World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Algorithmic Sovereignty and the New Security Dependencies: How Foreign AI Surveillance Technologies Reshape Domestic Autonomy in the Global South

Sheriffdeen Folaranmi Abiade *

Department of Global Studies, University of Massachusetts, Lowell, MA, USA.

World Journal of Advanced Research and Reviews, 2025, 27(02), 162-180

Publication history: Received on 25 June 2025; revised on 30 July 2025; accepted on 02 August 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.2.2845

Abstract

The proliferation of artificial intelligence (AI) technologies has intensified global interdependencies, particularly in the realm of digital surveillance and governance infrastructure. As AI surveillance tools become increasingly embedded in public security, migration control, and political intelligence operations, countries in the Global South face a new paradigm of strategic vulnerability algorithmic sovereignty. This refers to a nation's capacity to exercise full control over the data, infrastructure, and decision logic that underpin algorithmic systems operating within its borders. However, many states in the Global South have adopted foreign-built AI surveillance platforms primarily from dominant geopolitical actors without full access to source code, algorithmic parameters, or data governance rights. This dependency introduces critical security, privacy, and political risks, enabling vendor states to potentially monitor, manipulate, or extract sensitive domestic information under the guise of technological partnership. This study explores how such foreign AI surveillance technologies reshape domestic autonomy through opaque systems integration, extraterritorial data flows, and algorithmic opacity. By drawing on case studies from Africa, Southeast Asia, and Latin America, the paper highlights how imported AI infrastructures embed a form of digital neocolonialism, eroding institutional accountability and creating asymmetrical power relations. It further examines how these dependencies undermine local capacity-building efforts, distort national cybersecurity priorities, and challenge democratic oversight in public sector surveillance programs. The analysis concludes by advocating for regional algorithmic governance frameworks, indigenous AI development initiatives, and strategic procurement policies that reclaim sovereign control over data-driven decision systems. Addressing algorithmic sovereignty is not merely a technical concern but a fundamental aspect of maintaining political independence and safeguarding civil liberties in an increasingly AI-mediated global order.

Keywords: Algorithmic Sovereignty; AI Surveillance; Digital Dependency; Global South; Foreign Technology; National Autonomy

1. Introduction

1.1. Define Algorithmic Sovereignty and Its Strategic Significance in Modern Governance

Algorithmic sovereignty refers to a state's capacity to exercise autonomous control over the design, deployment, regulation, and oversight of algorithmic systems that influence public administration, security, and civic life. In a digitally networked world, algorithms are no longer neutral tools; they shape access to services, determine security responses, and mediate political discourse [1]. As algorithmic systems become embedded in public institutions particularly in law enforcement, border control, and social services the ability of governments to audit, modify, or decommission these systems becomes a central question of sovereignty [2].

* Corresponding author: Sheriffdeen Folaranmi Abiade

Modern governance increasingly relies on data-driven decision systems. Algorithmic sovereignty, therefore, is not just a technical issue but a strategic imperative one that intersects with national security, civil liberties, and digital industrial policy. Without sovereign control, governments risk relying on black-box technologies that operate without local accountability or contextual relevance. This undermines public trust and may entrench asymmetrical power relations between the host country and the foreign technology provider [3].

The concept becomes especially urgent for countries in the Global South, where AI infrastructure is often imported and controlled by external vendors. In these cases, algorithmic sovereignty defines the difference between self-directed digital development and externally shaped technological dependence [4].

1.2. Introduce the Geopolitical Dynamics of AI Surveillance Exports

The global trade in AI surveillance technologies is not merely commercial it is deeply geopolitical. As states like China and the United States compete to shape global AI norms, the export of AI-enabled surveillance systems has become a tool of influence in foreign policy. These systems often include facial recognition, predictive policing software, and behavioral analytics embedded in smart city platforms or public safety networks [5].

China’s Digital Silk Road initiative has expanded the reach of Chinese AI vendors into Africa, Latin America, and Southeast Asia, offering turnkey surveillance infrastructures bundled with concessional financing and political alignment incentives [6]. Meanwhile, U.S. and European companies provide cloud-based surveillance-as-a-service models with advanced analytics but retain significant control over the data and update mechanisms [7].

This dynamic creates a form of digital clientelism, where recipient nations become dependent on the vendor state’s technological ecosystem. As foreign surveillance tools proliferate in the Global South, so does the influence of the exporting countries’ legal frameworks, security paradigms, and industrial standards [8]. These geopolitical dynamics are not just shaping bilateral relationships; they are redefining how domestic autonomy is negotiated in an era where algorithms mediate sovereign decision-making [9].

1.3. Brief Overview of Dependence Challenges in the Global South

Many nations in the Global South adopt foreign AI surveillance tools due to gaps in local infrastructure, lack of technical expertise, and funding constraints. However, this adoption comes with strategic trade-offs. Most foreign AI systems are opaque governments often receive no access to source code, limited transparency over algorithmic logic, and minimal leverage in negotiating terms of data ownership or system modification [10].

This dependency weakens national capacity to enforce legal protections, conduct independent audits, or ensure human rights compliance. In several countries, imported systems have been linked to over-policing, biased decision-making, and the suppression of political dissent [11]. Yet governments frequently lack the institutional frameworks to contest or reform these embedded technologies once operational.

Furthermore, overreliance on foreign surveillance vendors introduces cybersecurity risks and the potential for extraterritorial surveillance. For example, remote software updates, cloud-based data storage, and foreign-managed analytics pipelines present serious vulnerabilities in critical state functions [12]. These risks are amplified by the lack of domestic legislation governing AI procurement, data localization, or accountability mechanisms.

As illustrated in Figure 1, the proliferation of foreign surveillance systems correlates with sharp increases in AI infrastructure dependency across sub-Saharan Africa, Southeast Asia, and Latin America over the last decade [13].

1.4. Research Questions and Objectives

This study investigates how foreign AI surveillance technologies reshape domestic autonomy in the Global South by challenging the principles of algorithmic sovereignty. It aims to answer four central questions:

- What structural and operational characteristics of imported AI surveillance systems contribute to dependency in the Global South?
- How do these dependencies manifest in legal, technical, and political forms of diminished domestic control?
- What are the geopolitical and security implications of vendor lock-in and data externalization?
- How can states reclaim or establish algorithmic sovereignty through policy reform, indigenous capacity-building, and regional cooperation?

The objective is to provide a comprehensive analysis that blends geopolitical insight with technical critique. The paper draws on case studies, system design comparisons, and governance frameworks to explore the strategic risks associated with externally sourced surveillance AI. It also seeks to identify actionable strategies for nations seeking to reduce dependency and build sovereign digital infrastructures aligned with democratic values and local priorities [14].

Table 1 presents a typology of surveillance system attributes across major vendors, detailing access rights, data ownership models, and control hierarchies. These comparisons offer empirical grounding for the analysis of sovereignty erosion and enable the formulation of governance recommendations in subsequent sections [15].

Table 1 Typology of Surveillance System Attributes Across Major Vendors

Attribute	**Vendor A (e.g., China)**	**Vendor B (e.g., U.S.)**	**Vendor C (e.g., EU)**
Source Code Access	No access; proprietary & encrypted	Partial access under strict NDA	Limited access via certified partners
Data Ownership Model	Vendor-controlled or co-owned	Government-owned, vendor-accessible	Locally-owned, with export restrictions
System Update Control	Remote auto-updates; no local veto	Negotiated patches; vendor-initiated	Local control with vendor collaboration
Cloud Hosting Location	Primarily offshore (vendor jurisdiction)	Mixed local/foreign data centers	EU-compliant local hosting mandates
Auditability	Closed-loop system, non-auditable	Third-party audit possible with vendor	Independent audits permissible by design
User Customization	Minimal; fixed use-case configurations	Medium; adaptable through APIs	High; modular and standards-driven
Jurisdictional Control	Foreign legal jurisdiction dominates	Shared legal responsibility	National sovereignty prioritized
Algorithm Transparency	None; model logic obscured	Partial explanations provided	Full explainability frameworks required

2. The rise of foreign AI surveillance technologies

2.1. Historical Context of Surveillance Tech Transfers

The export of surveillance technology has long been intertwined with geopolitical strategy. During the Cold War, superpowers exported surveillance infrastructure not merely as security tools but as instruments of ideological alignment and influence projection. The United States, for instance, equipped allies with telephone wiretaps, signal interception systems, and intelligence-gathering radar networks under military aid packages and strategic cooperation agreements [6]. These systems were often bundled with training and operational support, creating long-term dependencies that mirrored broader military alliances.

