universal education” online. The envisioned model uses a **hub-and-spoke network**: premier public universities and institutes act as “spokes” under a central hub of cutting-edge ICT expertise. The NDU is to offer personalized, multilingual courses through ICT platforms, with extensive stakeholder consultations (UGC, AICTE, MoE departments, NIELIT, etc.) carried out to design its structure. This national initiative aims to democratize access to top-quality courses across India via digital means.

8.3 AI Governance Framework

- **NITI Aayog’s “AI for All” Strategy (2018)²⁶**: The government’s flagship AI strategy (brandname #AIforAll) identifies inclusive growth through AI. It spotlights five priority sectors (Healthcare, Agriculture, Education, Smart Cities, Smart Mobility) where AI can solve major challenge. The document stresses that India should leverage its data and talent to become an AI leader for the Global South. It also acknowledges key barriers: lack of high-quality data ecosystems (data access), insufficient AI expertise, and privacy/security gaps due to weak regulations. The strategy thus advocates building data repositories, AI research centers, and capacity-building (e.g. Centres of Research Excellence and AI application labs) to overcome these challenges.
- **Responsible AI Reports²⁷**: In 2021 NITI Aayog released a two-part approach on “*Responsible AI*”, developed with the World Economic Forum. This work articulates core ethical principles for Indian AI: for example, **Privacy & Security** (data used only by authorized entities with strong safeguards), **Transparency** (AI systems should be explainable and auditable), **Accountability** (stakeholders in design and deployment remain answerable for outcomes) among others. These principles (echoing global “FATE” standards) are meant to guide government, industry and academia. The papers encourage institutions to adopt bias-mitigation, human-centric design, and grievance-redress mechanisms. In sum, India’s Responsible AI framework applies constitutional values (non-discrimination, dignity) to guide AI governance.
- **IndiaAI Mission (2024)²⁹**: The Cabinet approved an ambitious IndiaAI Mission (“Making AI in India and Making AI Work for India”) with a ₹10,372 crore budget over five years. Implemented by a new IndiaAI hub (MeitY), the mission has already deployed over 38,000 high-end GPUs (up from an initial target of 10,000) to democratize compute access at subsidized rates. Its seven “pillars” include: (1) **Compute Pillar** – subsidized AI compute infrastructure (GPUs at ~₹65/hour); (2) **AI**

for India-specific Applications – developing AI tools for healthcare, agriculture, education, etc. (30 applications approved by mid-2025); (3) **AIKosh** – a unified government data platform (now hosting thousands of anonymized datasets and models) to fuel AI innovation; (4) **Foundation Models** – creating indigenous large multimodal AI models using Indian data and languages, to ensure sovereign AI capabilities; (5) **FutureSkills** – training AI talent via funded PhDs and courses (hundreds of AI fellowships awarded by 2025); plus other pillars for startup incubation and sectoral pilots. Together, these initiatives aim to build a homegrown AI ecosystem and infrastructure.

8.4 Data Sovereignty and Digital Colonialism

- **National Data Governance Framework (2022 Draft)³⁰**: The government's draft NDGF Policy treats non-personal government data as a national resource. It proposes an India Data Management Office (IDMO) and controlled data platforms so that anonymized non-personal data sharing happens only via approved Indian repositories. The policy's objectives include standardized whole-of-government data practices, interoperable APIs, and open digital platforms for data access – all while ensuring “*privacy, safety and trust*”. In effect, it centralizes public data for use in AI and governance (e.g. expanding the “India Datasets” program) but restricts foreign transfers: any non-personal data export must go through IDMO-certified channels. This framework reflects a data-sovereignty approach by keeping control of large data pools within India.
- **Open/Public Data Initiatives³¹**: Beyond policy drafts, India has built extensive **digital public infrastructure** (Aadhaar identity system, UPI payments, digitized land/tax records, etc.) which serve as de facto public data commons. Data.gov.in (Open Government Data platform) and the Digital Public Goods Alliance further promote accessible government datasets. These initiatives aim to ensure that valuable data (on citizens, economy and resources) benefit Indian stakeholders and innovators rather than being siphoned abroad.
- **Sovereign AI Infrastructure**: The IndiaAI Mission's pillars reinforce sovereignty: notably the **Foundation Models** pillar seeks Indian-created AI models on local languages. By funding domestic LLM development, the government is reducing reliance on foreign AI platforms and intellectual property. Similarly, the proliferation of affordable GPU farms and AI compute (38,000 GPUs) builds indigenous capacity so

that key AI training/inference happens within national infrastructure. These steps strengthen “sovereign” AI ecosystems.

