IIAR JOURNALS

Innovating Knowledge. Advancing Research.

IIAR Journal of Urban Development, Infrastructure, and Smart Cities

Vol 1, No 1, 2026

Urban Surveillance, Safety and the Right to the City: A Theoretical Analysis of AI-Enabled Policing Infrastructure, Public Space and Civic Freedom

Paul Idowu Bamigbola[1], NWOGBOJI Emmanuel Usulor[2], OGAH SUNDAY OGBO[3], Atolagbe Umar Kawu[4]

[1,2,3,4] Veristzon Global Research Lab

ABSTRACT

Cameras, facial recognition, licence-plate readers and predictive policing analytics are being installed in African cities as safe-city infrastructure, often financed and supplied through foreign partnerships, in response to real problems of crime and insecurity. This theoretical paper analyses urban surveillance as an infrastructure of public space. Drawing on urban theory including the right to the city, on surveillance studies, on criminological evidence on the effects of camera surveillance on crime, and on recent research on smart-policing and safe-city deployments in Africa, it distinguishes three effects of surveillance infrastructure, on safety (whether crime falls), on behaviour (how people use public space) and on power (who can watch whom), and argues that the evidence for the first is narrower than claimed, the second is systematically underestimated, and the third is the effect that persists after the technology's crime-fighting value is exhausted. The paper develops a framework in which the legitimacy of urban surveillance depends on effectiveness, proportionality, accountability and the preservation of anonymous public presence, derives seven propositions about the conditions under which surveillance improves safety without eroding civic freedom, and examines the governance problems created when the infrastructure is vendor-controlled and the data leaves the jurisdiction. Nigeria's safe-city and security-technology initiatives, with Lagos as the anchoring case, ground the analysis. The paper closes with implications for city and state governments, regulators, vendors and the research agenda of African urban studies. It concludes that the right to the city in the age of the camera is the right to be in public without being known, and that a surveillance infrastructure which preserved that right while reducing the crimes that threaten it would be a genuine contribution to urban safety, whereas one that does not is a contribution to something else.

Keywords: urban surveillance; smart policing; facial recognition; CCTV; public space

Urban Surveillance, Safety and the Right to the City: A Theoretical Analysis of AI-Enabled Policing Infrastructure, Public Space and Civic Freedom

1. INTRODUCTION

Across Africa, cities are acquiring eyes. Safe-city and smart-city programmes have installed networked cameras, automatic number-plate recognition, facial-recognition capability and integrated command centres in capitals and commercial hubs from Nairobi to Kampala, Lusaka, Dakar, Kigali and Lagos, frequently supplied by a small number of foreign vendors under state-to-state financing arrangements (Da Vinha, 2024; Lin, 2024). The stated purpose is safety. Crime, kidnapping, terrorism and traffic death are real and pressing, and governments that cannot police their cities by conventional means are offered a technology that promises to see everything, remember everything and respond in real time. Artificial intelligence is the latest addition: the camera that merely recorded now identifies, tracks, predicts and alerts (Yigitcanlar et al., 2026; Mhlanga, 2026).

This paper examines urban surveillance as what it is physically: an infrastructure of public space, laid over streets, markets, junctions and squares, whose effects on the city are not limited to the crimes it detects. It asks three questions. Does the infrastructure make cities safer? What does it do to the way people use public space? And who, once it is installed, can watch whom? The paper argues that these three questions correspond to three distinct effects, on safety, on behaviour and on power, and that the public case for surveillance rests almost entirely on the first while the lasting consequences lie in the second and third.

The argument is theoretical and normative rather than empirical. It draws on the right-to-the-city tradition in urban theory and its recent application to the smart city in the Global South (Alizadeh & Prasad, 2024; Dorostkar & Najarsadeghi, 2026), on surveillance studies and the legal scholarship on facial recognition in public space (Gikay, 2023; Zalnieriute, 2025; Gabrielli, 2025), on the criminological evidence on camera surveillance and crime (Lang et al., 2025; Widmark, 2026), on the predictive-policing literature (Almasoud & Idowu, 2025; Kim & Chung, 2025), and on the recent research on safe-city deployments and digital authoritarianism in Africa (Da Vinha, 2024; Lin, 2024; Achinivu, 2025). From these it builds a framework for assessing the legitimacy of urban surveillance and derives propositions about the conditions under which surveillance improves safety without eroding civic freedom.