While Cold War-era surveillance was primarily hardware-based and limited to analog systems, the post-9/11 period saw a rapid transition to digital surveillance, biometric scanning, and data-driven intelligence platforms. The rise of global internet connectivity and mobile telecommunication opened new avenues for surveillance at scale, enabling remote monitoring and real-time threat detection across national boundaries [7]. Governments began investing in automated systems capable of parsing vast datasets for behavioral anomalies, predictive risk scoring, and social media sentiment tracking.

This transition culminated in the current age of algorithmic surveillance, where intelligence is not merely collected but interpreted and acted upon by machine-learning systems. This shift has introduced new power dynamics: countries that develop and export AI-powered surveillance systems now wield influence not only through access to data flows but also through control over decision logic embedded in critical public functions [8].

In this context, technology transfer has evolved beyond physical equipment to include software platforms, algorithmic models, and proprietary interfaces. The recipient countries in the Global South frequently lack visibility into how these imported systems function, what data is retained or shared, and how they evolve over time. As Figure 1 illustrates, this evolution from Cold War hardware to contemporary algorithmic platforms has accelerated since 2005, with a surge in AI surveillance exports from dominant states to resource-constrained nations across Africa, Asia, and Latin America [9].

2.2. Dominant Exporters: China, U.S., and EU Perspectives

The global landscape of AI surveillance exports is dominated by a handful of countries that combine technological capacity with geopolitical ambition. China, the United States, and the European Union represent the principal exporters, each advancing different architectures of influence through their respective platforms and regulatory models.

China's Digital Silk Road, an extension of its Belt and Road Initiative, provides recipient states with comprehensive AI-enabled surveillance infrastructure. These exports include facial recognition cameras, smart city platforms, data analytics software, and cloud-based command centers. Major companies like Huawei, ZTE, and Hikvision are central to these deployments, often underpinned by concessional loans and state-backed diplomatic agreements [10]. China frames these exports as tools for modernization and urban management, yet their proliferation raises concerns about embedded political influence and data exfiltration capabilities.

In contrast, U.S.-based firms typically offer surveillance-as-a-service models hosted on proprietary cloud platforms. Companies like Palantir, Amazon Web Services, and IBM export intelligence solutions such as crime prediction systems, biometric identification, and data fusion platforms, largely targeting law enforcement and national security agencies [11]. While these services are often marketed as technically superior and rights-compliant, they also involve significant vendor lock-in and limited recipient control over underlying algorithms and data repositories.

The European Union's approach emphasizes regulatory harmonization and ethical AI principles but still enables the export of surveillance technologies through firms based in France, Germany, and Sweden. Although the EU promotes human rights in AI governance, it faces criticism for allowing dual-use surveillance systems to be deployed in countries with poor accountability frameworks [12].

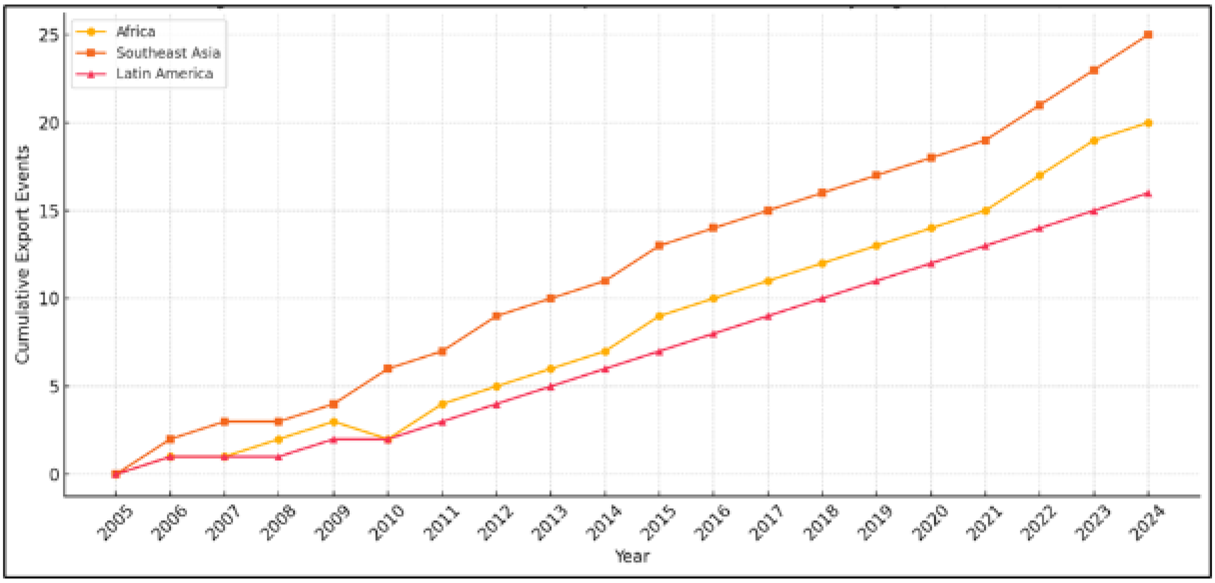

Figure 1 Timeline of Ai survelliance exports to the global south by region (2005-2024)

As shown in Figure 1, surveillance technology exports have diversified by origin and complexity over the past two decades, yet the shared outcome is the emergence of opaque, externally-controlled infrastructures within Global South nations. This diffusion raises critical questions about sovereignty, consent, and long-term technological dependence [13].

2.3. Adoption in the Global South: Trends and Motivations

The adoption of AI-powered surveillance systems in the Global South is shaped by both pragmatic needs and structural vulnerabilities. Governments facing rising urban crime, insurgency threats, and resource constraints often view surveillance technology as a low-cost, high-impact solution. Platforms that offer facial recognition, license plate scanning, and predictive policing capabilities are promoted as tools for crime reduction, border security, and counter-terrorism without necessarily investing in institutional reforms or human oversight frameworks [14].

Another key driver is aid-driven deployment, wherein surveillance systems are integrated into development packages offered by foreign governments or multinational corporations. These arrangements often prioritize infrastructure delivery over transparency or democratic accountability. For example, a city may receive AI-equipped security cameras bundled into a larger smart city initiative funded by foreign investment or bilateral loans. The technologies arrive pre-configured, often with closed-source software, limiting local control and customization [15].

Moreover, the lack of indigenous AI capacity means that local officials must rely on foreign vendors for system maintenance, updates, and interpretation of analytics further reinforcing technological dependence. These dependencies are rarely acknowledged in procurement contracts or public statements, and oversight bodies may lack the technical literacy to evaluate long-term implications.

As Figure 1 demonstrates, since 2005 there has been a marked increase in the deployment of surveillance systems across the Global South, with peaks corresponding to political unrest, pandemic response, and major international summits. The trend indicates a reactive pattern of adoption, where surveillance technologies are implemented in crisis contexts without full consideration of sovereignty, privacy, or governance [16].

3. Anatomy of algorithmic dependence

3.1. Source Code Blackboxing and Vendor Lock-In

One of the most critical yet under-addressed challenges associated with the adoption of foreign AI surveillance technologies in the Global South is the issue of source code blackboxing and vendor lock-in. Most imported systems come as closed-source platforms, offering recipient governments little to no access to the algorithmic logic driving surveillance decisions. This opacity extends from the machine learning models used for facial recognition and anomaly detection to the threshold-setting mechanisms that define which behaviors are flagged as suspicious [11].

The lack of code auditability means domestic authorities cannot independently verify how decisions are made, what data is prioritized, or whether biases are embedded in the system. In practical terms, this creates a scenario in which national security decisions are partially outsourced to algorithmic processes controlled by foreign vendors. Moreover, without access to the source code, even well-trained domestic experts remain unable to interpret system outputs or make meaningful alterations to adapt the technology to local contexts [12].

Compounding this issue are non-negotiable update structures. Foreign vendors typically retain exclusive rights to modify, patch, or upgrade the surveillance software, often doing so remotely and without local oversight. These updates can introduce new functionalities or alter existing rules without the knowledge or consent of national security agencies. This arrangement reinforces vendor lock-in, making it exceedingly difficult for countries to migrate to alternative platforms without significant financial and operational disruption [13].

As illustrated in Table 1, the level of access, customization, and update rights varies significantly across major vendors, with Chinese systems offering minimal source transparency, and Western platforms offering limited interpretability under commercial confidentiality clauses. In either case, the recipient state’s agency in controlling the technological logic of surveillance remains severely compromised. This dependency undermines algorithmic sovereignty and risks embedding foreign influence deep within national decision-making architectures [14].