- **Cross-Border Data and Privacy:** Under the DPDP Act, India explicitly preserved cross-border controls: the law applies to any processing of Indian residents’ data (even by foreign companies). It also authorizes the government to notify countries to which data flows can or cannot go, effectively letting India block transfers deemed risky. Historically, India has already imposed localization for certain data categories (in financial services, health, etc.). As noted by policy analysts, India “*has actively advanced data sovereignty through localization mandates requiring certain categories of data to be stored domestically*”. In the education/AI context, this means data generated by students or academic institutions must often remain under Indian jurisdiction and subject to local regulation.

9. International Legal Framework: Comparative Analysis

9.1 UNESCO Ethics and Education Frameworks.³²

UNESCO’s 2021 *Recommendation on the Ethics of AI* sets broad, human-rights-based norms: e.g. it emphasizes **transparency** (“understandable decisions and outcomes”), **fairness/non-discrimination** (avoiding bias against any group), **accountability** and **data privacy**. It also calls for multi-stakeholder governance and inclusiveness. Likewise, the 2019 *Beijing Consensus on AI and Education* stresses that AI in schools must support **SDG 4** and equity: it warns that AI “**should not deepen the digital divide**” or bias against minorities. It urges ethical, privacy-by-design data use in education. These UNESCO texts promote *human-centered AI* in education (mandating inclusion, culturally aware curricula, teacher training, and respect for linguistic diversity). However, they remain **aspirational and universal**. They scarcely grapple with Global South realities: for example, while Principle 10 of the UNESCO Ethics Recommendation asserts that “States shall be able to regulate the data generated within or passing through their territories”, it offers no concrete mechanisms to counteract infrastructure dependency on foreign cloud services. In practice, UNESCO’s call for cultural diversity and participation means little if local systems lack data control or technical capacity.

9.2 OECD Principles (2019)³⁴.

The OECD’s *AI Principles* promote “innovative and trustworthy AI” that respects rights and democratic values. They emphasize values familiar from UNESCO: e.g. AI should enhance sustainable growth and “the well-being of people” while ensuring **fairness, transparency and**

explainability. Indeed, many non-OECD states nevertheless align with these principles as a soft-law benchmark. ASEAN, for instance, explicitly adopted ethics principles (“transparency, explainability, fairness and equity” etc.) that OECD notes are “closely aligned” with both its own Principles and UNESCO’s. Yet scholars caution that OECD norms reflect a **Global North perspective** that may not fit Global South contexts. One analysis observes that Western-centric prescriptions “are often rooted in Western perspectives... and may not translate easily” in different social settings. Another notes that many African countries “rely significantly on AI... produced by the Global North,” creating a technological dependence that OECD-style guidance does little to redress. In sum, OECD’s framework supplies a common vocabulary but essentially cements a Northern model of AI governance, with limited Global South agency.

9.3 EU AI Act (2024).³⁵

The EU’s new *Artificial Intelligence Act* is the first **binding, risk-based AI law**. Its stated goal is to create a “uniform legal framework... to promote human-centric and trustworthy AI”. The Act categorizes AI systems by risk: for example, many educational applications (e.g. admission/screening systems, adaptive learning assessments, exam monitoring or proctoring, student behavior tracking) are listed as **high-risk**. Providers of such systems must comply with strict requirements (impact assessments, technical documentation, human oversight, robustness, etc.). The Act even **prohibits** certain uses: e.g. *any* AI that “infers the emotional state of a person in educational institutions” is banned (unless for medical/safety reasons). It also imposes broad **transparency** rules: all “limited-risk” AI (like chatbots or deepfakes) must disclose to users that they are interacting with an AI. Crucially, the EU Act has **extraterritorial scope**: it applies to high-risk systems marketed or used *in* the EU regardless of where the provider is based. This means global edtech firms must follow EU rules even outside Europe. By effectively exporting EU standards (a classic “Brussels Effect”), the Act will shape AI governance worldwide. For the Global South, this can cut both ways: it raises the bar for student data protection and fairness, but it also forces compliance with a Northern regime.

