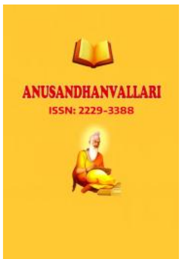


Anusandhanvallari
Vol 2024, No.1
December 2024
ISSN 2229-3388

Data Colonialism, Algorithmic Justice, and the Law: A Global South Perspective

[1]Saptaparni Raha, [2]Dr. Joydeb Patra

[1]Doctoral Research Scholar

School of Law

Brainware University

E-mail ID: saptaparniraha475@gmail.com

[2]Assistant Professor

School of Law

Brainware University

E-mail ID: joydebajoy@gmail.com

Corresponding Author: Dr Joydeb Patra, E-mail ID: joydebajoy@gmail.com

Abstract: The expansion of artificial intelligence (AI) and algorithmic governance has ushered in a new era of power relations defined by data. In the Global South, the intersection of historical legacies of colonialism, economic dependency, and weak legal frameworks has produced a landscape where data extraction and algorithmic control often replicate older forms of domination. This paper explores the concept of **data colonialism**—the systematic appropriation of personal, social, and communal data by global corporations and states—as a new frontier of imperialism. It examines how algorithmic systems, often designed in the Global North but deployed in the Global South, perpetuate structural inequalities, exacerbate surveillance, and challenge democratic and legal institutions. The notion of **algorithmic justice** is evaluated through sociological and legal lenses, considering questions of fairness, transparency, and accountability. Drawing on case studies from India, Africa, and Latin America, the paper highlights how algorithmic governance in welfare, finance, and criminal justice has disproportionately affected marginalized groups. Finally, it argues that algorithmic justice in the Global South requires both a rethinking of legal norms and a sociological re-engagement with postcolonial theory, emphasizing the need for local epistemologies, stronger regulatory frameworks, and global digital solidarity.

Keywords: Data Colonialism, Algorithmic Justice, Global South, Law, Postcolonialism

Introduction

The rapid advancement of artificial intelligence (AI) and algorithm-driven governance is reshaping the fabric of modern societies in unprecedented ways. Decisions that were once firmly within the discretion of human officials—such as welfare distribution, policing, or credit approval—are increasingly automated through predictive models, biometric authentication systems, and algorithmic profiling. Governments and corporations present these technologies as objective and efficient solutions to longstanding problems of bureaucracy, corruption, and inefficiency. Yet, beneath this promise lies a more troubling reality: algorithms are not neutral tools, but socio-technical systems that reflect and reproduce the inequalities embedded in the societies that create and deploy them.

For the Global South—encompassing Asia, Africa, Latin America, and parts of the Middle East—the consequences of algorithmic governance are even more complex. Here, the adoption of AI intersects with colonial histories, fragile democratic institutions, economic dependency, and weak regulatory safeguards. This intersection produces what scholars call a "new terrain of justice and sovereignty", where the challenges of fairness, accountability, and human rights are magnified by global inequalities.

AI-driven governance is often framed in terms of efficiency and scale. Predictive models allow police departments to identify "crime-prone" areas, biometric systems like fingerprints and iris scans ensure secure identification for welfare benefits, and algorithmic credit scoring expands financial services to those excluded from traditional banking. In theory, these systems minimize human error and corruption while accelerating service delivery.

However, these promises conceal critical risks. Algorithms often function as "black boxes," where the reasoning behind a decision is opaque even to their creators. This undermines due process and accountability. More importantly, because algorithms are trained on historical data, they often reproduce and magnify existing prejudices. Predictive policing in South Africa disproportionately targets Black communities, while in India, failures of biometric authentication in the Aadhaar system have excluded some of the poorest citizens from essential welfare programs. What emerges is a paradox: technologies meant to reduce inequality often end up deepening it.

To understand why these systems are particularly fraught in the Global South, the concept of data colonialism, developed by Nick Couldry and Ulises Mejias (2019), is crucial. Data colonialism describes how the extraction and commodification of data echoes the patterns of resource exploitation in classical colonialism. Just as imperial powers once seized land, labor, and raw materials from colonies, today's corporations and powerful states capture data—often from populations in the Global South—and convert it into profit.