3.2. Data Sovereignty Erosion and Cross-Border Transfers

Closely linked to algorithmic opacity is the issue of data sovereignty erosion, which emerges when surveillance systems are hosted on foreign-controlled infrastructures. Most modern AI surveillance platforms rely on cloud computing, remote analytics, and distributed storage. As a result, the raw footage, biometric records, and behavioral metadata collected from citizens in the Global South are often transmitted to data centers located in jurisdictions outside the host country’s legal reach [15].

This cross-border data transfer undermines a government's ability to enforce national data protection laws and raises significant concerns regarding extraterritorial surveillance and unauthorized third-party access. For instance, under various national security laws such as the U.S. CLOUD Act or China's 2017 Cybersecurity Law, companies based in those countries can be compelled to hand over data even when the data pertains to foreign citizens and is generated outside their borders [16].

Additionally, cloud-hosted infrastructures frequently lack physical and logical segmentation to isolate datasets by jurisdiction. This increases the risk of commingled data repositories, where sensitive national security information may be inadvertently exposed or misused. Such configurations erode state control over who accesses surveillance outputs and under what conditions, making it difficult to ensure compliance with national intelligence protocols or civil liberties protections [17].

Further complicating matters is the fact that many recipient countries lack formal bilateral data-sharing agreements with exporting states. As a result, data sovereignty is not just technically challenged but legally unrecognized, leaving surveillance data in a grey zone of jurisdictional ambiguity. This opens the door to both passive exploitation such as unauthorized data mining and active interference, such as algorithmic manipulation of decision-making outputs [18].

Table 1 details the hosting and ownership structures of AI surveillance platforms across vendors, showing that foreign jurisdiction over surveillance data is the rule rather than the exception. Without reforms in procurement and cloud governance, this model effectively nullifies national sovereignty over critical digital infrastructure [19].

3.3. Misalignment with Local Legal Norms and Human Rights

The integration of foreign surveillance AI into domestic security frameworks often results in serious misalignments with national legal norms and internationally recognized human rights principles. In many cases, imported systems are designed based on the legal and operational frameworks of the exporting countries, which may not align with the socio-political context or constitutional protections in the host nation [20].

This misalignment manifests in several ways. First, the criteria embedded in surveillance algorithms such as behavioral risk scores or biometric recognition thresholds are rarely calibrated to local legal standards regarding suspicion, arrest, or privacy. For example, predictive policing algorithms may classify neighborhood demographics as risk indicators, inadvertently reinforcing discriminatory practices and violating equal protection principles enshrined in domestic constitutions [21].

Second, legal safeguards such as judicial oversight, transparency requirements, and data minimization protocols are frequently bypassed or weakened under these imported systems. Due to a lack of domestic capacity to audit or interpret algorithmic processes, surveillance may be deployed in ways that contravene national laws on due process, freedom of assembly, and freedom of expression [22]. Moreover, oversight bodies often lack the technical resources to challenge or correct system abuses, leading to unchecked expansions of state surveillance power.

In contexts where political dissent or minority activism is already vulnerable to repression, foreign AI surveillance tools can inadvertently or deliberately facilitate authoritarian behavior. This is particularly problematic in post-conflict or transitioning democracies, where institutional trust is fragile and digital rights are still evolving [23].

As shown in Table 1, none of the leading AI surveillance vendors offer formal mechanisms to adapt algorithmic governance to host country legal codes. Instead, system design and functionality are pre-packaged, leaving limited room for localization. This creates a de facto legal extraterritoriality, where domestic policies are subordinated to the operational defaults of foreign technologies [24].

The cumulative effect is a profound erosion of civil liberties, democratic accountability, and rule-of-law integrity all of which are central to sovereign governance. Without enforceable interoperability between imported surveillance systems and national legal frameworks, algorithmic governance risks becoming an instrument of control rather than protection [25].

4. Case studies from the global south

4.1. Africa: Ethiopia's National Intelligence Surveillance Network

Ethiopia represents a compelling example of how foreign AI surveillance technologies can entrench both operational reach and systemic dependency. Since 2017, the Ethiopian government has invested in AI-enhanced national surveillance infrastructure, largely sourced from Chinese vendors such as Huawei and ZTE [16]. The systems include high-resolution facial recognition cameras, biometric monitoring databases, and AI-based behavioral analytics tools deployed in key urban centers, government compounds, and border control zones.

These systems were initially marketed as solutions for counterterrorism and urban crime management. However, their integration into the broader intelligence framework has triggered widespread concern over civil liberties and authoritarian misuse. Several investigative reports indicate that surveillance footage and algorithmically flagged "risk behaviors" have been used to monitor political opposition figures, restrict media activity, and preemptively disrupt peaceful demonstrations [17].

The opacity of the underlying algorithms, combined with the centralization of system control under the National Intelligence and Security Service (NISS), has undermined transparency and oversight. Civil society organizations and legal scholars have raised alarms about the absence of data protection laws or judicial review mechanisms for AI-generated evidence [18]. Furthermore, the NISS retains exclusive control over system access, with no parliamentary or civilian oversight bodies empowered to audit or amend operational protocols.

Public pushback has emerged in response. A coalition of Ethiopian digital rights groups filed a petition in 2022 demanding a moratorium on the use of Chinese AI surveillance platforms until legal accountability frameworks are established. The petition emphasized the risk of technological overreach and foreign influence on national decision-making processes [19].

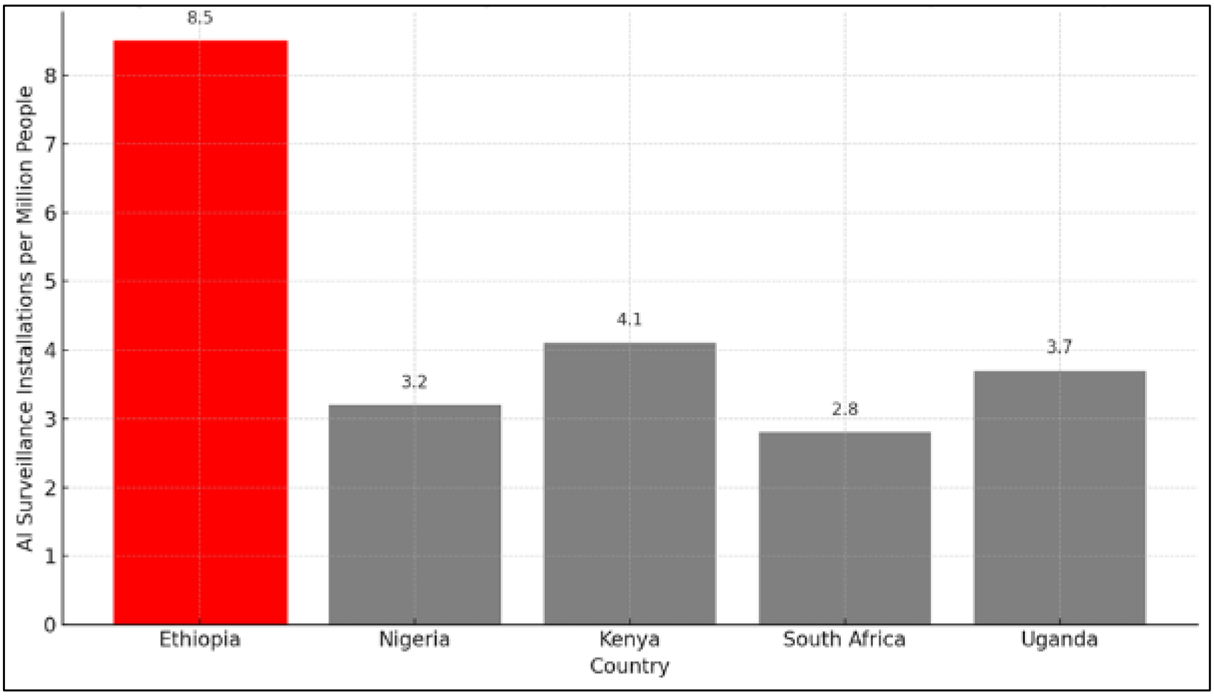

Figure 2 AI surveillance density in sub Saharan africa

Figure 2 shows that Ethiopia is among the most heavily surveilled countries in sub-Saharan Africa, particularly in terms of AI density relative to population. Table 2 highlights how this model of import-led surveillance has significant implications for local law, political participation, and public trust marking Ethiopia as a case where AI-driven surveillance may undermine rather than enhance national autonomy [20].