9.4 Council of Europe AI Convention (2024).³⁶

The new CoE *Framework Convention on AI* is a legally binding treaty (opened September 2024) anchoring AI in **human rights, democracy and the rule of law**. Rather than focusing on specific tech uses, it embeds broad principles: *legality, necessity, proportionality, transparency, accountability, non-discrimination, human dignity*. It covers AI use by both states and private actors whenever fundamental rights or democratic values are at stake. The

Convention requires signatory states to enact laws that define permitted AI uses, establish oversight (e.g. by data protection authorities or courts), and ensure redress. For high-risk domains (including many public services), governments must conduct mandatory human-rights impact assessments and safeguards before deployment. Notably, unlike the EU Act's risk-regime, the CoE treaty does *not* impose blanket bans on entire technologies; for example, it allows biometric ID if that use is justified, proportionate and strictly regulated. In essence, it provides a **rights-based** layer across Europe and beyond – one that complements the EU Act's technical rules, but so far has been largely a European exercise.

9.5 UN Global Digital Compact (2024)³⁷.

The UN's new Global Digital Compact (GDC) is a non-binding vision document aiming to galvanize multilateral action on digital issues. On AI and data, it is notably **inclusive**: Objective 5 explicitly calls for a “balanced, inclusive and risk-based approach” to AI governance with “full and equal representation of all countries, especially developing countries”. The GDC acknowledges glaring **digital divides**, stating that closing them is vital for everyone's benefit and that “these divides pose challenges for many countries, in particular developing countries... which have pressing development needs and limited resources”. It endorses UNESCO's recommendation and human-rights law as guiding frameworks and commits to harnessing AI for the SDGs (e.g. supporting diverse languages and locally generated data). Critically, it calls for concrete cooperation: building AI capacity and infrastructure in the Global South, promoting open models and data-sharing, and encouraging North-South/South-South partnerships. For example, it urges the UN system to help developing countries build AI skills, data sets and affordable compute, and to facilitate international standards and best-practice sharing. In sum, the Compact explicitly highlights inequality and capacity gaps, and calls for international support. However, as a compact it remains aspirational – the real test is whether powerful states and firms follow through.

9.6 African Union (AU) Strategies.³⁸

The AU has moved beyond rhetoric: its *Continental AI Strategy* (2024) is explicitly “Africa-centric, development-oriented and inclusive”. It prioritizes harnessing AI's benefits for citizens (in line with Agenda 2063) while minimizing risks (bias, disinformation, privacy violations, etc.). Crucially, it underscores **sovereignty**: e.g. the African Research Centre for AI (ARCAI) exists to “ensure Africa's sovereignty over modern digital tools”. The AU Strategy candidly notes Africa's disadvantages: only ~1.8% of the world's large data centers are in Africa, and

many countries lack the bandwidth or rules to use international cloud resources (“lack of adequate bandwidth and data sovereignty regulations” hinders AI experimentation). It warns that AI solutions developed elsewhere – and foreign-controlled data – “may undermine national sovereignty, Pan-African values and civil liberties” To counter this, the AU Strategy calls for massive investment in local **infrastructure** (green data centers, broadband) and skills, and for legal frameworks to protect against algorithmic bias. Its companion *Digital Transformation Strategy (2020–2030)* similarly champions infrastructure and data. For example, it explicitly promotes building continental data centers and insists that “soon it will be necessary to ensure localization of all personal data of Africa’s citizens”. It also advocates open data policies to spur African entrepreneurship. Overall, the AU documents recognize both the *promise* of AI (jobs, services, social progress) and the risk of digital dependency – and they set a development agenda accordingly. Implementation will be the challenge, but these strategies are among the most concrete Global South plans for asserting data sovereignty and algorithmic governance.

