INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

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.

ISSN: 2582-6433

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

ISSN: 2582-6433

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.

ISSN: 2582-6433

DIGITAL COLONIALISM IN THE AGE OF ARTIFICIAL INTELLIGENCE: DATA OWNERSHIP, TECHNOLOGICAL DEPENDENCY AND STRUCTURAL INEQUALITY IN THE GLOBAL SOUTH

AUTHORED BY - ITUNGO JOAN
LLM Student,
University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.

CO-AUTHOR - DR. RAJIV BHALLA
University Professor,
University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

Abstract

The use of artificial intelligence has been a catalyst for a trend that has been dubbed "digital colonialism" the control of data, infrastructure and value by a handful of companies and states, mostly in the Global North, and increasingly in China. This paper will explore how this pattern works in three interwoven ways: extraction of data from populations in the Global South with weak or absent ownership rules; dependency on technology from the outside, such as cloud services, compute servers, and models; and structural inequality when AI systems developed in other parts of the world are applied to populations that are not theirs. The paper is doctrinal and comparative in nature and draws on evidence from the Kenyan, Ugandan, Rwandan, and Indian data protection regimes and the instruments of the African Union, to show that although individual consent data protection laws are necessary, they cannot alone solve a collective and economic problem. Enforcement is still sporadic, with courts and regulators beginning to chip away at it, as evidenced by the recent World coin ruling by the Kenyan High Court in 2025. The paper suggests that the elements of a credible digital sovereignty agenda are collective data rights, conditional localization with benefit-sharing, public compute investment, and labour standards for AI supply chains and South–South regulatory coordination.

Keywords: Digital Colonialism; Artificial Intelligence; Data Sovereignty; Global South; Data Protection; Technological Dependency.

ISSN: 2582-6433

I. Introduction

Colonial economies were characterized by a simple imbalance: raw materials came into the colony at a lower price, and came out as manufactured products at a much higher price. In the medium of artificial intelligence (AI) economy, it is a different asymmetry. The everyday communications of Africans, South Asians and Latin Americans are captured, stored and analyzed on a platform in another part of the globe, and re-presented back to them as a service, adverts, and automated decisions that cost them money. Kwame Nkrumah said that formal independence could exist alongside economic control from outside; this is the modern day version of that warning in the AI economy.[1]

The purpose of this paper is to address three questions. Esther's first question is, "How does data extraction in the AI era mimic the colonial mode of appropriation?" Second, are the laws of some Global South jurisdictions sufficiently addressing that extraction? Third, what reforms would help those jurisdictions to shift from dependency to real digital sovereignty? The method used is doctrinal and comparative. India is analyzed as a big digital economy and a proactive regulatory stance, and Kenya, Uganda and Rwanda are explored as newly enacted data protection laws in East African states. African Union (AU) instruments are considered as the main regional response.

II. Conceptualizing Digital Colonialism

It was the work of Couldry and Mejia's that has fully articulated the concept of "data colonialism," which they see as a new way of appropriation akin to historical colonialism.[2] Kwet has focused on ownership of the digital "ecosystem" itself and argues that ownership of software, hardware, and network connections equates to imperial power in the hands of United States companies over the Global South.[3] Both share Quijano's understanding that the "coloniality of power" persists after formal colonialism has ceased, thus creating a hierarchy of knowledge, labour and race.[4] Ricaurte then applies his analysis to data epistemologies, demonstrating that the idea of quantification of everything reflects the world view of the people who own the instruments of quantification.[5]

[1] Kwame Nkrumah, Neo-Colonialism: The Last Stage of Imperialism (Thomas Nelson & Sons, London, 1965).
[2] Nick Couldry and Ulises A. Mejias, The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism (Stanford University Press, Stanford, 2019).
[3] Michael Kwet, "Digital Colonialism: US Empire and the New Imperialism in the Global South" 60 Race & Class 3 (2019).
[4] Aníbal Quijano, "Coloniality of Power, Eurocentrism, and Latin America" 1 Nepantla: Views from South 533 (2000).
[5] Paola Ricaurte, "Data Epistemologies, The Coloniality of Power, and Resistance" 20 Television & New Media

ISSN: 2582-6433

Zuboff's description of surveillance capitalism focuses on the production of behavioral data as a profit motive, but is largely about citizens of rich, democratic nations.[6] The colonial lens brings geography and history. Birhane illustrates how AI systems brought into Africa under the guise of development can take the place of local knowledge and external values, something she calls algorithmic colonization.[7] The authors of the report, Mohamed, Png and Isaac, also cite algorithmic oppression, exploitation and dispossession as common occurrences in the use of AI outside the Global North.[8]

Digital colonialism is defined in this paper as a structural condition which consists of three elements: (a) the production of data from the Global South happens elsewhere and is captured and sold as data elsewhere; (b) technologies or tools that process the data of the Global South belong to the outside; and (c) the rules for producing and processing the data of the Global South are external to it. The statement is not intended to be a definition. No actor must have an intention of domination; it's an arrangement of ownership and dependency.