The analysis opens with the safe-city model and its critics, and then characterises public space and insecurity in African cities. It develops the three-effect decomposition before presenting the legitimacy framework and the propositions that follow from it, and it gives separate attention to the governance problems created when the infrastructure is vendor-controlled and its data leaves the jurisdiction, before anchoring the analysis in Nigeria and Lagos and drawing out its implications.

2. LITERATURE REVIEW

2.1 The Safe-City Model and Its Critics

The model

The safe city is the security module of the smart city: a network of cameras and sensors feeding a command centre where video is monitored, analysed and linked to police dispatch, with analytics layered on top, number-plate recognition, facial matching against watchlists, behaviour detection, and increasingly predictive models that direct patrols to forecast hotspots. Reviews of smart-city governance list public safety among the principal applications (Almulhim & Yigitcanlar, 2025; Das et al., 2026), and the African smart-city literature records safe-city components in most national and city strategies (Maatallah et al., 2026). The model's appeal to governments is straightforward: it offers visible action against insecurity, it can be financed and delivered as a package, and it extends the state's capacity to see into a city it otherwise governs partially.

The critics

Three strands of criticism have formed. The first concerns effectiveness. The criminological evidence on camera surveillance is longer and more cautious than the marketing. Lang et al. (2025), assessing camera installation at property-crime hotspots, find effects that are real but modest and conditional on context, consistent with a literature that finds camera surveillance most effective for vehicle and property crime in enclosed settings such as car parks and least effective for violent crime in open public space. Widmark (2026), in a systematic review and meta-analysis of environmental-design approaches to residential crime prevention, situates camera

© IIARJournal. All rights reserved.

surveillance within a broader set of measures whose effects depend on implementation and on the crime type. The predictive-policing literature is more sceptical still: Almasoud and Idowu (2025) review the fairness problems of predictive systems, and Kim and Chung (2025), in a systematic review, call for a more contextual approach that attends to the data, institutional and social conditions in which predictions are made and acted on.

The second strand concerns civic freedom. Gikay (2023) analyses the regulation of live facial recognition by law-enforcement authorities in public space and proposes an incremental approach, recognising that the technology's capacity to identify every passer-by changes the character of public space itself. Zalnieriute (2025) focuses on the chilling effect of facial-recognition surveillance on protest and assembly, and Gabrielli (2025) examines the risk that its use at peaceful protests amounts to mass surveillance incompatible with human-rights protection. Yigitcanlar et al. (2026) treat AI-enabled urban surveillance as a mode of statecraft in which safety narratives obscure behavioural regulation, data extraction and the consolidation of power. Tedeschi (2024) frames the issue as one of digital spatial justice, and Dorostkar and Najarsadeghi (2026) describe the struggle over urban public space in the digital city as a struggle over surveillance, exclusion and digital rights.

The third strand concerns Africa specifically. Da Vinha (2024) asks for whom African smart cities are smart and finds that safe-city systems supplied by Chinese vendors have been used to extend state control as readily as to reduce crime. Lin (2024) argues that the effect of Chinese artificial intelligence in Africa cannot be captured by the binary of authoritarianism and liberal democracy and must be understood through African governments' own purposes. Achinivu (2025) examines digital authoritarianism in Nigeria and finds that the drivers are domestic as much as imported. Ayodele (2026) shows that surveillance in African peacebuilding is shaped by local innovation and local politics rather than simply transferred from abroad. The critical smart-city literature supplies the frame: Datta (2023) on the digitalising state and its informational peripheries, Alizadeh and Prasad (2024) on the right to the smart city in the Global South, Bandauko and Nutifafa Arku (2023) on the exclusionary character of African smart-city interventions, and Sen et al. (2026) on the informal settlements that subsidise the smart enclave.

The critics establish that the safe city's claims are overstated and its risks understated. What they have not supplied is a structure for assessing any particular deployment. That is the task of the following sections.

2.2 Public Space and Insecurity in African Cities

Public space as livelihood

Public space in African cities is not primarily recreational. It is where a large share of the population works: street vendors, informal transport operators, artisans, hawkers, porters and the many whose livelihoods depend on being present, visible and anonymous in the street. It is also where the informal city meets the formal, the market, the junction, the terminal, and where the state's presence is most intermittent. The right-to-the-city tradition, developed for Northern cities, acquires a sharper meaning here: the right to be in public space without being identified, recorded or moved on is a condition of economic survival for the majority (Alizadeh & Prasad, 2024; Dorostkar & Najarsadeghi, 2026).