9.7 ASEAN Guide on AI (2021/24).³⁹

Southeast Asia’s *ASEAN Guide on AI Governance and Ethics* is a soft-law *practical guide* (endorsed end-2023) for ASEAN members. It articulates seven core principles – **transparency & explainability, fairness & equity, security & safety, robustness, human-centricity, privacy & data governance, accountability & integrity** – and stresses **regional alignment** of national policies. Like OECD/UNESCO, it urges risk assessments and multi-disciplinary oversight (e.g. national AI ethics boards). It also recommends building AI talent, infrastructure, and regulatory capacity. In essence, ASEAN’s framework echoes the language of OECD/UNESCO (indeed, it *aligns* with those) and aims to foster interoperability between countries. The Guide is notable for its emphasis on “human-centric” AI and education (the title even emphasizes **Governance and Ethics**), reflecting Asian values of social harmony. But as a voluntary guideline it carries no enforcement. It omits any mention of restricting data flows or platform dependency. In practice, ASEAN states (like others) still rely heavily on foreign cloud providers and imported AI platforms. Thus, while the Guide signals a regional consensus on AI principles, it remains modest on hard issues like data sovereignty or decolonizing algorithmic power.

9.8 Latin American initiatives.⁴⁰

Latin American governments likewise seek South–South approaches. UNESCO’s *LAC AI in Education Observatory* (launched 2024) unites all 33 Ministries of Education in the region. It

operates on the motto “AI cannot govern education; education must govern AI,” reflecting UNESCO’s ethos. It aims to gather evidence, build capacity, and ensure that AI in classrooms serves equity and local learning needs. Alongside this, the CEPAL-ILIA Index (2025) provides a detailed governance snapshot: it shows **critical gaps** in talent and infrastructure. For example, 90% of Latin America’s supercomputing capacity is in Brazil, and most countries have almost no high-performance AI compute or local data centers. The ILIA report⁴¹ also notes that open-source AI is emerging as a democratizing force (e.g. Honduras, Cuba excel in open-source development) which can help “generate solutions tailored to local realities”. These findings echo the UNESCO mandates on inclusivity and diversity. In practice, the region has less formal binding law than the EU, but these observatories and indices help Latin American countries share best practices and advocate collectively – for example, by pushing for data localization or funding regional AI infrastructure.

10. Recommendations

10.1 International Governance Recommendations

- 1. Global South Representation in AI Governance:** AI governance is currently dominated by OECD/EU agendas and private tech actors. Studies note that most global AI ethics documents have been led by industry, with under-representation of Global South voices⁴². Moreover, fragmented forums and overlapping agendas have “resulted in diminished participation from Global South stakeholders” in global AI policymaking⁴³. To counter this, we recommend formal mechanisms to ensure Global South leadership: for example, mandating Global South seats in emerging UN-led AI dialogues, and creating dedicated South-led bodies. UNESCO or the UN could establish a **Global South AI Council** and an international **AI-in-Education Observatory** that collects data on educational AI deployment. Such transnational platforms (modelled on UNESCO’s AI Ethics Observatory) would enable South–South cooperation and ensure that the Global South co-authors AI treaties and norms. These bodies should be empowered to negotiate AI agreements (akin to an “Educational AI Convention”) that reflect southern priorities (data sovereignty, equitable access, etc.). In short, strengthening UN-anchored processes and inclusive multi-stakeholder forums is crucial to “make a common voice reach other spaces”^{[42][43]}.
- 2. Cross-Border Educational Data Regulation:** We urge international agreements to classify educational data as a sensitive category and to establish norms for its transfer. Unlike health data (widely acknowledged as sensitive), educational data often lack

strong protections despite their growing scale⁴⁶. For example, biometric proctoring and learning analytics in Global South universities are routinely processed on foreign servers, raising data-extraction concerns⁴⁵. Global safeguards should require that cross-border flows of student and institutional data meet high standards of consent, privacy and security. Possible steps include extending GDPR-like **Adequacy Mechanisms** to cover education AI, and encouraging countries (as India's DPDP Act and South Africa's PDP Bill do) to impose localization for government-held or sensitive educational data. The African Union's Data Policy Framework, for instance, emphasizes sovereignty of data governance and has begun exploring regional data pools⁴⁷. We recommend that international bodies (UNESCO/ITU/OECD) include education-specific data safeguards – e.g. obliging EdTech vendors to store critical data locally or in certified jurisdictions, and to obtain special approvals for cross-border transfers. Classifying educational records as “sensitive” under national laws would enforce stricter export controls. Such measures would build on existing frameworks (EU adequacy, India's DPDP, AU strategies) and treat educational data as a **sovereign resource** requiring extra protection.