III. Data Ownership and the Extraction Economy

Most legal systems do not recognize property in personal data. Data protection laws on the other hand consider data subjects or data principals as the owners of rights of access, correction and erasure, and consent as the main access for lawful processing. But as Chander and Lê have pointed out, raw data nationalism can be counterproductive for developing economies, and the consent model has its drawbacks. Click-through consent is more of a legal fiction than a true option in the absence of digital literacy, economic necessity and language.[9]

The Kenya case is illustrative. In 2023, the project scanned the DNA of hundreds of thousands of Kenyans for cryptocurrency tokens. The Data Protection Act, 2019 in Kenya mandates that a Data Protection Impact Assessment (DPIA) be conducted prior to processing that may pose a high risk.[10] On May 5, 2025, in a lawsuit filed by the Katiba Institute and ICJ Kenya, the High Court at Nairobi ruled that the collection was illegal, that providing tokens in exchange for biometric information was not informed and freely given consent, and ordered the

350 (2019).

[6] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs, New York, 2019).

[7] Abeba Birhane, "Algorithmic Colonization of Africa" 17 SCRIPTed 389 (2020).

[8] Shakir Mohamed, Marie-Therese Png and William Isaac, "Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence" 33 Philosophy & Technology 659 (2020).

[9] Anupam Chander and Uyên P. Lê, "Data Nationalism" 64 Emory Law Journal 677 (2015).

[10] The Data Protection Act, 2019 (No. 24 of 2019) (Kenya), s. 31.

ISSN: 2582-6433

data to be deleted permanently under the supervision of the Data Protection Commissioner.[11] The judgment is important, but it's also been two years since the collection, and just because civil society litigated.

It is not always restrictive to respond to the extraction. India's digital public infrastructure public tools and systems for identity, payments and data-sharing shows the potential for a state to own and control the rails on which private services operate, retaining a stake in value and a stake in control at home. The model, of course, could be subject to its own dangers of state surveillance and exclusion, as the Aadhaar litigation revealed, but it demonstrates that technological isolation can be the end of the road for the alternative to foreign platform ownership.

A more fundamental difference is in aggregated and non-personal data (agricultural production, public health trends, mobility data, language corpora and the like). This data is frequently the most useful source for training AI systems but, once anonymized, it typically does not come under the scope of data protection law. India's Committee of Experts on Non-Personal Data observed this and recommended that communities should be seen as beneficial owners of the data generated by them and the data trustees should act on their behalf.[12] The proposal has not yet gone into effect. What this means is that the overall value that the population of the Global South creates is legally unowned and thus open to any entity who has the infrastructure to capture it.

IV. Technological Dependency: Infrastructure, Compute and Labour

If the power to analyze data is elsewhere, then so is the data. USA and China have a combined market capitalization of nearly 90 per cent of the world's seventy largest digital platforms and over 75 per cent of the cloud computing market, according to the United Nations Conference on Trade and Development (UNCTAD).[13] The report by its later, revealed that the two nations also account for approximately half the world's hyper scale data centers and accounted for 94 per cent of the funding of AI start-ups in the previous five years.[14] With the costs of compute power and specialized chips required to train frontier AI models out of reach

[11] "Kenya Court Rules Against Sam Altman's World, Orders Data Deletion and Halts Biometrics Collection"
[12] Ministry of Electronics and Information Technology, Report by the Committee of Experts on Non-Personal Data Governance Framework (Government of India, New Delhi, 2020).
[13] United Nations Conference on Trade and Development, Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries (United Nations, Geneva, 2019).
[14] United Nations Conference on Trade and Development, Digital Economy Report 2021: Cross-border Data Flows and Development: For Whom the Data Flow (United Nations, Geneva, 2021).

ISSN: 2582-6433

for most states, governments, universities, and companies in the Global South are paying other providers to use their services, and the terms remain out of their control.

It is also created at the point of accessing. The zero-rated services, which provide a selected platform for customers with no data charges, can direct first-time customers towards one company's platform. In 2016, India opted out of this model by repealing Facebook's Free Basics programme with a ruling from the Telecom Regulatory Authority of India that banned data discriminatory charges to the benefit of social media companies.[15] There are few developing countries that have made a similar move.