This process operates on multiple levels. First, the South is a data source: billions of people are newly connected to the internet and digital platforms, generating vast amounts of personal information that flows to tech giants in the Global North. Second, the South serves as a testing ground for algorithmic technologies. India's Aadhaar project, the largest biometric identification system in the world, has become a model for similar projects elsewhere, despite widespread evidence of exclusion and privacy risks. In Africa, Chinese surveillance technologies have been exported under the Belt and Road Initiative, embedding powerful monitoring tools in fragile political contexts. In Latin America, algorithmic credit scoring has become widespread, using alternative data such as phone usage or social media activity—often without robust privacy safeguards.

The result is a global imbalance: the North dominates the design, ownership, and regulation of algorithmic systems, while the South bears the risks of experimentation, exploitation, and exclusion. This asymmetry brings us to the question of algorithmic justice. At its core, algorithmic justice seeks fairness, transparency, and accountability in how algorithms shape human lives. But it is not enough to view this issue only as a technical problem of "fixing bias" in code or datasets. Nor can it be treated merely as a legal problem of drafting privacy laws and data protection regulations. Algorithmic justice must be understood as a sociological and political struggle, situated in the broader structures of inequality, colonial legacies, and global capitalism.

Law, of course, plays a crucial role. Constitutional guarantees of equality and privacy, data protection acts, and international human rights frameworks all offer tools for resisting the most harmful effects of algorithmic governance. Yet, in the Global South, the law often lags behind technology. India's Digital Personal Data Protection Act (2023), Brazil's LGPD (2018), and Nigeria's NDPR (2019) all mark important steps, but enforcement remains weak, and these frameworks often borrow heavily from European models like the GDPR without addressing local realities. Moreover, national governments in the South are themselves complicit in data colonialism, as they rely on these technologies for governance, surveillance, and control.

Thus, algorithmic justice must be grounded in a broader rethinking of sovereignty and rights in the digital age. It requires acknowledging that algorithmic harm is not distributed equally: marginalized groups—whether women, racial minorities, lower castes, or the poor—are disproportionately affected. It also requires reimagining data governance beyond individual rights, incorporating community perspectives, indigenous epistemologies, and collective forms of data ownership.

1. Conceptualizing Data Colonialism

1.1 From Classical Colonialism to Data Colonialism

Classical colonialism involved the appropriation of land, labor, and resources by imperial powers, often legitimized by legal and religious frameworks. In contemporary times, **data colonialism** operates through the extraction of data from individuals, communities, and nations, facilitated by global corporations and states. Instead of occupying land, digital infrastructures occupy the **informational sphere**, capturing every aspect of human activity—from social interactions and consumer behavior to biometric and genomic information.

As Couldry and Mejias argue, data colonialism is not merely about surveillance or privacy but about the restructuring of society around continuous data extraction. Just as colonial powers once drew maps and censuses to control populations, today algorithms map digital behaviors, creating new regimes of governance and control.

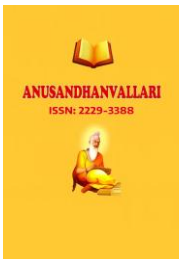
1.2 Global North–South Divide in Data Colonialism

The asymmetry between the Global North and South is stark. The North dominates the design of AI systems, cloud infrastructure, and intellectual property, while the South provides raw data, cheap labor for data annotation, and weakly regulated testing grounds. This mirrors the dependency structures of the colonial and postcolonial economy. For example, African nations often rely on Chinese or Western surveillance technologies, while Latin American data markets are dominated by U.S. corporations like Meta, Google, and Amazon.

