African smart cities: A critical analysis

An exercise in open source intelligence using an AI-powered search engine.

Bill Anderson, Data Landscapers – January 2026

Introduction

It may be strange to start a paper with its methodology, but in this case it is necessary. This entire study was researched and written by Perplexity, an AI-powered answer engine that combines large language models with real-time internet search capabilities. Unlike traditional search engines that return lists of links, Perplexity interprets natural language questions, conducts comprehensive web searches across multiple sources and, most importantly, generates results with inline citations linking to original sources. This transparency in sourcing enables relatively easy verification of information to maintain research rigour. My role in this, as in all my open source intelligence projects, is to design the concept, build metadata, write instructions and review outcomes. **The full methodology, outlining the design of the project through incremental iterative interactions with Perplexity, can be found here.**

This analysis examines initiatives across twelve major African urban centres: Abidjan, Accra, Cairo, Dakar, Johannesburg, Kampala, Kigali, Lagos, Lusaka, Nairobi, Rabat, and Tunis. The selection, based on rankings in the African Smart City Index 2024, reflects a spectrum of development levels, from emerging technology hubs like Nairobi and Kigali to established metropolitan centres such as Johannesburg and Cairo, alongside rapidly urbanising cities like Lagos and Accra.

Nearly all twelve cities have deployed or are planning surveillance systems with facial recognition capabilities, frequently supplied by Chinese technology firms. Intelligent transport systems feature prominently in Nairobi, Johannesburg, Cairo, and Rabat. Digital government platforms have been implemented across most cities, with varying degrees of comprehensiveness and citizen uptake. Mobile money systems have achieved remarkable success in East Africa, with Kenya's M-Pesa serving as a continental model. Greenfield smart city developments are also emerging, from Egypt's New Administrative Capital to Senegal's Diamniadio Lake City and Morocco's Mohammed VI Technopolis.

A central finding of this analysis is that the "smart city" model as currently implemented across Africa functions, in significant part, as a vehicle for mass surveillance. Monitoring infrastructure — overwhelmingly supplied by Chinese technology firms operating under opaque contracts — is being normalised through public safety branding, deployed ahead of any legal framework, and built in ways that create permanent, difficult-to-reverse capabilities for state control. This paper examines that concern alongside related questions of governance, financing, ownership, inclusivity, and accountability.

While smart city initiatives across these twelve cities have generated tangible benefits in service delivery, financial inclusion, and environmental management, their distribution remains uneven and their sustainability uncertain. The analysis that follows documents those benefits briefly before turning in greater detail to the governance failures, financial dependencies, and surveillance risks that pose significant threats to rights, equity, and democratic governance.

Benefits

Digital government platforms have demonstrably improved access to public services in several cities. Nairobi's eCitizen portal provides access to over 16,000 government services, significantly reducing the time and cost citizens previously expended navigating bureaucratic processes. Kigali's Irembo platform has achieved remarkable uptake with over 3 million registered users accessing services including birth certificates, business registration, and driving licences through digital channels. Revenue collection has improved through digital systems in Accra, Lagos, and Nairobi, reducing leakage and improving fiscal capacity.

Financial inclusion has advanced dramatically through mobile money systems, particularly in East Africa. Kenya's M-Pesa has become the continental exemplar, providing financial services to previously unbanked populations and enabling digital economic participation. Nairobi's technology startup ecosystem secured $638 million in venture capital funding in 2024, and Lagos has emerged as West Africa's technology hub. Smart waste management systems have improved collection efficiency in Kigali, and smart metering has reduced non-revenue water losses in several cities. Intelligent transport systems have improved traffic flow in Cairo and Nairobi, though benefits remain concentrated in affluent corridors.

These gains are real. They are, however, insufficient to justify current approaches when set against the governance failures, financial dependencies, exclusionary patterns, and surveillance expansion documented below.

Governance

Governance of smart city initiatives exhibits troubling patterns of institutional fragmentation, policy incoherence, and capacity deficits. Rather than integrated smart city strategies with clear accountability, most cities display disconnected projects operating under different institutional arrangements with minimal coordination. In Nairobi, the county government, national government, urban roads authority, and national police all operate separate systems with no overarching coordination. Similar fragmentation appears in Johannesburg and Cairo. Resources are wasted on duplicative and incompatible technologies, and private vendors exploit coordination gaps to lock different agencies into proprietary systems.

Regulatory frameworks consistently lag technological deployments. Data protection regulations frequently lack implementing rules, resourced enforcement agencies, or effective penalties. Procurement regulations designed for traditional infrastructure prove inadequate for digital technologies, creating opportunities for corruption. Multi-stakeholder governance remains largely rhetorical. Civil society participation is superficial, limited to consultation ceremonies rather than genuine co-design. Marginalized communities facing the sharpest impacts of smart city deployments have minimal voice in processes dominated by officials and vendors.