Insecurity as real and unevenly distributed

Insecurity in African cities is not a pretext. Violent crime, kidnapping, robbery and, in Nigeria, insurgency and banditry impose real costs on real people, and the demand for safety is strongest among the poor, who are most exposed and least protected. The distribution of security technology, however, follows a different map. Abraham et al. (2025), examining unguarded areas and insecurity in Nigeria, find that security technologies are concentrated in the places the state already governs and absent from the rural and peripheral spaces where insecurity is worst, so that the technology's deployment maps onto existing state presence rather than onto need. The same pattern holds within cities: cameras cluster in central business districts, government quarters and elite residential areas, and are sparse in the informal settlements where most residents live and where the demand for protection is greatest.

Policing as a relationship

Surveillance is introduced into a relationship between police and public that in many African cities is characterised by low trust, allegations of extortion and brutality, and the experience of policing as a threat rather than a protection. Van Riet (2023) describes the asymmetries of security provision in a South African city where private companies, neighbourhood watches and police

© IIARJournal. All rights reserved.

overlap, so that who is protected depends on who can pay. In this setting a technology that extends the police's capacity to see is experienced differently by those who expect to be protected and those who expect to be targeted. The safety case for surveillance assumes the first; the lived experience of many is the second.

3. CONCEPTUAL FRAMEWORK

3.1 Three Effects of Surveillance Infrastructure

Surveillance infrastructure has three effects that are analytically distinct, evidentially unequal and politically confused.

Safety: narrower than claimed

The first effect is on crime. The evidence, reviewed above, supports a modest and conditional claim: camera surveillance reduces certain crimes, vehicle theft, property crime, offences in enclosed and well-monitored spaces, where cameras are actively monitored, linked to a capable response, and combined with other measures such as lighting and design (Lang et al., 2025; Widmark, 2026). It does not support the claim that pervasive camera networks reduce violent crime in open public space, nor that facial recognition or predictive analytics add substantially to the effect, and the predictive-policing literature documents the risk that forecasts reproduce the biases of the data on which they are trained and direct enforcement toward already over-policed populations (Almasoud & Idowu, 2025; Kim & Chung, 2025). In African cities the conditions for even the modest effect, active monitoring, capable and trusted response, are frequently absent, so that the realised safety effect of safe-city deployments is likely to be smaller than the already modest Northern evidence would predict. The safety effect is real, bounded and dependent on institutional capacity the technology does not supply.

Behaviour: systematically underestimated

The second effect is on how people use public space. Surveillance changes behaviour whether or not it changes crime, and it does so most among those whose presence in public space is precarious. The legal scholarship on facial recognition documents the chilling effect on assembly and protest (Zalnieriute, 2025; Gabrielli, 2025; Gikay, 2023): people who know they may be identified do not gather, or gather differently. Yigitcanlar et al. (2026) note that the visibility of monitoring works as a disciplinary signal. In cities where public space is livelihood, the behavioural effect extends beyond protest. Vendors, hawkers and informal operators whose activities are tolerated but not licensed avoid surveilled space, and the enforcement that cameras enable, against street trading, informal transport, unauthorised structures, reshapes who can be where. This effect is almost never measured in safe-city evaluations, which count crimes and arrests, and it is therefore systematically underestimated. It falls hardest on the informal majority.

Power: the effect that persists

The third effect is on who can watch whom. A surveillance infrastructure, once installed, is a capability held by whoever controls the cameras, the analytics and the data. Its crime-fighting value is bounded and decays as offenders adapt; its capacity to identify, track and record persists and can be turned to any purpose its controller chooses, political opposition, journalists, protesters, communities marked for clearance. Da Vinha (2024) and Achinivu (2025) document this turn in African cases, and Lin (2024) shows that the purpose is set by the African government, not only by the vendor. Datta's (2023) digitalising state and Yigitcanlar et al.'s (2026) surveillance-as-statecraft describe the same mechanism: the infrastructure built for safety becomes the infrastructure of governance. This is the effect that persists after the safety effect is exhausted, and it is the effect the safety case does not mention.