10.2 National-Level Recommendations

- 1. Educational AI Regulation Statute:** Countries should enact a comprehensive “Educational AI Accountability Framework” to govern all AI tools in higher education. This statute should require routine *algorithmic audits*, explainability and bias testing for any AI used in universities (e.g. automated grading, admissions screening, or learning analytics). Transparency obligations would compel institutions to disclose the use of AI (e.g. notifying students when essays are AI-graded) and maintain documentation of the algorithms. The law should provide clear student grievance mechanisms for AI harms and require impact assessments before procurement of new AI systems. For example, taking cues from the EU AI Act, all high-risk systems (such as automated admissions or proctoring software) must undergo pre-deployment risk assessments⁴⁸. Embedding these requirements in law – rather than voluntary policy – ensures accountability. Procurement rules should forbid unassessed “black-box” tools: governments and universities must demand *algorithmic due diligence* from vendors (third-party audits, open code inspection, etc.). In practice, this means, for instance, requiring that any AI-based proctoring system be certified for privacy, anti-bias performance, and explainability before use. By codifying explainability, fairness and

oversight into an AI in Education statute, countries can turn abstract ethics into enforceable rights for students.

2. **Data Sovereignty Measures:** Governments should invest in indigenous digital infrastructure and declare educational data a strategic national asset. This means building local **education data clouds** and encouraging domestic AI models trained on nationally representative curricula. For example, the African Union’s 2024 Digital Transformation Strategy explicitly identifies “AI sovereignty” and reducing reliance on foreign infrastructure as a goal⁴⁹. Likewise, countries could mandate that public universities host their learning-management and assessment systems on national data centres (or approved cloud platforms). Sovereign cloud infrastructure would keep educational records under local control. Beyond storage, states should support the development of *home-grown AI models* for education (e.g. state-sponsored LLMs in local languages or open educational datasets) rather than outsourcing to global tech firms. Framing educational data as a *decolonial asset*, policy must require that any foreign-operated platform comply with local data protection law and, ideally, involve co-ownership of data. Taken together, these steps – local clouds, sovereign AI, public digital infrastructure – safeguard autonomy. Governments should articulate an explicit **decolonial strategy**, treating student data and academic outputs as a sovereign resource (not a free commodity). This could involve, for example, classifying national higher-education databases under special legal protection and prohibiting their untrusted foreign use.
3. **Public-Interest AI Funding:** To counter epistemic colonialism, states should directly invest in open, multilingual educational AI. This can take the form of publicly funded *multilingual language models* and datasets. For instance, supporting projects like the open-access BLOOM LLM (with 176B parameters across many languages⁵⁰) or building similar models in under-represented languages. Governments can fund the creation of national corpora (literature, lecture transcripts, exam archives) so that AI reflects local knowledge. In practice, this means financing university consortia to curate Indigenous studies datasets, or underwrite regional AI labs like AfricaNLP. Open educational platforms (with public grants) can promote AI ecosystems free from proprietary lock-in. In addition, scholarships and grants should nurture a domestic AI R&D workforce: e.g. programs for Indian, African or Latin American AI researchers to develop new pedagogy tools. Such public investment not only fosters digital sovereignty but also enriches the global commons. By funding models with broad

accessibility (open-source licenses, free APIs for schools), governments counteract the dominance of Western LLMs and ensure AI research addresses local curricula and languages.