This dependence is strengthened by international trade law. The WTO had a moratorium on customs duties on electronic transmissions since 1998 and several countries, including South Africa, Indonesia and India, have doubted the revenue cost of such a moratorium as more goods and services go digital.[16] Plurilateral negotiations on digital trade also advance calls for free movement of data and restrict data localization and disclosure of source codes. Such agreements could also diminish the policy space available for developing countries to develop their domestic AI capacity, as the earlier trade agreements did with industrial policies.

The provision of AI is also like colonial trade. To make large models useful, they will need to be labelled with data and moderated for the content, tasks which are often outsourced to the Global South. In a recent investigation, the workers hired by a Kenyan outsourcing company to label toxic content for the artificial intelligence company OpenAI were paid less than $2 an hour.[17] The hidden workforce, as described by Gray and Suri, is called “ghost work”.[18] The same applies to the minerals on which AI hardware relies, says Crawford.[19] The Global South, therefore, provides raw data, raw labour and raw materials, and consumes the final product, while the platform owners collect rents.[20]

[15] Telecom Regulatory Authority of India, Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 (No. 2 of 2016), dated Feb. 8, 2016.
[16] World Trade Organization, Declaration on Global Electronic Commerce, WT/MIN(98)/DEC/2, adopted on May 20, 1998.
[17] Billy Perrigo, “Exclusive: OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic” Time (Jan. 18, 2023), available at: https://time.com/6247678/openai-chatgpt-kenya-workers/ (last visited on Nov. 13, 2026).
[18] Mary L. Gray and Siddharth Suri, Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass (Houghton Mifflin Harcourt, Boston, 2019).
[19] Kate Crawford, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence (Yale University Press, New Haven, 2021).
[20] Nick Srnicek, Platform Capitalism (Polity Press, Cambridge, 2017).

ISSN: 2582-6433

V. Structural Inequality and Algorithmic Harm

AI systems trained mainly on data from wealthy populations perform worse on those who are under-represented. Buolamwini and Gebru found that commercial gender-classification systems had error rates of up to 34.7 per cent for darker-skinned women, compared with 0.8 per cent for lighter-skinned men.[21] When such systems are deployed in credit scoring, identity verification or policing in Africa and South Asia, the cost of their errors falls on populations that had no say in their design. Languages spoken by hundreds of millions are poorly served by dominant models, which compounds exclusion from digital public services.

Inequality also extends to rule-making. The United Nations High-level Advisory Body on AI found that 118 countries were parties to none of the sampled international AI governance initiatives, while only seven, all from the Global North, were parties to all of them.[22] Developing countries therefore tend to become rule-takers, adopting standards shaped in Brussels or Washington through what Bradford calls the "Brussels Effect".[23] Regulatory transplantation is not inherently harmful, but it imports the priorities of jurisdictions whose central concern is individual privacy rather than collective economic development.

VI. Legal Responses in Selected Jurisdictions

India. The Supreme Court's recognition of privacy as a fundamental right under Article 21, including informational privacy, provides a constitutional foundation for data governance.[24] In the Aadhaar judgment the Court further restricted private entities from relying on the identity database.[25] The Digital Personal Data Protection Act, 2023 permits cross-border transfers except to countries the Central Government restricts by notification,[26] a marked retreat from the localization of critical data proposed by the Srikrishna Committee.[27] On the infrastructure side, the IndiaAI Mission approved in 2024 commits public funds to shared compute capacity and indigenous foundation models,[28] an explicit attempt to reduce dependency.

---

[21] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" 81 Proceedings of Machine Learning Research 77 (2018).

[22] United Nations High-level Advisory Body on Artificial Intelligence, Governing AI for Humanity: Final Report (United Nations, New York, 2024).

[23] Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford University Press, New York, 2020).

[24] *Justice K.S. Puttaswamy (Retd.)* v. *Union of India*, (2017) 10 SCC 1.

[25] *Justice K.S. Puttaswamy (Retd.)* v. *Union of India*, (2019) 1 SCC 1.

[26] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 16.

[27] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India, New Delhi, 2018).