4.2. Southeast Asia: Smart City Projects in Cambodia and Laos

In Southeast Asia, the export of AI surveillance systems is increasingly embedded within broader smart city initiatives, most notably in Cambodia and Laos. These projects financed and built predominantly by Chinese firms under the Digital Silk Road integrate surveillance functionality into traffic management, utility monitoring, emergency services, and citizen identification systems [21].

In Phnom Penh and Vientiane, thousands of cameras equipped with facial recognition, license plate detection, and crowd behavior analysis have been installed across critical infrastructure points. The vendors mostly Huawei, Dahua, and Hikvision operate under turnkey contracts that include cloud hosting, analytics services, and ongoing software updates managed remotely from vendor-controlled servers [22]. These installations form part of what officials describe as "urban modernization" but lack accompanying legal or technical frameworks for civilian protection.

Government statements emphasize public safety and traffic optimization as motivations, yet local journalists and opposition groups contend that the real intent is political surveillance. Reports suggest that protest organizers and independent media personnel have been tracked and apprehended using footage from smart city infrastructure without judicial warrants or legislative scrutiny [23].

The critical challenge in both Cambodia and Laos is the near-total absence of local technical capacity. No domestic authority has access to or control over the algorithmic backend of the imported systems. System logs, metadata, and real-time footage are processed and stored off-site, often in encrypted environments that national IT teams cannot access. Local ministries depend entirely on foreign contractors for maintenance, which includes AI model retraining and camera recalibration [24].

These gaps raise broader concerns about technological sovereignty. Cambodia's national telecommunications authority confirmed in 2021 that no AI certification or security protocol assessments had been conducted on imported platforms. In Laos, parliamentary attempts to review public surveillance policy were stalled due to lack of technical documentation and vendor non-disclosure clauses.

Figure 2 depicts extensive surveillance saturation in Southeast Asian capitals, highlighting how smart city branding conceals state-wide surveillance expansion. As shown in Table 2, these deployments weaken democratic oversight, diminish civic engagement, and entrench state surveillance with minimal external or internal accountability [25]. Southeast Asia's experience underlines the dangers of bundling AI surveillance into development assistance packages without parallel governance reform.

4.3. Latin America: Predictive Policing in Ecuador and Honduras

Latin America presents a distinctive variation in AI surveillance adoption: the integration of predictive policing platforms algorithms that use historical crime data to forecast future criminal activity into law enforcement strategies. Ecuador and Honduras have emerged as prominent adopters of such tools, largely sourced from U.S.-based firms offering software-as-a-service solutions with centralized cloud architectures [26].

In Ecuador, the government launched the "Safe City" initiative in 2018, deploying thousands of interconnected surveillance cameras and AI-powered command centers across Quito and Guayaquil. The project, executed by a partnership between Chinese and U.S. vendors, introduced real-time crowd analysis, vehicle tracking, and facial recognition integrated with crime databases. The AI model also generates risk scores for neighborhoods, informing where patrols are dispatched and which individuals are deemed "of interest" [27].

Honduras has adopted a similar architecture under its "Secure Homeland" program, which includes algorithmic crime mapping and predictive risk dashboards used by national police. These systems rely heavily on imported machine learning models trained on incomplete and often biased datasets. Critics have warned that the platforms reinforce existing patterns of over-policing in marginalized neighborhoods, exacerbating racial and economic profiling without clear channels for correction or appeal [28].

Both countries suffer from weak institutional oversight. National privacy laws are either outdated or selectively enforced, and there are no independent bodies authorized to audit AI surveillance practices. Requests for algorithmic transparency from civil society organizations have been repeatedly denied on grounds of "commercial sensitivity," a clause commonly inserted into vendor contracts [29].

Furthermore, reports indicate a troubling trend of politicization of surveillance. In Honduras, several opposition leaders and journalists have alleged that predictive policing systems were used to monitor political activity under the guise of public safety. Metadata from surveillance systems has allegedly been used in investigations without warrants, raising due process concerns [30].

In Ecuador, legal scholars have raised alarms over the extraterritorial storage of biometric data, noting that the country lacks data localization laws. This places sensitive civic information under the purview of foreign jurisdictions, weakening national control and complicating legal recourse for wrongful data use or false positives.

As shown in Figure 2, Latin American countries have among the highest densities of AI-based predictive policing per urban square kilometer. Table 2 illustrates the operational, legal, and civic consequences of such deployments, emphasizing how algorithmic opacity and foreign dependence enable systemic abuses.

These case studies demonstrate that while AI surveillance is often adopted under the guise of modernization and safety, the absence of oversight, legal adaptability, and technical sovereignty renders these systems ripe for misuse. Without structural reforms and multilateral cooperation, such technologies risk entrenching authoritarianism under digital pretenses [31].

5. Strategic risks and political ramifications

5.1. National Security Vulnerabilities

One of the most pressing but under-recognized threats associated with foreign AI surveillance systems is the compromise of national security through embedded backdoors, remote access points, and algorithmic control pathways. Imported surveillance infrastructures often include cloud-based architectures and proprietary software that can be altered or disabled remotely by the exporting vendor. This creates a potential kill-switch scenario, in which a foreign government or corporate entity could intentionally deactivate or manipulate a nation's surveillance capabilities during geopolitical tension or conflict [21].

Several governments in the Global South rely on turnkey platforms with minimal in-country data storage and limited source code access. This structure leaves host states vulnerable to algorithmic sabotage where critical threat classification models or alert mechanisms could be subtly altered to misidentify threats or ignore real-time security risks [22]. Such sabotage is difficult to detect due to the opacity of the systems and the absence of domestic auditing capabilities.

Additionally, data exfiltration risks are inherent in vendor-hosted platforms. Surveillance data involving military zones, governmental movements, or national infrastructure layouts can be captured and stored in foreign jurisdictions. These risks are compounded when software updates and patch management are controlled exclusively by vendors, effectively handing over operational sovereignty to external entities [23].

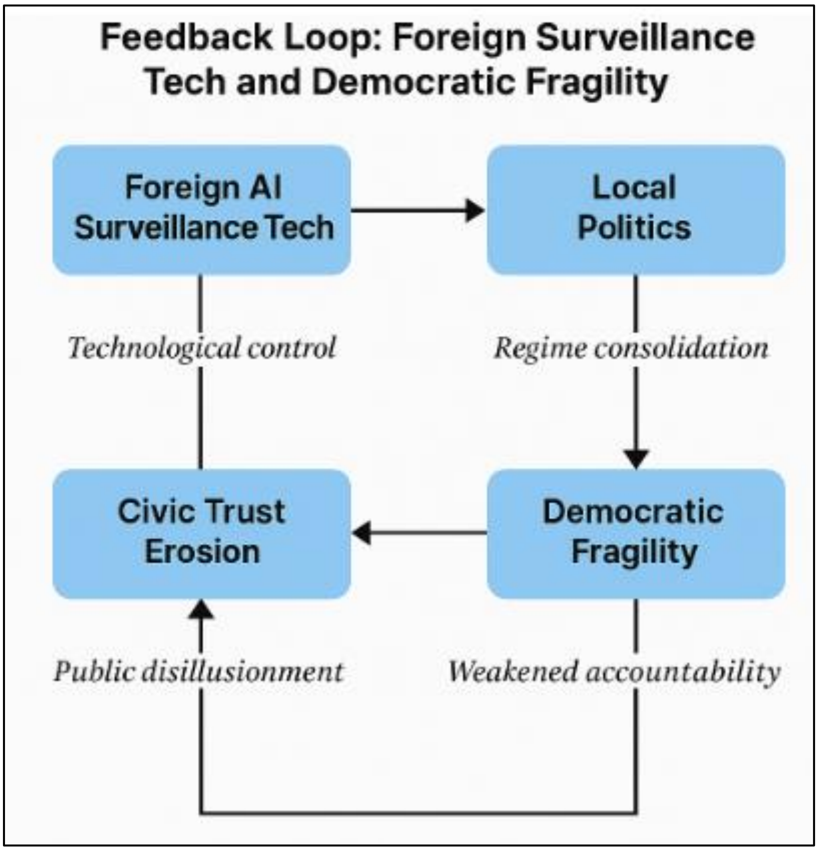

Figure 3 Feedback loop

Figure 3 highlights the feedback loop in which foreign technological control interacts with domestic political systems and erodes both autonomy and responsiveness. These vulnerabilities demand immediate reevaluation of AI procurement practices, data localization laws, and national cybersecurity protocols. Without asserting sovereignty over critical AI infrastructure, states risk the instrumentalization of surveillance systems not just for social control but as vectors for foreign influence and strategic disruption [24].