The confusion

The three effects are politically confused because the first is used to justify the infrastructure, the second is not counted, and the third is the lasting result. A government that installs cameras to fight crime acquires, as a by-product it may or may not have intended, a capacity to regulate behaviour in public space and to watch anyone it chooses. The framework that follows separates the effects so that each can be assessed and so that the by-product is treated as the primary object of governance.

3.2 A Legitimacy Framework and Propositions

Four criteria

The framework holds that the legitimacy of an urban surveillance deployment depends on four criteria, each corresponding to one of the effects or to the relationship between them. Effectiveness asks whether the deployment can be expected, on the evidence, to reduce the crimes it is justified by, under the institutional conditions that actually obtain. Proportionality asks whether the behavioural and power effects are proportionate to the safety

© IIARJournal. All rights reserved.

effect, whether the chilling of assembly, the displacement of informal livelihoods and the creation of a tracking capability are justified by the crime reduction achieved. Accountability asks who controls the infrastructure and its data, under what rules, with what oversight and with what remedies for misuse. Preservation of anonymous public presence asks whether the deployment leaves residents a practical capacity to be in public space without being identified, whether, in the terms of the right to the city, the city remains a place one can be in without being known.

Propositions

Proposition 1. The safety effect of urban surveillance is bounded by the capacity of the response it feeds, and in cities where monitoring, dispatch and trusted police response are weak, the realised effect will be substantially smaller than the Northern evidence base predicts; evaluation must measure realised rather than assumed effects. Proposition 2. The behavioural effect of surveillance on public space falls disproportionately on those whose presence is informal or tolerated, and will reduce the livelihood access of the urban poor in proportion to the enforcement capability the surveillance enables. Proposition 3. The power effect of surveillance infrastructure outlasts its safety effect, so that the governance of the capability must be designed for the period after its crime-fighting rationale has weakened. Proposition 4. Facial recognition and predictive analytics add more to the power effect than to the safety effect, and their inclusion in a deployment shifts the proportionality balance against legitimacy unless specific safeguards are present. Proposition 5. Surveillance deployed in a low-trust policing relationship will reduce rather than increase perceived safety among populations that expect to be targeted, and the net effect on public use of space will be negative for those populations. Proposition 6. The spatial distribution of surveillance follows existing state presence rather than need, so that safe-city deployments will protect the already-protected and leave the most insecure spaces unguarded unless distribution is an explicit design criterion (Abraham et al., 2025). Proposition 7. Where the infrastructure, analytics or data are controlled by a vendor or a foreign party, accountability cannot be secured by domestic rules alone, and the legitimacy of the deployment depends on contractual, technical and jurisdictional arrangements that are rarely in place.

Using the framework

The framework is designed to be applied before a deployment is procured, when the choices that determine its effects are still open, and after it is installed, when its actual effects can be measured. For governments, it supplies the questions that the safety case omits. For regulators and courts, it supplies criteria for review. For researchers, it supplies propositions that comparative study of African safe-city deployments can test.

4. ANALYSIS AND DISCUSSION

4.1 Vendor Control and Data Governance

The African safe city has a feature that distinguishes it from most Northern deployments: the infrastructure is usually supplied, financed, installed and often serviced by a foreign vendor, and the data it generates may be processed on vendor systems or transmitted outside the jurisdiction. Da Vinha (2024) and Lin (2024) describe the Chinese-supplied systems in a number of African capitals, and Yang et al. (2026), in a systematic review of regulation and governance in smart-city infrastructure, identify algorithmic surveillance and vendor lock-in as linked risks and propose data sovereignty and procurement power as the levers available to governments.

The governance problem has three layers. The first is control: the government that commissions the system may not control its analytics, its updates or its data architecture, and may be unable to audit what the system does. The second is jurisdiction: data processed or stored abroad is subject to foreign law and foreign access, and the residents it describes have no remedy. The third is dependence: a city whose security infrastructure is vendor-serviced cannot change course without the vendor, and the vendor's commercial and political interests enter the city's security governance. Achinivu (2025) and Ayodele (2026) are careful to locate the drivers of surveillance in African politics rather than solely in foreign supply, and Lin (2024) resists the authoritarian-export narrative; the point here is narrower. Whatever the purpose, accountability for a surveillance infrastructure requires control of it, and control is what vendor-supplied systems most often lack.