2. Algorithmic Justice: Definitions and Challenges

Algorithmic justice refers to the equitable design, deployment, and regulation of algorithmic systems in ways that uphold principles of fairness, accountability, transparency, and non-discrimination. In today's data-driven world, algorithms play an increasingly central role in shaping access to services, opportunities, and rights. From welfare distribution and credit approval to law enforcement and border control, these systems now mediate crucial aspects of social and political life. While their proponents often claim that algorithms enhance efficiency and objectivity, the reality is far more complex. Algorithmic justice reminds us that technologies are never neutral; they are shaped by social contexts, economic structures, and political choices. Therefore, ensuring justice in algorithmic governance requires not only technical adjustments to reduce bias but also a deeper confrontation with the structural inequalities that these systems often reproduce or exacerbate.

At the heart of algorithmic justice lies the recognition that biases can operate at multiple levels. On the surface, there are **technical biases**, which arise when training data reflects the prejudices, exclusions, or imbalances of the societies from which it is drawn. For instance, if a crime prediction system is trained on historical policing data, and that data disproportionately reflects arrests of marginalized communities, the algorithm will inevitably "learn" to target those groups more heavily. On a deeper level, however, algorithmic systems are embedded in **structural inequalities**—those long-standing patterns of social hierarchy and domination based on race, caste, class, gender, and ethnicity. In societies of the Global South, where these inequalities are particularly pronounced due to histories of colonialism, economic dependency, and fragile legal safeguards, algorithmic governance often magnifies rather than mitigates injustice.



One clear example of this dynamic can be seen in the domain of **predictive policing in South Africa**. These systems are promoted as tools for crime prevention, capable of allocating police resources more efficiently by identifying "high-risk" areas or individuals. Yet, in practice, predictive policing disproportionately targets Black communities, echoing the racial biases of apartheid-era policing practices. The data used to train these systems is not neutral; it reflects decades of over-policing in Black neighborhoods, thereby reinforcing a cycle of criminalization. Instead of reducing crime, predictive policing risks entrenching racial profiling under the guise of technological objectivity. What appears as a rational and scientific allocation of resources is, in reality, an algorithmic perpetuation of racialized surveillance and control.

A second example is **India's Aadhaar biometric identification system**, which is the largest of its kind in the world. Launched with the aim of streamlining welfare distribution and reducing corruption, Aadhaar relies on fingerprint and iris scans to authenticate individuals before they can access services such as food rations, pensions, or healthcare. While the project has been celebrated for its scale and ambition, it has also been widely criticized for its failures. Biometric mismatches and authentication errors disproportionately affect the poor, elderly, and manual laborers—groups whose fingerprints may be worn out due to physical work. For these populations, a failed biometric scan can mean denial of essential food supplies or social benefits. Far from ensuring inclusion, Aadhaar has in many cases facilitated exclusion, highlighting how algorithmic systems can exacerbate vulnerability when deployed without adequate safeguards.

The issue is not confined to policing or welfare but extends to financial systems as well, particularly in **Latin America's algorithmic credit scoring practices**. Traditional banking institutions in the region have long excluded low-income populations due to lack of formal financial history or collateral. Algorithmic credit scoring was introduced as a supposed solution, using alternative data such as phone usage patterns, social media activity, or utility payments to assess creditworthiness. However, these systems often replicate structural disadvantages. Individuals who cannot afford stable internet access, who live in informal settlements without utility bills, or who rely on precarious forms of employment are systematically penalized. Instead of expanding financial inclusion, algorithmic scoring entrenches inequality by embedding socioeconomic hierarchies into automated decision-making. The result is that the very groups meant to benefit from technological innovation are rendered more vulnerable to exclusion and exploitation.

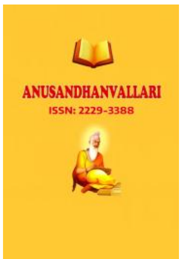
Taken together, these cases illustrate the urgent need for **algorithmic justice frameworks** in the Global South. The problem is not only that algorithms are technically flawed but also that they are being deployed in societies marked by profound inequality and weak legal protections. Without strong mechanisms for accountability, transparency, and redress, algorithmic systems risk legitimizing old hierarchies in new digital forms. More fundamentally, they reveal how the global promise of AI-driven governance is shaped by historical legacies of power: colonial domination, racialized surveillance, and economic exploitation.