5.2. Civic Trust Erosion and Democratic Backsliding

The widespread deployment of foreign AI surveillance systems has tangible consequences for public trust, political participation, and the integrity of democratic processes. Citizens in the Global South are increasingly aware that AI surveillance tools particularly facial recognition and predictive policing are being used in ways that exceed conventional crime prevention mandates. As more cases of political surveillance, wrongful arrests, and overreach surface, civic trust in state institutions declines [25].

Public resistance movements in countries such as Kenya, Colombia, and the Philippines have emerged in response to opaque surveillance practices. These movements demand greater algorithmic transparency, human rights safeguards, and cessation of AI deployments that lack community consultation or legal oversight [26]. Despite this, governments have often ignored such calls, citing national security and modernization imperatives to justify continued use of foreign-controlled systems.

AI surveillance tools have also been strategically deployed to silence dissent. Activists, journalists, and opposition leaders are often tracked using biometric identifiers or movement patterns extracted from smart city systems. The chilling effect produced by such monitoring suppresses lawful protest, reduces freedom of expression, and reconfigures the relationship between citizen and state into one of suspicion and coercion [27].

The problem is amplified when legal institutions are either complicit or technically unequipped to investigate algorithmic rights violations. In several instances, courts have deferred to executive claims of “national security,” bypassing judicial review of surveillance programs. This erosion of checks and balances contributes directly to democratic backsliding, wherein institutions nominally remain intact, but their functions are hollowed out by unaccountable algorithmic governance.

As illustrated in Figure 3, foreign surveillance systems reinforce autocratic tendencies by supplying regimes with the tools of control without the regulatory counterbalances that democratic governance requires. In the absence of public accountability, AI surveillance becomes not a tool for safety but a mechanism of systemic disenfranchisement [28].

5.3. Policy Co-optation and Elite Capture

The importation of AI surveillance technologies is not always a passive process. In many cases, it is actively driven by political elites seeking to consolidate power, suppress opposition, or secure geopolitical alignment. This phenomenon, known as policy co-optation, sees foreign surveillance platforms integrated into national governance structures in ways that prioritize regime security over public interest or institutional accountability [29].

Elite capture of AI policy occurs when a narrow circle of political actors often presidents, security ministers, or military leaders sign bilateral agreements with foreign vendors without multistakeholder consultation or parliamentary approval. These agreements typically bypass public procurement norms and are framed as “national security initiatives,” thus excluding civil society, technologists, and opposition parties from meaningful engagement [30].

In return, foreign vendors gain exclusive market access, regulatory exemptions, and long-term servicing contracts that lock recipient states into a dependent relationship. In practice, this dynamic creates an opaque governance structure, where critical digital infrastructure is governed by informal networks of political loyalty and corporate discretion, rather than law and public interest.

Moreover, the surveillance data generated by these systems is often monopolized by elite actors. For example, metadata and facial recognition outputs can be used for political intelligence, enabling incumbent regimes to monitor rival movements, preempt protest organization, or intimidate critics through targeted surveillance. This reorients AI technology from public utility to regime preservation tool, particularly in hybrid or fragile democracies [31].

Figure 3 visualizes this dynamic, showing how policy co-optation creates a closed loop between foreign vendors, elite interests, and democratic fragility. Table 2 further elaborates how legal norms, operational transparency, and civic engagement are suppressed under such configurations. Without institutional reforms that limit executive overreach and mandate transparency in AI deployments, algorithmic governance risks becoming an entrenched pillar of authoritarian consolidation in the Global South [32].

Table 2 Impact of Imported AI Surveillance on Legal, Operational, and Civic Dimensions in the Global South

Dimension	Observation	Example (Ethiopia)	Implications
Operational Control	Foreign vendors manage software updates and data storage	Surveillance systems installed via bilateral contracts with Chinese firms [20]	Limits domestic technical capacity, weakens state control over system evolution and auditing
Legal Oversight	Lack of AI-specific legislative frameworks and judicial redress mechanisms	National laws lag behind in regulating automated data capture and biometric analytics	Legal opacity enables executive overreach and misuse of surveillance data
Data Sovereignty	Cloud-hosted data accessible by foreign jurisdictions	Data centers hosted outside national boundaries or on vendor-owned hybrid clouds	Raises cybersecurity risks, subjects domestic data to foreign intelligence interception
Civic Participation	Public consultations and civil society inputs absent in procurement processes	Civil society and opposition groups excluded from surveillance policy development	Deepens mistrust, reduces legitimacy of AI deployments, and increases societal resistance
Transparency & Redress	Algorithmic decisions not subject to audit or public explanation	Automated identification systems lack explainability or public grievance protocols	Citizens have no means to challenge wrongful surveillance or predictive profiling outcomes

Political Use	AI tools leveraged for regime stability and dissent suppression	Reports of surveillance targeting ethnic activists and opposition journalists [32]	Reinforces authoritarian tendencies under the guise of digital modernization

6. Reclaiming algorithmic sovereignty

6.1. Building Indigenous AI Capacities

Reclaiming algorithmic sovereignty in the Global South begins with sustained investment in indigenous AI capabilities, including research, development, and talent cultivation. Local universities and startups play a foundational role in this process, not only by training technical professionals but by anchoring algorithmic systems in local languages, governance contexts, and cultural norms [25]. This localization ensures that AI technologies reflect public values and legal expectations rather than importing the logic of foreign platforms wholesale.

Universities in Brazil, Kenya, and Indonesia have initiated AI research clusters that focus on ethical design, local datasets, and context-aware applications such as agriculture, public health, and smart infrastructure. These institutions increasingly partner with government agencies to provide technical expertise for AI policy drafting and regulatory sandboxing. For instance, Kenya's Jomo Kenyatta University of Agriculture and Technology collaborates with public agencies on AI deployments for biometric authentication in e-governance platforms [26].

Startups also contribute to the democratization of AI by experimenting with open-source models, low-resource computing architectures, and algorithmic fairness audits. Local ventures often fill critical gaps left by large vendors such as language processing for indigenous dialects or mobile-first AI tools for remote communities. However, many of these startups struggle to scale due to limited funding, brain drain, and restrictive procurement environments.

To bridge these gaps, public-private R&D partnerships are essential. Governments can provide grants, tax incentives, and innovation clusters that facilitate long-term collaboration between academia, startups, and public sector institutions. These partnerships create ecosystems that retain talent, generate homegrown IP, and align technological outputs with policy goals [27].

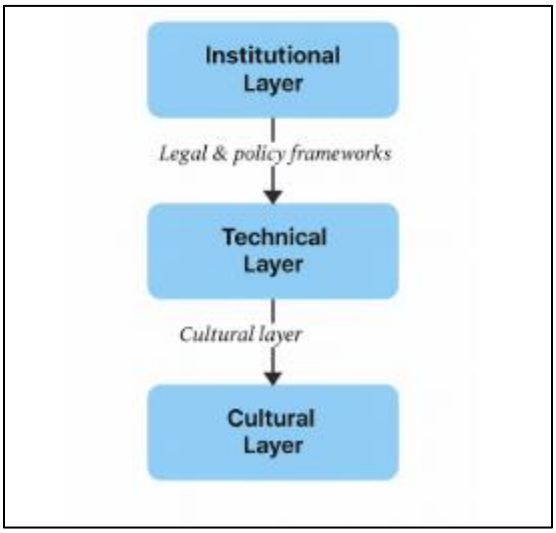

Figure 4 Policy Architecture for reclaiming algorithmic soverign

Figure 4 presents a multi-layered policy architecture in which indigenous capacity-building operates at the technical core. This approach integrates technical autonomy with broader institutional reforms. As shown in Table 3, countries with stronger domestic AI ecosystems are better positioned to negotiate fairer terms with foreign vendors and to resist exploitative surveillance deployments that undermine sovereignty [28].

6.2. Regional AI Governance Frameworks

National initiatives must be complemented by regional governance frameworks that harmonize standards, pool resources, and establish ethical baselines for AI deployment. Given the transnational nature of AI supply chains and data flows, regional coordination enhances bargaining power and provides a buffer against technological hegemony by dominant exporter states [29].