10.3 University-Level Recommendations

- 1. AI Governance Boards:** Universities should establish formal AI oversight structures: ethics committees or AI review boards with faculty, student and external participation. These bodies would vet new AI deployments (e.g. approving a shift to automated grading) and continuously monitor compliance with the Accountability Framework. Importantly, students and marginalized community representatives must sit on these boards to ensure diverse perspectives. Research on Global South AI policy emphasizes inclusive participation: “it will be necessary to include those who are most affected by AI developments... [or risk] leaving relevant perspectives invisible”⁴⁴. In practice, a university’s AI Committee could require all AI projects (research or administrative) to be registered and reviewed; it could also sanction vendors that fail to meet transparency standards. These governance boards serve as a grassroots check on opaque AI – a place to raise grievances and seek remedies. Universities might also create a Student AI Ombudsperson office for reporting issues. Overall, institutionalizing AI ethics oversight ensures that critical questions (privacy, bias, pedagogical impact) are addressed before and after new technologies are introduced.
- 2. Mandatory AI Transparency Policies:** Academic institutions must adopt policies requiring disclosure whenever AI is used in student evaluation or surveillance. For example, if a course uses automated essay scoring or predictive analytics for student success, the syllabus and student code of conduct must explicitly state this usage. Similarly, any use of facial-recognition or behavior-monitoring software in proctoring exams must be publicly documented. The EU AI Act already classifies many educational AI uses as “high risk” (e.g. determining admissions or evaluating learning outcomes⁵¹). Universities should mirror this by enforcing transparency: students should have the right to know if an algorithm is grading them, and the basis of its decisions. Practically, universities can publish “Algorithmic Registers” listing all deployed AI tools and linking to their audit reports. Surveillance and analytics systems (attendance trackers, engagement monitors) should require opt-in consent and provide students with the logic of any decisions (e.g. why a student was flagged). By making automated processes visible, institutions uphold accountability and allow community oversight. In

short, mandatory transparency (with clear policies and accessible disclosures) is a basic safeguard to demystify educational AI.

3. **Algorithmic Impact Assessments:** Drawing on the EU AI Act and human-rights frameworks, every new AI system in a university should undergo a formal impact assessment for discrimination, linguistic bias, privacy harms and accessibility. Borrowing the EU model, this means analyzing worst-case scenarios of the system and documenting mitigation plans. For instance, before approving a new AI-driven admissions tool, the university would test its decision criteria across gender, ethnicity, language groups, and check for unequal false positives. The assessment should also evaluate cultural fit: does the AI reinforce only English-language resources, or neglect local knowledge contexts? (As the literature warns, Western-trained AIs “encode cultural and linguistic biases” and undervalue non-Western academic traditions⁵¹.) Impact assessments would cover how personal student data flows, ensuring privacy safeguards. Accessibility checks (e.g. compatibility with assistive technologies) must also be part of the review. Universities can adapt existing Human Rights Impact Assessment guides to this context. Publishing summary results of these assessments (with redacted details) would inform the campus community and external regulators. Embedding rigorous impact evaluation makes AI adoption much more sophisticated – it shifts the focus from blindly using “innovative” tech to carefully safeguarding educational equity and rights.

10.4 Pedagogical Recommendations

1. **Decolonial AI Pedagogy:** Curricula should teach *critical AI literacy* and integrate local knowledge traditions. Students need not only technical skills but also an understanding of AI’s cultural biases and power dynamics. Educators can introduce exercises (e.g. as Bhusal (2025) demonstrates) where students use AI tools like ChatGPT to compare responses in their mother tongues versus English⁵². This promotes multilingual and multicultural perspectives. We recommend developing AI-assisted learning materials in local languages, and including case studies of AI impacts in Global South contexts. Crucially, AI literacy must be framed as “not neutral” – students should analyze how training data and algorithms can marginalize non-Western voices. AI tools should be taught as **instruments**, not authorities: educators can use them to enrich diverse curricula (e.g. generating examples from indigenous texts, simulating dialogue in vernacular), always with teacher supervision. By foregrounding local epistemologies

and encouraging students to question AI outputs, pedagogy becomes decolonial. Multilingual AI platforms should be incorporated so that all learners can engage with AI in familiar languages. In sum, developing critical thinking about AI, and weaving local culture into AI education, empowers learners to reclaim knowledge rather than passively consume Western-centric content.