Proposition 7 follows, and so does its remedy. Legitimacy under vendor supply requires, at minimum, contractual rights to audit analytics and data flows, technical arrangements that keep data within the jurisdiction and under domestic access

© IIARJournal. All rights reserved.

rules, procurement conditions that prevent lock-in, and a domestic legal framework, of the kind Gikay (2023) proposes incrementally for facial recognition, that governs use regardless of supplier. Where these are absent, the deployment fails the accountability criterion however sound its safety case.

4.2 Nigeria and Lagos as an Anchoring Case

Nigeria faces insecurity of a severity that makes the demand for surveillance technology entirely understandable: insurgency in the north-east, banditry and kidnapping across the north-west and centre, and urban crime in its cities. Federal and state governments have invested in camera networks, command centres and security-technology partnerships, and Lagos State has been the most active, with city-wide camera deployment, traffic enforcement cameras, a state emergency command centre and the branding of Lagos as a smart and safe city. Achinivu (2025) examines the Nigerian case as one of digital authoritarianism whose drivers are domestic, and Egba et al. (2026) record the enthusiasm of Nigerian public institutions for artificial intelligence in public service.

Safety

Proposition 1 applies directly. Lagos's camera networks feed a response capacity, police, emergency services, traffic enforcement, that is uneven, under-resourced and, in the experience of many residents, untrusted. The realised safety effect is therefore bounded by that capacity, and the deployments have been most visibly effective in traffic enforcement, where the response is a fine rather than a patrol, and least in violent crime. Proposition 6 applies as well: the cameras are densest on Victoria Island, Ikoyi, Lekki and the government corridors of Alausa and Ikeja, and sparsest in the settlements where most residents live. Abraham et al.'s (2025) finding that Nigerian security technology follows state presence rather than insecurity holds within the city as between city and countryside.

Behaviour

Lagos's public space is the livelihood of millions, street traders, danfo operators, okada riders, hawkers at junctions, whose activities are variously prohibited, tolerated and taxed. Camera-enabled enforcement against street trading and informal transport, and the use of surveillance to support the clearance of informal settlements that Olajide and Lawanson (2025) document, illustrate Proposition 2: the behavioural effect falls on the informal majority, and it reshapes who can be where in the city. Where the same infrastructure is turned toward assembly and protest, as the capability permits, the chilling effect that Zalnieriute (2025) and Gabrielli (2025) describe follows, and Achinivu's (2025) account of digital authoritarianism in Nigeria locates the drivers of such use in domestic politics rather than only in imported technology.

Power

Proposition 3 and Proposition 7 describe the Lagos infrastructure's future. The cameras will outlast the crime wave that justified them; the capability to identify, track and record will remain; and its governance will depend on arrangements with vendors and on a domestic legal framework that Nigeria's Data Protection Act 2023 has begun to supply but that does not yet specifically govern public-space surveillance by security agencies. Whether the capability is used for safety, for the regulation of informal life, or for the surveillance of political opponents is a question the technology does not settle and the framework insists be asked.

The possibility

Lagos could build a legitimate surveillance infrastructure. It would be distributed by need rather than by existing state presence; it would be evaluated by realised crime reduction rather than by cameras installed; it would exclude facial recognition and predictive analytics until specific safeguards were in place; it would be governed by rules on retention, access and use that protected anonymous public presence; and its data and analytics would be under domestic control and subject to audit. None of this is beyond the state's capacity. All of it requires that safety be treated as one of three effects rather than the only one.

4.3 Implications

For city and state governments

Governments procuring surveillance infrastructure should require, before procurement, an assessment against all four criteria: expected effectiveness under actual response capacity, proportionality of behavioural and power effects, accountability arrangements including vendor and data control, and preservation of anonymous public presence. They should distribute deployments by insecurity rather than by state presence, should evaluate by realised outcomes, and should treat facial

© IIARJournal. All rights reserved.

recognition and predictive analytics as separate decisions requiring separate justification.

For regulators and legislatures

The use of surveillance in public space by security agencies needs a specific legal framework, incremental, as Gikay (2023) proposes, covering what may be collected, how long it is retained, who may access it, for what purposes it may be used, and what remedies exist. Data-protection law is a foundation but not a substitute. Regulators should have audit rights over vendor-supplied analytics and should require that data remain within the jurisdiction.

For vendors and financiers

Vendors and the financing arrangements that deliver safe-city systems to African governments bear responsibility for the governance gaps the systems create. Contracts that confer audit rights, keep data in-country and prevent lock-in are feasible and should be standard. Financiers should condition support on their presence.