In Africa, the African Union (AU) is advancing a Continental AI Strategy that emphasizes data sovereignty, inclusive innovation, and digital solidarity among member states. The strategy proposes shared regulatory templates for public sector AI use, cross-border data governance protocols, and ethical review boards for AI applications in sensitive domains such as policing and healthcare [30]. It also recommends the creation of pan-African AI research centers and capacity-building programs to reduce reliance on external expertise.

Similarly, ASEAN has developed a Digital Data Governance Framework that includes a roadmap for digital sovereignty and algorithmic accountability. Member states are encouraged to establish domestic AI codes of practice aligned with regional principles, including transparency, explainability, and non-discrimination. Although implementation levels vary, the framework represents an important move toward shared sovereignty in algorithmic governance [31].

A core element of these frameworks is the principle of interoperability ensuring that AI systems developed within one country can be integrated with regional infrastructure without ceding control to external entities. This reduces the risk of vendor lock-in and enables resource-constrained countries to benefit from pooled infrastructure, shared technical standards, and open-source toolkits designed specifically for regional contexts.

Another key principle is ethical use, including provisions for community consent, transparency in public procurement, and human rights impact assessments. These are essential for ensuring that AI systems enhance rather than undermine democratic governance.

Figure 4 illustrates how regional governance acts as a structural layer above national policy efforts, reinforcing accountability and resilience. As detailed in Table 3, countries engaged in regional AI collaboration such as Kenya through the AU and Indonesia via ASEAN exhibit stronger legal protections and a more diversified AI supply base than those operating in isolation [32].

Regional frameworks also provide diplomatic platforms for contesting exploitative AI exports. They can coordinate responses to surveillance overreach, investigate data sovereignty breaches, and collectively negotiate with large vendors. Over time, such mechanisms can reconfigure the balance of power in the global AI economy and support a more equitable distribution of algorithmic autonomy across the Global South.

6.3. Sovereign Procurement and Open-Source Mandates

One of the most actionable levers for reclaiming algorithmic sovereignty lies in sovereign procurement reform. Governments must design procurement policies that not only prioritize local innovation but also enforce technical transparency and legal accountability in AI systems sourced from abroad. This includes mandates for open-source access, explainable algorithms, and enforceable contract terms regarding data governance and update control [33].

National technology audits should be conducted for all foreign surveillance and AI platforms prior to deployment. These audits would assess algorithmic bias, data flow structures, update protocols, and cybersecurity risks. Independent technology commissions ideally composed of technical experts, civil society representatives, and legal scholars should be empowered to review contracts, reject non-compliant technologies, and propose alternatives where necessary [34].

Such commissions have already been piloted in Brazil, where the city of São Paulo adopted an AI procurement policy requiring vendors to disclose training datasets, error rates, and all system inputs related to public decision-making. Kenya’s Communications Authority is also developing guidelines to ensure public-sector AI systems conform to standards of auditability and open access for redressal mechanisms [35].

Open-source mandates serve as both a technical and strategic tool for sovereignty. Requiring vendors to release source code, APIs, and model documentation allows for independent auditing and local customization. This reduces reliance on foreign-controlled update cycles and enables national experts to understand, modify, or decommission AI systems as needed. Open-source also facilitates capacity building, as domestic institutions can train personnel on real-world tools rather than inaccessible black-box systems.

Moreover, legal reforms must align procurement with public interest objectives. This includes enacting algorithmic accountability laws that define liabilities in cases of system malfunction, data misuse, or rights violations. In Indonesia, recent legislative proposals include clauses that hold both foreign vendors and domestic implementing agencies jointly liable for harms caused by AI deployments in surveillance or public services [36].

Figure 4 shows how sovereign procurement intersects with legal frameworks, technical capacity, and regional collaboration to form a holistic strategy for reclaiming algorithmic autonomy. As depicted in Table 3, countries that implement audit-based procurement and open-source mandates show reduced foreign dependency and improved alignment between AI systems and constitutional protections [37].

Table 3 Comparative Analysis of National AI Governance Efforts in the Global South (Brazil, Kenya, Indonesia)

Country	Domestic AI Ecosystem Strength	AI Procurement Transparency	Data Sovereignty Provisions	Vendor Negotiation Leverage	Surveillance Oversight Mechanisms
Brazil	Moderate–High (university R&D + startups)	Medium (open tenders in key sectors)	Strong data protection laws (LGPD)	Medium–High (local development clauses)	Civil society watchdogs, legal redress paths
Kenya	Moderate (growth in fintech/AI hubs)	Low (frequent bilateral agreements)	Weak data localization enforcement	Low (limited bargaining power)	Minimal oversight, parliamentary gaps
Indonesia	High (national AI strategy, strong tech base)	Medium–High (mixed public–private)	Active data protection reforms underway	High (vendor diversification strategy)	Inter-ministerial coordination, pilot reviews

Beyond procurement, governments should invest in public-sector digital infrastructure that enables in-house development and evaluation of AI tools. National AI labs, public data repositories, and algorithm testbeds can help establish a feedback loop between developers, policymakers, and end-users. These structures not only enhance trust but ensure that AI systems are built with local priorities, rights frameworks, and operational realities at their core [38].

In sum, procurement is not merely a transactional process it is a sovereign decision-making act that defines the architecture of national governance. By embedding transparency, accountability, and openness into procurement law and practice, states in the Global South can shift from passive recipients to active architects of their algorithmic futures [38].

7. Theoretical and normative reflections

7.1. Surveillance Capitalism vs. Sovereign Autonomy

The rise of surveillance capitalism, as theorized by Zuboff, fundamentally reshaped the logic of data commodification by turning human experience into behavioral surplus for predictive products [40]. While originally applied to Western corporate data practices, this framework gains new urgency when analyzed through the lens of the Global South. In these contexts, the surveillance capitalist model often arrives pre-packaged within imported AI infrastructure, especially in the domain of public safety, border control, and biometric governance.

Unlike voluntary data transactions between users and corporations, AI surveillance in the Global South is frequently government-sanctioned and externally provisioned—transforming entire populations into passive data subjects. These systems harvest large-scale behavioral data that may be processed, stored, or monetized abroad with minimal transparency or local benefit. The behavioral data extracted via traffic cameras, facial recognition, and predictive policing software is often inaccessible to the very governments deploying these tools [30]. This exacerbates not only technical dependencies but structural power asymmetries that challenge democratic oversight and legal redress.

A critical tension emerges between the promise of AI innovation efficiency, crime reduction, and service delivery and the erosion of algorithmic autonomy. Foreign vendors provide turnkey solutions, often through concessional loans or aid packages, making them politically palatable but technically opaque. This duality fosters a Faustian bargain: technological advancement at the cost of sovereign control over data, algorithms, and national security posture [31].

Efforts to reclaim algorithmic sovereignty must therefore resist the exportation of surveillance capitalism under the guise of modernization. Instead, they should promote a rights-based model where digital infrastructure development is contingent on local data ownership, explainability, and inclusive accountability structures. This realignment is essential to disrupt extractive paradigms and anchor AI adoption in principles of equity and democratic governance [32].

7.2. Rethinking "Digital Colonialism"

The concept of digital colonialism offers a powerful lens to examine how former imperial dynamics are reconstituted through technology. Traditionally understood as the domination of digital infrastructure, software, and platforms by corporations from the Global North, the term is evolving. In the context of AI surveillance, digital colonialism increasingly manifests as algorithmic colonization where not just tools, but governance logics and behavioral norms are exported and imposed [33].

This form of colonization differs from prior extractive paradigms in that it operates on predictive control rather than territorial occupation. For instance, AI models embedded within smart city programs in Southeast Asia and facial recognition in African urban centers are not merely technical imports they reflect epistemic impositions about how security should be defined, policed, and prioritized [34]. These systems often encode assumptions about "risk" and "normalcy" based on datasets from unrelated geopolitical contexts, thereby introducing algorithmic bias and misalignment with local norms.

The implications for global justice and equitable development are profound. When foreign-developed AI systems shape domestic policing, welfare eligibility, or immigration processes, they risk replicating systemic inequalities while bypassing democratic deliberation. These tools are rarely subject to domestic ethical review boards or open procurement contests. The opacity and asymmetry embedded in such arrangements constrain a nation's capacity to define its digital future on its own terms [35].