[28] Press Information Bureau, Government of India, "Cabinet Approves Over Rs 10,300 Crore for IndiaAI

ISSN: 2582-6433

Kenya. Article 31 of the Constitution of Kenya, 2010 guarantees privacy, and the Data Protection Act, 2019 empowers the Cabinet Secretary to require that certain processing be carried out through servers and data centres located in Kenya on grounds of strategic interest.[29] The World coin judgment shows that the statute can be enforced against powerful foreign actors, though largely through litigation rather than proactive regulation.[30]

Uganda. Article 27 of the 1995 Constitution protects privacy, and the Data Protection and Privacy Act, 2019 permits processing outside Uganda only where the recipient country offers adequate protection or the data subject consents.[31] The framework is sound on paper, but the Personal Data Protection Office operates with limited resources, and consent can again serve as an easy route around the adequacy requirement.

Rwanda. Rwanda's Law No. 058/2021 makes the storage of personal data outside the country conditional on authorization by the supervisory authority, giving it one of the stronger localization regimes in East Africa, and its National AI Policy of 2023 links data governance to domestic capacity-building.[32]

African Union. The Malabo Convention on Cyber Security and Personal Data Protection entered into force on June 8, 2023.[33] The AU Data Policy Framework treats data as a shared continental resource and favors intra-African data flows,[34] and the Continental AI Strategy, endorsed by the AU Executive Council in Accra in July 2024, calls for an Africa-centric, development-oriented approach to AI.[35]

Taken together, these responses share three limitations. First, they are built on an individual-rights template that leaves collective and non-personal data unprotected. Second, localization powers are largely discretionary and rarely exercised. Third, none of the instruments addresses compute dependency or the labour conditions of AI supply chains, which are the economic core of digital colonialism.

Mission", Press Release dated Mar. 7, 2024.

[29] The Constitution of Kenya, 2010, art. 31; The Data Protection Act, 2019 (No. 24 of 2019) (Kenya), s. 50.

[30] *Supra note* 11.

[31] The Constitution of the Republic of Uganda, 1995, art. 27; The Data Protection and Privacy Act, 2019 (Act 9 of 2019) (Uganda), s. 19.

[32] Law No. 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy (Rwanda); Ministry of ICT and Innovation, The National AI Policy (Government of Rwanda, Kigali, 2023).

[33] African Union Convention on Cyber Security and Personal Data Protection, 2014, entered into force on June 8, 2023.

[34] African Union, AU Data Policy Framework (African Union Commission, Addis Ababa, 2022).

[35] African Union, Continental Artificial Intelligence Strategy: Harnessing AI for Africa's Development and Prosperity (African Union Commission, Addis Ababa, 2024), available at: via https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy (last visited on Nov. 13, 2026).

ISSN: 2582-6433

VII. Towards Digital Sovereignty: Recommendations.

Collective data rights. Legislatures need to acknowledge communities as beneficial owners of data created from them, which is part of the Indian non-personal data proposals[36], and on the CARE Principles for Indigenous Data Governance, which emphasize collective benefit and control.[37] Data trusts would be able to independently negotiate access on communities' behalf.

Conditions-based localization with benefits. Instead of generalization, states could demand access to high-value datasets in the fields of health, agriculture and language under licences that give some value back to the source community. The access and benefit-sharing model of the Nagoya Protocol provides a proven template.[38]

Open and public compute models. Public investment in shared compute is possible, as witnessed by the IndiaAI Mission. Such investment might be made collectively at the regional level on the African continent, under the AU strategy, with special focus on open models trained in local languages. It would also, as mentioned, provide universities and start-ups with a cheaper option than having to rent capacity from a few foreign providers, and enable the processing of sensitive public datasets according to domestic law.

Contextual impact assessment. Permit the deployment of high-risk AI systems in areas such as credit, health, policing, or identity verification only after deployment after testing the system on the local population and after publication of results. In the World-coin case, Kenya's data protection impact assessment is required, and this model can be expanded from data processing to algorithmic outcomes.

Labour standards for Data work. Labour law should expressly apply to outsourced annotation and moderation and public procurement of AI systems should include standards for minimum requirements for the data workforce.

Coordination and regulatory capacity between southern countries. Global South governments must collectively negotiate on forums that are responsible for digital trade and AI, and provide sufficient resources for the data protection authorities and ensure their independence. Rights that can't be enforced will have no impact on the structure described in this paper.

[36] *supra note* 12.
[37] Global Indigenous Data Alliance, CARE Principles for Indigenous Data Governance (2019).
[38] Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization to the Convention on Biological Diversity, 2010.

ISSN: 2582-6433

VIII. Conclusion

Digital colonialism is a description and not a metaphor for how value flows in the AI economy. Data come from the Global South, models, platforms and profits are elsewhere, and the rules are written mainly by the ones who benefit. Important protections have been put in place in these jurisdictions, and the Kenyan World-coin judgment demonstrates that courts will take action. However, the law, enacted on a basis of individual consent, can do nothing to change a structural imbalance. Collective data rights, benefit-sharing, public infrastructure, fair labour standards and coordinated diplomacy are essential aspects of real digital sovereignty. If these are absent, the Global South will be caught up in the same cycle of history it has been pursuing for decades in the land and resources domain – in data.