- 2. Human-in-the-Loop Educational Systems:** AI should assist educators, not replace them. Aligning with UNESCO's human-centered approach, any classroom AI must augment teacher decision-making and creativity⁵³. For instance, an AI tutor that suggests personalized exercises should leave the teacher in control of final lesson plans. Pedagogical AI systems should be designed with clear teacher oversight checkpoints. In practice, this means: maintaining easy ways for teachers to override or correct an AI's output; requiring that automated grading systems allow manual review; and ensuring that the educator is always the "responsible user" of any AI tool. International guidance stresses that AI "should complement, not replace, the vital roles of teachers in education"⁵³. Thus, professional development should train teachers as AI-interpreters, not as absentee overseers. For example, schools might adopt *semi-automated grading*, where AI generates initial feedback but a teacher validates it. This human-in-the-loop model preserves the social and ethical dimension of teaching. By emphasizing AI as a tool to relieve routine tasks (e.g. auto-tagging of exam questions) while keeping educators central, we resist purely algorithmic pedagogy and reinforce human values in learning.

10.5 Technical Recommendations

- 1. Open-Source AI Ecosystems:** We strongly advocate building on open-source AI platforms. Open-source models (e.g. BLOOM, LLaMA, community-driven tools) reduce dependency on Western tech monopolies and enhance transparency. Studies highlight that open models can be **adapted to local cultures and languages** much more easily and avoid vendor lock-in⁵⁴. For example, an open LLM can be fine-tuned on African literature or Indigenous knowledge, whereas closed systems rarely support such customization. Governments and universities should support the use of open frameworks (Hugging Face, OpenAI open licenses, etc.) and contribute to them. This includes hosting open model hubs for education and funding open-source research. Open ecosystems also invite local developers into the loop, which builds capacity. Internationally, promoting open standards and requiring model cards (detailed

documentation) can improve safety and accountability. Overall, investing in open AI (both code and data) not only democratizes innovation but also makes algorithmic decision-making visible and contestable by scholars and students.

2. **Bias Auditing and Dataset Diversification:** Finally, continuous bias audits and richer training data are essential. AI tools must be tested in the field for fairness across demographics and languages. Universities can partner with civil society to conduct periodic audits of campus AI systems (e.g. using synthetic tests for gender/racial bias in admissions algorithms). Any detected bias should trigger system retraining or decommissioning. Alongside, efforts should be made to diversify AI training corpora: collect local language texts, cultural content and images so that models are not solely Western-centric. For instance, educational datasets should include examples from the country's history, literature and examples in vernaculars. The literature warns that Western-trained AI "encodes cultural and linguistic biases" and undervalues non-Western traditions⁴⁹ – we must counter this by expanding representation. In practice, this means allocating funds to gather and annotate under-represented data (e.g. digitalize rural classroom interactions, record lectures in multiple languages). Periodic bias audits would use techniques from fairness research to quantify disparities (e.g. differing error rates by language or gender). By institutionalizing these technical checks, universities and policy-makers make sure AI tools evolve toward equity, not away from it.

11. Conclusion

This paper has shown that the increasing use of AI in higher education is not merely a question of innovation or administrative efficiency; it is also a question of power, control, and sovereignty. Through the lenses of digital colonialism, data sovereignty, and algorithmic governance, the analysis demonstrates that universities in the Global South often become dependent on foreign-owned infrastructures, proprietary platforms, and English-centric AI systems that shape what is taught, how it is assessed, and whose knowledge is made visible. In that process, AI can reproduce old hierarchies in new digital forms, affecting privacy, equality, cultural rights, academic freedom, and even cognitive autonomy. The paper's case studies and rights-based analysis therefore make clear that AI in education cannot be treated as a neutral tool, because its design and deployment are deeply tied to structural dependency and epistemic exclusion.

At the same time, the paper is not anti-technology. Its central message is that AI can serve

higher education in genuinely transformative ways if it is governed on decolonial and public-interest terms. The legal, institutional, technical, and pedagogical recommendations point toward a more balanced future: sovereign digital infrastructure, stronger accountability, open-source and multilingual systems, meaningful human oversight, and greater Global South participation in global norm-making. If these measures are pursued seriously, AI could help expand access, support diverse learners, and improve educational quality without sacrificing autonomy or justice. The most promising future for AI in higher education, therefore, is one in which universities do not simply adopt AI, but actively shape it so that it serves local knowledge, democratic governance, and the broader project of educational self-determination.