Financing

The financing architecture of smart city initiatives reveals troubling patterns of external dependency, debt accumulation, and opacity. Nairobi alone has accumulated over $1.3 billion in documented external borrowing for smart city infrastructure, from Korean, Chinese, and Italian sources. Egypt's New Administrative Capital, with total costs estimated in the tens of billions, has been financed through multiple external sources including Chinese loans and UAE investments, contributing to debt levels that triggered an IMF programme.

Contracts for Chinese-financed projects typically include confidentiality clauses preventing public disclosure of loan conditions, interest rates, repayment schedules, and collateral arrangements. Citizens are asked to service debts whose terms remain

unknown. When technology vendors also provide or arrange financing, they become both creditors and suppliers — an arrangement that drives up costs, discourages competitive bidding, and locks cities into vendor ecosystems determined by financing sources rather than local need.

Ownership

Chinese technology firms, particularly Huawei and its surveillance subsidiary Hikvision, dominate smart city implementations across the majority of the twelve cities. Nairobi's Safe City surveillance system was implemented by Huawei, which also supplied the data centre infrastructure for Konza Technopolis. Kampala's Safe City CCTV network was installed by Huawei. Lagos, Cairo, Lusaka, Kigali, and others have similarly turned to Chinese firms for surveillance and smart city infrastructure.

The nature of these vendor relationships reflects technology provision rather than genuine partnership. African governmental entities function primarily as clients purchasing complete technology solutions. Vendors implement pre-packaged systems with minimal local adaptation, provide training limited to basic operation, and depart leaving governments dependent on vendor support for any substantial maintenance or modification. Data ownership structures remain fundamentally unclear. Contracts rarely provide public clarity on data ownership, access rights, retention obligations, or exit procedures. Governments own expensive physical equipment they cannot independently operate, while vendors retain the intellectual property and technical capacity that determines functionality.

Proprietary technologies create deep lock-in. When surveillance systems use proprietary video formats and algorithms, governments cannot switch vendors without replacing entire infrastructure. Financial lock-in compounds this: governments have invested billions in smart city infrastructure, and switching to alternative vendors requires writing off these investments while incurring new costs. Once locked in, vendors can increase prices for maintenance and upgrades without competitive pressure.

Inclusivity

Smart city initiatives demonstrate alarming patterns of exclusion that contradict the rhetoric of inclusive digital transformation. Digital infrastructure deployment exhibits stark spatial inequalities. Affluent neighbourhoods receive high-speed connectivity and

dense smart city infrastructure; informal settlements that house significant proportions of urban populations experience dramatically inferior connectivity. In Nairobi's Mathare informal settlement, residents face limited reliable internet access despite proximity to the city centre. Johannesburg's spatial apartheid legacy persists in digital infrastructure distribution.

Even where infrastructure exists, affordability barriers remain prohibitive. Internet costs, though declining, consume significant portions of household budgets for low-income families. Smartphone ownership remains limited among the poorest populations. Women experience lower mobile phone ownership, internet access, and digital literacy than men across African contexts. Older adults face exclusion as traditional in-person services are withdrawn without adequate digital alternatives. Informal economy participants — large proportions of urban workforces — are systematically excluded by systems designed around formal economy assumptions of registered addresses, bank accounts, and tax identification numbers.

Accountability

Accountability mechanisms for smart city initiatives remain severely underdeveloped. Procurement transparency is consistently inadequate. Contracts are often awarded through non-competitive processes justified by urgency, technical complexity, or national security. Chinese-financed projects exemplify the pattern: bundled financing-procurement arrangements predetermine technology suppliers, eliminating meaningful competition, while confidentiality clauses prevent public scrutiny.

Performance accountability is undermined by absent metrics and weak enforcement of contractual obligations. Vendor claims about system capabilities frequently exceed realised performance, yet misrepresentation carries minimal consequences. Data governance accountability is particularly weak despite profound rights implications. Citizens have minimal visibility into what data smart city systems collect, who has access, and for what purposes it is used. Data breaches often go unreported. Participation mechanisms prove weak or absent: consultation processes, when they occur, take place after key decisions are made, reducing participation to rubber-stamping.

Surveillance

Surveillance systems represent the most troubling dimension of smart city initiatives across the twelve cities. Extensive deployment of monitoring technologies is proceeding with minimal legal frameworks, inadequate oversight, limited transparency, and profound implications for privacy, freedom of expression, freedom of association, and political participation. The normalisation of comprehensive monitoring under "smart city" and "public safety" branding obscures the fundamental transformation of state-society relationships that ubiquitous surveillance enables.