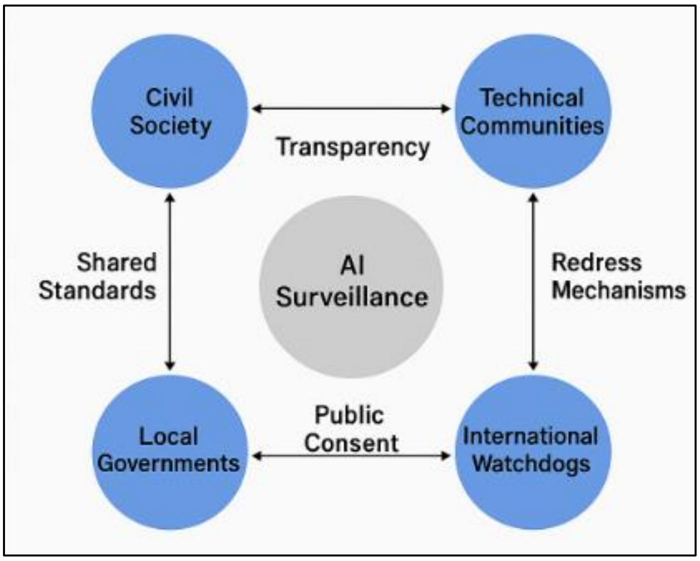

Figure 5 Recommended Multi-Stakeholder Governance Model for AI Surveillance in the Global South

The diagram illustrates a collaborative framework integrating civil society, local governments, technical communities, and international watchdogs into AI surveillance governance. Central pillars include transparency, interoperability standards, algorithmic redress mechanisms, and public consent protocols. This model promotes participatory oversight and policy alignment to reclaim algorithmic sovereignty and mitigate foreign influence in domestic AI infrastructure.

As shown in Figure 5, a multi-stakeholder governance model is needed one that integrates civil society, technical communities, local governments, and international watchdogs into the AI decision-making process. This model emphasizes transparency, shared standards, redress mechanisms, and public consent as central pillars for reclaiming algorithmic autonomy.

Only by confronting the algorithmic expressions of digital colonialism can the Global South assert normative authority and technological self-determination in an AI-driven world [36].

8. Conclusion and recommendations

8.1. Recap of Findings and Key Insights

This article examined how foreign AI surveillance technologies are reshaping domestic autonomy across the Global South, raising profound concerns over algorithmic sovereignty. We began by defining algorithmic sovereignty as the capacity of states to govern their data ecosystems, algorithmic tools, and decision-making processes without undue foreign interference. From historical analysis to current adoption patterns, the study mapped the geopolitical entanglements underpinning AI surveillance exports by dominant actors such as China, the U.S., and the EU.

We highlighted key challenges: source code blackboxing, data sovereignty erosion, and misalignment with local legal norms. Case studies from Ethiopia, Southeast Asia, and Latin America revealed concrete implications ranging from democratic backsliding to weakened legal oversight. However, the article also identified pathways toward reclaiming autonomy, including indigenous AI capacity-building, regional governance frameworks, and procurement reforms rooted in transparency and open-source mandates.

Theoretical reflection through the lens of surveillance capitalism and digital colonialism reframed the current trajectory as a continuation of asymmetrical power structures. The analysis underscored the urgent need for multi-level reforms to transition from passive technological recipients to proactive stewards of digital governance. Algorithmic sovereignty, as presented, is not simply a technical issue it is a foundational pillar of modern democratic statehood and social justice.

8.2. Risks of Passive Adoption vs. Active Agency

Passive adoption of foreign AI surveillance systems poses serious risks for national autonomy and civic freedoms. When countries import turnkey surveillance solutions without demanding access to source code, control over updates, or jurisdictional clarity on data storage, they risk embedding foreign control into critical governance functions. These systems, once deployed, are difficult to audit, adapt, or dismantle especially when legal, financial, or diplomatic obligations lock governments into long-term vendor agreements.

This technological dependence limits states' ability to enforce constitutional safeguards, protect citizens' rights, and uphold transparent governance. More dangerously, it grants foreign developers latent influence over public infrastructure, law enforcement, and civil registry systems. In some cases, foreign actors may retain kill-switch capabilities, inject algorithmic biases, or condition technical support on geopolitical alignment.

In contrast, active agency means asserting legal, technical, and normative control over AI systems. It involves developing domestic capacity, instituting procurement guidelines based on transparency and fairness, and insisting on interoperability with national regulatory frameworks. Agency also includes public engagement ensuring civil society and local communities understand, scrutinize, and co-design AI systems used to govern them. The difference between passive adoption and active agency defines whether AI becomes a tool of empowerment or a mechanism of control.

8.3. Role of International Institutions

International institutions like the United Nations (UN), World Trade Organization (WTO), and International Telecommunication Union (ITU) have a critical role to play in shaping the governance of cross-border AI systems. These bodies can help establish binding norms and non-binding guidelines that uphold algorithmic transparency, data sovereignty, and equitable technology transfer.

The UN can facilitate a global treaty on ethical AI deployment, especially in areas involving public surveillance, predictive policing, and biometric identification. A rights-based framework led by the UN Human Rights Council could integrate algorithmic risk assessments into global human rights reviews. The UNDP could further support capacity-building in low- and middle-income countries to audit and govern AI systems effectively.

The WTO should revisit trade agreements that touch on data flows, software-as-a-service models, and procurement sovereignty. Existing frameworks often favor large tech exporters and fail to provide protections for states seeking to regulate foreign surveillance systems. The WTO could help carve out regulatory space for countries implementing algorithmic accountability laws.

The ITU can set technical standards that ensure interoperability and auditability across AI systems. It could also act as a clearinghouse for best practices, independent testing labs, and certification of ethical compliance. Such initiatives would give the Global South tools to negotiate more equitable terms with AI vendors.

8.4. Recommendations for National Governments, Civil Society, and Technologists

For National Governments:

- Mandate source code transparency and enforce local access to AI system updates and data logs.
- Require algorithmic impact assessments before deployment of public-facing AI surveillance tools.
- Reform procurement frameworks to prioritize open-source, auditable, and locally adaptable solutions.
- Invest in national AI research centers and technical training programs to reduce dependency.
- Incorporate AI governance into constitutional law, ensuring judicial oversight and redress mechanisms.

For Civil Society:

- Advocate for public consultation on AI deployments affecting civil liberties, especially in law enforcement and border control.
- Develop AI literacy programs that enable communities to understand the implications of surveillance technologies.
- Establish watchdog coalitions to monitor foreign AI contracts and push for independent audits.
- Engage in strategic litigation when AI systems violate privacy rights or result in discriminatory outcomes.
- For Technologists and Developers:
- Design AI systems with modularity, allowing governments to tailor them to local needs.
- Contribute to open-source AI repositories that prioritize transparency and fairness.
- Collaborate with local stakeholders to ensure contextual relevance and ethical alignment of AI tools.
- Refuse to engage in projects where surveillance use lacks democratic legitimacy or oversight.
- The combined effort of these actors is essential to build a governance ecosystem where AI strengthens not undermines national autonomy and civil rights.

8.5. Future Research Directions

Several promising avenues exist for future research on algorithmic sovereignty. First, longitudinal studies are needed to assess the evolving impact of foreign surveillance technologies on institutional independence, electoral integrity, and public trust. Empirical work should explore how these systems influence policymaking, citizen behavior, and resistance movements over time.

Second, comparative legal research can illuminate the gaps and innovations in national AI regulations across the Global South. Such work would inform harmonized frameworks that can serve as building blocks for regional governance.

Third, technical research should focus on developing lightweight, explainable, and interoperable AI tools suited for resource-constrained environments. This includes algorithmic decolonization designing systems rooted in local languages, norms, and historical experiences.

Lastly, interdisciplinary research that merges political science, computer science, and postcolonial theory can provide richer insights into how AI reshapes sovereignty in an interconnected world. As algorithmic systems grow in scope and power, so too must our tools for analyzing and governing them.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ishkhanyan A. The sovereignty-internationalism paradox in AI governance: digital federalism and global algorithmic control. Discover Artificial Intelligence. 2025 Jun 23;5(1):123.

[2] Ishkhanyan A. Governing AI across borders: corporate power, state sovereignty and global regulation. Digital Policy, Regulation and Governance. 2025 Jun 24.

[3] Garcia EV. The technological leap of AI and the Global South: Deepening asymmetries and the future of international security. InResearch Handbook on Warfare and Artificial Intelligence 2024 Jul 23 (pp. 370-387). Edward Elgar Publishing.

[4] Souza J, Avelino R, da Silveira SA. Artificial intelligence: dependency, coloniality and technological subordination in Brazil. InElgar Companion to Regulating AI and Big Data in Emerging Economies 2023 Dec 5 (pp. 228-244). Edward Elgar Publishing.