Thus, algorithmic justice must be understood as both a technological and sociological project. On the one hand, it requires innovations in design, such as bias detection tools, explainable AI, and inclusive datasets. On the other hand, it demands structural reforms: stronger legal safeguards, participatory governance models, and recognition of the unique vulnerabilities faced by marginalized communities. Most importantly, algorithmic justice requires a decolonial perspective that situates technological development within global power relations. Only then can we move toward systems that not only minimize bias but also genuinely contribute to equity, dignity, and social justice.

2.3 Challenges for Justice

Algorithmic justice faces multiple obstacles:

1. **Opacity** – Proprietary algorithms are often "black boxes."



2. **Legal Lag** – Law develops more slowly than technology.
3. **Global Power Imbalances** – Corporations in the North shape global digital norms.
4. **Weak Local Institutions** – Legal safeguards in the Global South are often inadequate.

3. Legal Perspectives on Algorithmic Governance

3.1 International Legal Frameworks

Global debates on AI regulation are dominated by the EU, US, and China. The **EU AI Act** emphasizes risk-based regulation and fundamental rights, while the US approach focuses on innovation and self-regulation. However, there is little representation of Global South voices in these discussions.

3.2 Constitutional and Human Rights Dimensions

From a legal standpoint, algorithmic governance implicates core constitutional rights:

- **Right to equality and non-discrimination**
- **Right to privacy and data protection**
- **Right to due process and fair trial**

For instance, the Indian Supreme Court's *Puttaswamy v. Union of India* (2017) judgment recognized privacy as a fundamental right, but practical enforcement remains weak given the dominance of state and corporate data collection.

3.3 National Data Protection Laws

Some countries in the Global South have enacted data protection laws (e.g., Brazil's General Data Protection Law 2018, India's Digital Personal Data Protection Act 2023, Nigeria's NDPR 2019). However, enforcement capacity remains limited, and these frameworks often mirror European GDPR norms without addressing local sociological contexts.

4. Data Colonialism in the Global South: Case Studies

4.1 India: Aadhaar and Biometric Governance

India's Aadhaar project, the world's largest biometric ID system, has enrolled over a billion citizens. While intended to improve welfare delivery, it has also led to exclusion, especially among marginalized groups whose fingerprints or iris scans fail. Cases of starvation deaths linked to Aadhaar authentication failures illustrate how algorithmic governance can produce **lethal inequalities**. Moreover, private corporations have gained access to Aadhaar-linked databases, raising concerns about surveillance and profiteering.

4.2 Africa: Chinese Surveillance Infrastructure

Across Africa, China has exported AI-driven surveillance technologies under its "Digital Silk Road." From Ethiopia to Zimbabwe, facial recognition and monitoring systems are deployed ostensibly for security but often serve authoritarian purposes. Local populations rarely have a say in how their data is used, illustrating external domination reminiscent of colonial interventions.

4.3 Latin America: Algorithmic Finance

In countries like Mexico and Brazil, fintech companies use alternative data—social media activity, phone usage, geolocation—to generate credit scores. While this expands financial inclusion, it also risks predatory lending and deepens inequalities by penalizing those without digital footprints.

5. Sociological Dimensions: Power, Inequality, and Resistance

5.1 Postcolonial Theory and Algorithmic Power

Postcolonial theory provides a powerful lens for understanding the deeper implications of algorithmic governance and data colonialism. Scholars like **Frantz Fanon** and **Gayatri Chakravorty Spivak** remind us that colonial domination was not only about political control or economic exploitation but also about reshaping knowledge, culture, and subjectivity. Colonialism operated as a system of categorization, defining who was civilized and who was not, whose knowledge counted as legitimate, and whose voice was silenced. These insights help us see that algorithmic governance is not merely a technical or legal issue but fundamentally about power. Algorithms are not neutral—they encode values, assumptions, and priorities that reshape how individuals and groups are seen, classified, and managed by institutions.