References

1. Kwame Nkrumah, *Neo-Colonialism: The Last Stage of Imperialism* (1965).
2. Aníbal Quijano, “Coloniality of Power, Eurocentrism and Latin America” (2000).
3. Walter D. Mignolo, *The Darker Side of Western Modernity* (2011).
4. Michael Kwet, “Digital Colonialism: US Empire and the New Imperialism in the Global South” (2019). ([ResearchGate](#))
5. Miranda Fricker, *Epistemic Injustice* (2007).
6. Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press 2018).
7. Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Polity Press 2019).
8. Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
9. Digital Personal Data Protection Act, 2023 (India).
10. Regulation (EU) 2016/679 (GDPR).
11. Regulation (EU) 2024/1689 (EU AI Act).
12. UNESCO Recommendation on the Ethics of Artificial Intelligence (2021).
13. ICCPR, 1966.
14. ICESCR, 1966, Art. 13.
15. Committee on Economic, Social and Cultural Rights, General Comment No. 13 (1999).
16. UNESCO Convention on Cultural Diversity (2005).
17. UN Declaration on the Rights of Indigenous Peoples (2007).
18. Safiya Umoja Noble, *Algorithms of Oppression* (2018).
19. OpenAI, ‘California State University Expands Access to ChatGPT Edu’ (2025).
20. Reuters, ‘Google Commits \$1 Billion in AI Support for Universities’ (6 August 2025).

21. UNESCO, 'Two-Thirds of Higher Education Institutions Have or Are Developing Guidance on AI Use' (2025)..
22. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).
23. Government of India, *Information Technology Act, 2000*. Government of India, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*.
24. Ministry of Education, Government of India, *National Education Policy 2020*.
25. University Grants Commission, *University Grants Commission (Open and Distance Learning Programmes and Online Programmes) Regulations, 2020*.
26. NITI Aayog, *National Strategy for Artificial Intelligence: #AIForAll* (2018).
27. NITI Aayog, *Responsible AI for All: Approach Document* (2021).
28. NITI Aayog, *Operationalizing Principles for Responsible AI* (2021).
29. Ministry of Electronics and Information Technology, *IndiaAI Mission* (2024).
30. Ministry of Electronics and Information Technology, *National Data Governance Framework Policy (Draft), 2022*.
31. Government of India, *Open Government Data Platform (data.gov.in)*.
32. UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
33. UNESCO, *Beijing Consensus on Artificial Intelligence and Education* (2019).
34. OECD, *OECD Principles on Artificial Intelligence* (2019).
35. European Union, *Artificial Intelligence Act (Regulation (EU) 2024/1689)* (2024).
36. Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (2024).
37. United Nations, *Global Digital Compact* (2024).
38. African Union, *Continental Artificial Intelligence Strategy for Africa* (2024).
39. ASEAN, *ASEAN Guide on AI Governance and Ethics* (2024).
40. UNESCO, *Latin America and the Caribbean AI in Education Observatory* (2024).
41. ECLAC (CEPAL) & ILIA, *Latin American Artificial Intelligence Index (ILIA) Report* (2025).
42. Open Data Charter, *AI Governance for and from the Global South*
43. South Centre (2025), *Artificial Intelligence Governance and the Global South: Policy Brief No. 148*
44. Open Data Charter, *discussion on inclusive participation and Global South representation*.

45. *Frontiers in Education* (2026), *Algorithmic Dependence and Digital Colonialism: A Conceptual Framework for AI in Education and Knowledge Systems of the Global South* – educational data extraction and digital colonialism
46. UNICEF Innocenti, *Data Governance Manifesto* – educational data as a sensitive category
47. CSIS discussion of African Union AI strategy, regional data pools, and data sovereignty
48. European Union AI Act – education systems classified as high-risk AI applications
49. Same *Frontiers in Education* article – epistemic colonialism, cultural and linguistic bias
50. Same *Frontiers in Education* article – open-source AI initiatives such as BLOOM and Africa NLP
51. European Union AI Act – education systems classified as high-risk AI applications
52. Bhusal (2025), *Fostering Critical AI Literacy through a Decolonial Use of ChatGPT in ESL/EFL Classrooms*
53. UNESCO, *AI Competency Frameworks for Students and Teachers* – human-centered AI and teacher oversight
54. CSIS, *An Open Door: AI Innovation in the Global South amid Geostrategic Competition* – advantages of open-source AI