The scale and sophistication of deployed systems is significant. Nairobi's Safe City network comprises approximately 2,000 CCTV cameras with facial recognition capabilities, operating 24/7 with footage stored in cloud systems managed by Huawei. Johannesburg has deployed extensive CCTV networks across the city, with particular density in commercial districts. Cairo's surveillance infrastructure has expanded dramatically. Lagos, Kampala, Kigali, Rabat, Tunis, Lusaka, Dakar, Accra, and Abidjan have all deployed or announced surveillance systems, typically implemented by Chinese technology firms.

These systems extend far beyond traditional CCTV. Facial recognition enables identification and tracking of individuals across urban space. Licence plate recognition tracks vehicle movements and location histories. Integration with national ID systems, vehicle registration, criminal records, and mobile phone records enables comprehensive profiling. Some systems incorporate behavioural analysis algorithms claiming to predict suspicious activities. Video analytics enable retrospective searches for specific individuals across time and space.

Huawei's dominant role raises sovereignty and security concerns beyond the domestic surveillance implications. China's National Intelligence Law requires organisations and citizens to support and cooperate with state intelligence work, creating legal obligations on Chinese firms that may conflict with host country data sovereignty. African governments operating surveillance systems dependent on Chinese technology firms cannot guarantee that surveillance data remains exclusively under their control. Security researchers have documented serious vulnerabilities in Hikvision cameras widely deployed in African cities, including remote access vulnerabilities allowing unauthorised control.

Legal frameworks governing surveillance remain grossly inadequate. Most countries lack dedicated surveillance legislation establishing permissible purposes, authorisation requirements, oversight mechanisms, data retention limits, and redress procedures. Data protection frameworks, where they exist, typically contain broad exemptions for security and law enforcement that effectively exclude surveillance from privacy protections. Oversight mechanisms prove profoundly inadequate: independent oversight bodies capable of accessing surveillance systems, reviewing footage, and investigating complaints rarely exist.

The chilling effects of surveillance on freedom of expression and association deserve emphasis. When citizens know or suspect that their movements and associations are monitored, self-censorship increases. Political organising becomes riskier as surveillance enables identification of activists and anticipatory disruption of mobilisation. Journalists investigating government actions face heightened risks. Evidence from multiple contexts suggests that surveillance cameras concentrate in poor neighbourhoods and informal settlements rather than affluent areas, inverting any rational crime-prevention logic and serving social control objectives. Algorithmic bias in facial recognition compounds these problems: systems trained primarily on lighter-skinned faces perform poorly on darker-skinned individuals, creating higher false positive rates and discriminatory outcomes.

A particularly alarming dimension is normalisation by gradual expansion. Initially, cameras appear in high-crime areas with public safety justifications that attract broad support. Coverage expands with minimal public discussion. By the time surveillance becomes comprehensive, resistance potential has diminished and reversal becomes politically difficult. Surveillance systems built under one regime remain available to successors regardless of political orientation, creating path-dependent infrastructure for control that outlasts the governments that deploy it.

Conclusion

This analysis has revealed a complex landscape where genuine benefits coexist with profound governance challenges, financial sustainability concerns, inclusivity deficits, accountability gaps, and surveillance risks. The African Union's data, digital transformation, and AI frameworks provide clear continental commitments against which current trajectories fall short. Closing the gap requires moving beyond policy articulation to enforcement mechanisms, capacity building, resource allocation, and genuine accountability.

The path forward requires acknowledging that smart city benefits are real but insufficient to justify current approaches' governance failures, financial dependencies, exclusionary patterns, accountability deficits, and surveillance expansion. A fundamentally different approach must prioritise governance before technology, rights alongside efficiency, inclusion as prerequisite for legitimacy, transparency as foundation for accountability, and African sovereignty over digital transformation pathways. The question is not whether African cities should pursue digital transformation — they must and will — but whether that transformation serves African peoples and their rights, or vendor profits and state surveillance capacity.

Sources and Methodology

Case Studies

The twelve case studies are available here:

- **Abidjan**
- **Accra**
- **Cairo**
- **Dakar**
- **Johannesburg**
- **Kampala**
- **Kigali**
- **Lagos**
- **Lusaka**
- **Nairobi**
- **Rabat**
- **Tunis**

Each city analysis draws on news sources, academic literature, government documents, and data collection spanning ownership, finance, technology, governance, surveillance, performance, social impact, environmental impact, economic benefit, and systems integration. These sources can be found in the annexes to each case study.

(The separation of the sources from the main body of text is not ideal but was the result of technical issues instructing the report writing engine.)

Annotated Bibliography

- An annotated bibliography of over 100 academic papers and policy briefs

Methodology

- The full methodology, outlining the design of the project through incremental iterative interactions with Perplexity, can be found here.

Data

- CSV download
- Metadata download