In contemporary societies, especially in the Global South, algorithmic power takes the form of biometric surveillance, predictive policing, and welfare targeting systems. These technologies claim to create objective categories—such as "high risk," "eligible," or "fraudulent"—yet they often reproduce colonial legacies of control and exclusion. For example, digital identification systems like **Aadhaar in India** or biometric registries in African states extend state power into the most intimate aspects of life, while simultaneously privileging Western technological models over indigenous governance practices. Just as colonial rulers once redefined identities through censuses and maps, algorithmic systems today reorder populations into datafied categories that shape access to rights and resources. Postcolonial theory thus highlights how algorithmic power is not only about efficiency or security but about the creation of new forms of subjectivity and governance that mirror older patterns of domination.

5.2 Intersectionality and Algorithmic Harm

Algorithmic harms are not evenly distributed across society. Drawing on **intersectional theory**, pioneered by **Kimberlé Crenshaw**, it becomes clear that the effects of algorithmic governance are amplified for those who already face structural inequalities. Gender, caste, race, class, and indigeneity intersect to shape how individuals experience algorithmic systems. Women, lower castes, racial minorities, indigenous groups, and the poor are often disproportionately affected because algorithms reflect and reinforce existing social biases embedded in the data they are trained on.

Concrete examples from the Global South illustrate these dynamics. In India, caste-based surnames have been shown to influence algorithmic filters in hiring platforms, reproducing long-standing discrimination in new digital forms. Similarly, in Latin America, indigenous populations are subjected to biometric registration and surveillance projects without their free, prior, and informed consent. These systems often misrecognize indigenous features or fail to accommodate local cultural contexts, leading to exclusion from state services. In predictive policing, algorithms deployed in South Africa or Brazil disproportionately flag poor, Black, or marginalized neighborhoods as "crime hotspots," subjecting communities to intensified surveillance and criminalization.

The sociological lesson here is that algorithmic systems cannot be separated from the social hierarchies in which they operate. What may appear to be a neutral technological tool is, in practice, a mechanism that reinforces gendered, racial, caste-based, and class-based inequalities. Intersectionality reveals that algorithmic governance is not just about individual bias but about structural reproduction of oppression, where multiple dimensions of identity converge to amplify harm. This underscores the urgency of developing an algorithmic justice framework that centers the voices of those most affected rather than treating fairness as a universal technical standard.

5.3 Resistance and Digital Activism

Despite the formidable power of data colonialism and algorithmic governance, civil society in the Global South has not remained passive. Across different regions, activists, NGOs, and community organizations have mobilized to contest algorithmic harms and reclaim control over data. These movements represent more than isolated protests; they signal the emergence of **digital resistance** as a form of decolonial struggle.

In Kenya, activists and opposition groups challenged the government's biometric voter registration system, raising concerns about privacy, disenfranchisement, and electoral manipulation. Their campaigns highlighted how algorithmic tools, far from being neutral, can be weaponized to consolidate political power in fragile democracies. In India, a wide range of NGOs and advocacy networks have documented and campaigned against exclusions caused by Aadhaar-linked welfare systems. Reports of starvation deaths due to biometric failures became rallying points for legal and political challenges, forcing courts and policymakers to confront the human costs of digital governance. In Latin America, grassroots movements such as the **Latin American Initiative for Data Justice** have demanded community ownership of data and emphasized collective rights over individualistic, Western models of privacy. By framing data as a shared resource tied to cultural and territorial sovereignty, these movements challenge the very foundations of data colonialism.

These examples illustrate that resistance is not simply about rejecting technology but about **reclaiming epistemic and political agency**. A decolonial approach to algorithmic justice requires valuing local knowledge systems, alternative visions of data governance, and community-led decision-making. Activists argue that sovereignty in the digital age must extend beyond territorial borders to include sovereignty over data, algorithms, and technological futures. In this sense, digital activism is not merely defensive but also creative, offering new imaginaries of justice that resist domination and build solidarities across the Global South.