Bibliography

Books

Bradford, Anu, The Brussels Effect: How the European Union Rules the World (Oxford University Press, New York, 2020).

Couldry, Nick and Mejias, Ulises A., The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism (Stanford University Press, Stanford, 2019).

Crawford, Kate, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence (Yale University Press, New Haven, 2021).

Gray, Mary L. and Suri, Siddharth, Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass (Houghton Mifflin Harcourt, Boston, 2019).

Nkrumah, Kwame, Neo-Colonialism: The Last Stage of Imperialism (Thomas Nelson & Sons, London, 1965).

Srnicek, Nick, Platform Capitalism (Polity Press, Cambridge, 2017).

Zuboff, Shoshana, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs, New York, 2019).

Articles

Birhane, Abeba, "Algorithmic Colonization of Africa" 17 SCRIPTed 389 (2020).

Buolamwini, Joy and Gebru, Timnit, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" 81 Proceedings of Machine Learning Research 77 (2018).

Chander, Anupam and Lê, Uyên P., "Data Nationalism" 64 Emory Law Journal 677 (2015).

Kwet, Michael, "Digital Colonialism: US Empire and the New Imperialism in the Global

ISSN: 2582-6433

South" 60 Race & Class 3 (2019).

Mohamed, Shakir, Png, Marie-Therese and Isaac, William, "Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence" 33 Philosophy & Technology 659 (2020).

Quijano, Aníbal, "Coloniality of Power, Eurocentrism, and Latin America" 1 Nepantla: Views from South 533 (2000).

Ricaurte, Paola, "Data Epistemologies, The Coloniality of Power, and Resistance" 20 Television & New Media 350 (2019).

Reports and Policy Documents

African Union, AU Data Policy Framework (African Union Commission, Addis Ababa, 2022).

African Union, Continental Artificial Intelligence Strategy: Harnessing AI for Africa's Development and Prosperity (African Union Commission, Addis Ababa, 2024).

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India, New Delhi, 2018).

Global Indigenous Data Alliance, CARE Principles for Indigenous Data Governance (2019).

Ministry of Electronics and Information Technology, Report by the Committee of Experts on Non-Personal Data Governance Framework (Government of India, New Delhi, 2020).

Ministry of ICT and Innovation, The National AI Policy (Government of Rwanda, Kigali, 2023).

United Nations Conference on Trade and Development, Digital Economy Report 2019 (United Nations, Geneva, 2019).

United Nations Conference on Trade and Development, Digital Economy Report 2021 (United Nations, Geneva, 2021).

United Nations High-level Advisory Body on Artificial Intelligence, Governing AI for Humanity: Final Report (United Nations, New York, 2024).

Statutes, Regulations and Treaties

African Union Convention on Cyber Security and Personal Data Protection, 2014.

Law No. 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy (Rwanda).

Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization, 2010.

Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 (TRAI).

The Constitution of Kenya, 2010.

ISSN: 2582-6433

The Constitution of the Republic of Uganda, 1995.

The Data Protection Act, 2019 (No. 24 of 2019) (Kenya).

The Data Protection and Privacy Act, 2019 (Act 9 of 2019) (Uganda).

The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

World Trade Organization, Declaration on Global Electronic Commerce, WT/MIN(98)/DEC/2 (1998).

Cases

Justice K.S. Puttaswamy (Retd.) v. *Union of India*, (2017) 10 SCC 1.

Justice K.S. Puttaswamy (Retd.) v. *Union of India*, (2019) 1 SCC 1.

Online Sources

"Kenya Court Rules Against Sam Altman's World, Orders Data Deletion and Halts Biometrics Collection" The Block (May 6, 2025), available at: https://www.theblock.co/news/regulation/2025-05-06-kenya-court-rules-against-sam-altmans-world-orders-data-deletion-and-halts-biometrics-collection-353182 (last visited on Nov. 13, 2026).

Perrigo, Billy, "Exclusive: OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic" Time (Jan. 18, 2023), available at: https://time.com/6247678/openai-chatgpt-kenya-workers/ (last visited on Nov. 13, 2026).

Press Information Bureau, Government of India, "Cabinet Approves Over Rs 10,300 Crore for IndiaAI Mission", Press Release dated Mar. 7, 2024.