[5] Sinha N. Aadhaar, AI, and Identity: Negotiating Power and Surveillance in the Global South. Социологическое обозрение. 2024;23(4):80-112.

[6] Adelakun Matthew Adebowale, Olayiwola Blessing Akinnagbe. Cross-platform financial data unification to strengthen compliance, fraud detection and risk controls. World J Adv Res Rev. 2023;20(3):2326–2343. Available from: https://doi.org/10.30574/wjarr.2023.20.3.2459

[7] Onuma EP. Multi-tier supplier visibility and ethical sourcing: leveraging blockchain for transparency in complex global supply chains. Int J Res Publ Rev. 2025;6(3):3579–93. Available from: https://doi.org/10.55248/gengpi.6.0325.11145

[8] Ilo E. Africa's Struggle for Sovereignty: Neo-Colonialism and External Control in the 21st Century. Abuja Journal of Humanities. 2025 Jun 9;6(1):187-94.

[9] Dorgbefu Esther Abla. Algorithmic bias and data ethics in automated marketing systems for manufactured housing affordability outreach. International Journal of Research Publication and Reviews. 2025;6(6). Available from: https://ijrpr.com/uploads/V6ISSUE6/IJRPR49463.pdf

[10] Jamiu OA, Chukwunweike J. DEVELOPING SCALABLE DATA PIPELINES FOR REAL-TIME ANOMALY DETECTION IN INDUSTRIAL IOT SENSOR NETWORKS. International Journal Of Engineering Technology Research & Management (IJETRM). 2023Dec21;07(12):497–513.

[11] Iqbal S, Tabeer S. Digital Strategic Autonomy in South Asia: Artificial Intelligence and Cyberspace. Journal of Security & Strategic Analyses. 2024 Jul 11;10(1):72-86.

[12] Andrew Nii Anang and Chukwunweike JN, Leveraging Topological Data Analysis and AI for Advanced Manufacturing: Integrating Machine Learning and Automation for Predictive Maintenance and Process Optimization (2024) https://dx.doi.org/10.7753/IJCATR1309.1003

[13] Calzada I. Postpandemic technopolitical democracy: Algorithmic nations, data sovereignty, digital rights, and data cooperatives. InMade-to-Measure Future (s) for Democracy? Views from the Basque atalaia 2022 Nov 26 (pp. 97-117). Cham: Springer International Publishing.

[14] Dorgbefu EA. Improving investment strategies using market analytics and transparent communication in affordable housing real estate in the US. GSC Adv Res Rev. 2023;17(3):181–201. doi: https://doi.org/10.30574/gscarr.2023.17.3.0480.

[15] Chari SG. Power, Pixels, and Politics: The Geopolitics of Emerging Technologies in the Digital Age. London Journal of Research In Humanities and Social Sciences. 2025 Feb 14;25(2):1-99.

[16] Durowoju Emmanuel, Salaudeen Habeeb Dolapo. Advancing lifecycle-aware battery architectures with embedded self-healing and recyclability for sustainable high-density renewable energy storage applications. World Journal of Advanced Research and Reviews. 2022 May;14(2):744–765. doi: https://doi.org/10.30574/wjarr.2022.14.2.0439.

[17] Calderaro A, Blumfelde S. Artificial intelligence and EU security: The false promise of digital sovereignty. European Security. 2022 Jul 3;31(3):415-34.

[18] Dorgbefu EA. Enhancing customer retention using predictive analytics and personalization in digital marketing campaigns. Int J Sci Res Arch. 2021;4(1):403–23. doi: https://doi.org/10.30574/ijsra.2021.4.1.0181.

[19] Ehdaee A. The Impact of 21st-Century Emerging Technologies on the Shift of Power in the International System. Legal Studies in Digital Age. 2024 May 27;3(2):153-64.

[20] Odunaike A. Integrating real-time financial data streams to enhance dynamic risk modeling and portfolio decision accuracy. Int J Comput Appl Technol Res. 2025;14(08):1–16. doi:10.7753/IJCATR1408.1001. Available from: http://www.ijcat.com/archives/volume14/issue8/ijcatr14081001.pdf

[21] Poudel J. Changing international system: The role of technology in the 21st century global power relations. PhD diss., Department of International Relations and Diplomacy. 2021 Apr.

[22] Glasze G, Cattaruzza A, Douzet F, Dammann F, Bertran MG, Bômont C, Braun M, Danet D, Desforges A, Géry A, Grumbach S. Contested spatialities of digital sovereignty. Geopolitics. 2023 Mar 15;28(2):919-58.

[23] Khalid AA. Armed with Algorithms: US-China Tech Rivalry and Its Strategic Implications for Pakistan. ASSAJ. 2025 Jun 27;3(02):2123-34.

[24] Dorgbefu EA. Advanced predictive modeling for targeting underserved populations in U.S. manufactured housing marketing strategies. Int J Adv Res Publ Rev. 2024 Dec;1(4):131–54. Available from: https://ijarpr.com/uploads/V1ISSUE4/IJARPR0209.pdf

[25] Mohamed S, Png MT, Isaac W. Decolonial AI: Decolonial theory as sociotechnical foresight in artificial intelligence. Philosophy & Technology. 2020 Dec;33(4):659-84.

[26] Bria F. Europe's path to digital independence. InUncertain Journeys into Digital Futures 2025 Mar 13 (pp. 19-34). Nomos Verlagsgesellschaft mbH & Co. KG.

[27] Zaheer I, Abbas A. Weaponizing Algorithms: China's Strategic AI Ecosystem and the Erosion of US Informational Hegemony. Annual Methodological Archive Research Review. 2025 Jul 22;3(7):228-47.

[28] Dorgbefu Esther Abla. Integrating marketing analytics and internal communication data to improve sales performance in large enterprises. World Journal of Advanced Research and Reviews. 2022;16(3):1371–1391. doi: https://doi.org/10.30574/wjarr.2022.16.3.1216

[29] Lin B. Beyond authoritarianism and liberal democracy: Understanding China's artificial intelligence impact in Africa. Information, Communication & Society. 2024 Apr 25;27(6):1126-41.

[30] Korkmaz E. Smart borders, digital identity and big data: how surveillance technologies are used against migrants. Policy Press; 2023 Dec 8.

[31] Joseph Kumbankyet. The AI Revolution in Finance: Building a Sustainable Future. February 2025. Joseph Kumbankyet; 2025. ISBN: 9798310623071.

[32] Soare SR. Politics in the machine: The political context of emerging technologies, national security, and great power competition. InEmerging technologies and international security 2020 Nov 25 (pp. 103-122). Routledge.

[33] Madianou M. Technocolonialism: When technology for good is harmful. John Wiley & Sons; 2024 Oct 16.

[34] Aradau C, Blanke T. Algorithmic reason: The new government of self and other. Oxford University Press; 2022.

[35] Adegboye Omotayo, Arowosegbe Oluwakemi Betty, Olisedeme Prosper. AI optimized supply chain mapping for green energy storage systems: predictive risk modeling under geopolitical and climate shocks 2024. International Journal of Advance Research Publication and Reviews. 2024 Dec;1(4):63–86. doi:10.55248/gengpi.6.0525.1801.

[36] Fratini S. The Sociotechnical Politics of Digital Sovereignty: Frictional Infrastructures and the Alignment of Privacy and Geopolitics. Available at SSRN 5192550. 2025 Mar 25.

[37] Onabowale Oreoluwa. Innovative financing models for bridging the healthcare access gap in developing economies. World Journal of Advanced Research and Reviews. 2020;5(3):200–218. doi: https://doi.org/10.30574/wjarr.2020.5.3.0023

[38] Zuboff S. Surveillance capitalism or democracy? The death match of institutional orders and the politics of knowledge in our information civilization. Organization Theory. 2022 Nov;3(3):26317877221129290.

[39] Durowoju, Emmanuel & Salaudeen, Habeeb. (2022). Advancing lifecycle-aware battery architectures with embedded self-healing and recyclability for sustainable high-density renewable energy storage applications. World Journal of Advanced Research and Reviews. 14. 744-765. 10.30574/wjarr.2022.14.2.0439.

[40] Adelakun Matthew Adebowale, Olayiwola Blessing Akinnagbe. Leveraging AI-driven data integration for predictive risk assessment in decentralized financial markets. Int J Eng Technol Res Manag. 2021;5(12):295. Available from: https://doi.org/10.5281/zenodo.15867235