6. Rethinking Law and Justice in the Algorithmic Age

6.1 Beyond Legal Formalism

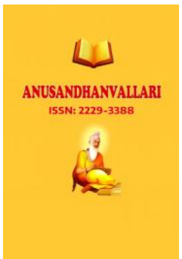
Traditional legal tools—such as data protection acts and constitutional rights—are necessary but insufficient. They often fail to address global asymmetries of power and the structural nature of data colonialism. Algorithmic justice requires a **sociologically informed legal approach** that recognizes power, inequality, and history.

6.2 Decolonial Legal Frameworks

Legal reforms in the Global South must avoid mere imitation of Northern models like the GDPR. Instead, they should embed local values, histories, and social contexts. For instance, indigenous perspectives on communal ownership of knowledge could inspire alternative models of **data commons**.

6.3 Global Digital Solidarity

Just as colonialism was resisted through anti-colonial solidarity, data colonialism requires transnational alliances. This includes South–South cooperation, demands for algorithmic accountability at the UN level, and rethinking intellectual property rights over data.



7. Conclusion

Data colonialism represents a new frontier of domination, reshaping global inequalities through algorithmic governance. In the Global South, the intersection of weak legal institutions, entrenched social hierarchies, and external corporate power produces heightened vulnerability. Algorithmic justice, therefore, cannot be reduced to technical fairness or legal compliance; it must be seen as a struggle for equality, sovereignty, and dignity.

This paper has shown that algorithmic systems, from Aadhaar in India to surveillance in Africa and fintech in Latin America, often replicate colonial logics of extraction and control. To counter this, we need a **decolonial vision of algorithmic justice**—rooted in local epistemologies, strengthened by global solidarity, and enforced through robust yet context-sensitive legal frameworks. Only then can the law move beyond being a passive instrument of algorithmic governance to an active guarantor of justice in the digital age.

References:

[1] Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

[2] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

[3] Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.

[4] Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

[5] Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

[6] Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code*. Polity.

[7] Couldry, N., & Mejias, U. A. (2020). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media, 21*(4), 336–349. https://doi.org/10.1177/1527476418796632

[8] Milan, S., & Treré, E. (2019). Big Data from the South(s): Beyond data universalism. *Television & New Media, 20*(4), 319–335. https://doi.org/10.1177/1527476419837739

[9] Gajjala, R. (2022). *Digital diasporas: Labor and affect in gendered Indian digital publics*. Rowman & Littlefield.

[10] Birhane, A. (2021). Algorithmic injustice: A relational ethics approach. *Patterns, 2*(2), 1–9. https://doi.org/10.1016/j.patter.2021.100205

[11] Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

[12] Taylor, L., Floridi, L., & van der Sloot, B. (Eds.). (2017). *Group privacy: New challenges of data technologies*. Springer.

[13] Moerel, L., & Prins, C. (2016). Privacy for the Homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the Internet of Things. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2784123

[14] Abebe, R., Barocas, S., Kleinberg, J., Levy, K., Raghavan, M., & Robinson, D. G. (2020). Roles for computing in social change. *Proceedings of the ACM on Human-Computer Interaction, 4*(CSCW2), 1–26. https://doi.org/10.1145/3415186

[15] Ghosh, S. (2022). Data colonialism and the Global South: Towards decolonizing data governance. *Journal of Information Policy, 12*, 1–23. https://doi.org/10.5325/jinfopoli.12.2022.0001

[16] Prainsack, B. (2019). Data solidarity: A blueprint for bottom-up data governance? *BioSocieties, 14*(1), 77–93. https://doi.org/10.1057/s41292-018-0127-3

[17] Srnicek, N. (2017). *Platform capitalism*. Polity.

[18] Latonero, M. (2018). Governing artificial intelligence: Upholding human rights & dignity. *Data & Society Research Institute*. https://datasociety.net/library/governing-artificial-intelligence

[19] United Nations Human Rights Council. (2021). *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights (A/HRC/48/31)*. United Nations. https://digitallibrary.un.org/record/3944753

[20] World Economic Forum. (2020). *Global technology governance report 2021: Harnessing Fourth Industrial Revolution technologies in a COVID-19 world*. WEF. https://www.weforum.org/reports/global-technology-governance-report-2021