For research

The propositions are testable. Realised safety effects can be measured by comparing crime trends across surveilled and unsurveilled areas with similar response capacity (Proposition 1). Behavioural effects can be measured by observing the use of public space by informal workers before and after deployment (Proposition 2). The spatial distribution of surveillance relative to insecurity can be mapped (Proposition 6). The governance arrangements of vendor-supplied systems can be documented (Proposition 7). The African safe city is almost entirely absent from the peer-reviewed criminological and urban literatures; the Lagos, Nairobi, Kampala and Kigali deployments need study on their own terms rather than through the authoritarian-export lens alone, as Lin (2024) and Ayodele (2026) urge.

Limits

The paper is conceptual. It treats the three effects as separable when deployments produce them together. It draws its criminological evidence from Northern studies whose transfer to African conditions is itself a proposition to be tested. It treats the informal majority as a group with shared interests in public space when traders, operators and residents have divergent ones. And it does not address private surveillance, the estate cameras, neighbourhood-watch networks and private-security systems that van Riet (2023) shows are often more extensive than the state's, which raises its own questions of accountability and exclusion.

5. CONCLUSION AND RECOMMENDATION

Urban surveillance is sold to African cities as a safety technology and installed as an infrastructure of public space. The safety effect is real, bounded and dependent on institutional capacity the technology does not supply. The behavioural effect, on who can be in public space, doing what, without being identified, is systematically uncounted and falls on the informal majority for whom public space is livelihood. The power effect, the capability to watch, held by whoever controls the cameras and the data, persists after the safety rationale is exhausted and is the lasting result. This paper has separated the three effects, proposed four criteria of legitimacy, effectiveness, proportionality, accountability and the preservation of anonymous public presence, derived propositions that make the framework testable, examined the governance problems of vendor-controlled infrastructure, and anchored the analysis in Lagos.

The conclusion is not that African cities should refuse surveillance technology. Insecurity is real and the demand for protection legitimate. It is that a city that installs eyes should decide, before it does so, what they will be allowed to see, who will be allowed to look, and whether the people who make their living in the street will still be able to do so unseen. The right to the city, in the age of the camera, is the right to be in public without being known. A surveillance infrastructure that preserved that right while reducing the crimes that threaten it would be a genuine contribution to urban safety. One that does not is a contribution to something else.

6. CONTRIBUTION TO EXISTING KNOWLEDGE

The paper contributes a decomposition of urban surveillance into its effects on safety, on behaviour and on power, and shows that the public case for it rests almost entirely on the first while its lasting consequences lie in the second and third.

It further contributes a legitimacy framework built on effectiveness, proportionality, accountability and the preservation of anonymous public presence, giving governments, regulators and vendors a standard for judging whether a surveillance deployment improves safety without eroding the civic freedom that public space sustains.

© IIARJournal. All rights reserved.

7. REFERENCES

Abraham, O. M., Mbah, P. O., Ocheni, M. M., & Obiagu, U. C. (2025). Unguarded areas and rural insecurity in Nigeria, 2010–2022. Journal of Asian and African Studies, 61(2), 1640–1655. https://doi.org/10.1177/00219096251318241

Achinivu, C. (2025). Understanding digital authoritarianism in Africa: The case of Nigeria. Journal of Contemporary African Studies, 43(3), 390–405. https://doi.org/10.1080/02589001.2025.2548785

Alizadeh, T., & Prasad, D. (2024). The right to the smart city in the Global South: A research agenda. Urban Studies, 61(3), 426–444. https://doi.org/10.1177/00420980231183167

Almasoud, A. S., & Idowu, J. A. (2025). Algorithmic fairness in predictive policing. AI and Ethics, 5(3), 2323–2337. https://doi.org/10.1007/s43681-024-00541-3

Almulhim, A. I., & Yigitcanlar, T. (2025). Understanding smart governance of sustainable cities: A review and multidimensional framework. Smart Cities, 8(4), 113. https://doi.org/10.3390/smartcities8040113

Ayodele, O. (2026). Local innovation and the politics of surveillance in African peacebuilding. South African Journal of International Affairs, 33(2), 317–341. https://doi.org/10.1080/10220461.2026.2692484

Bandauko, E., & Nutifafa Arku, R. (2023). A critical analysis of 'smart cities' as an urban development strategy in Africa. International Planning Studies, 28(1), 69–86. https://doi.org/10.1080/13563475.2022.2137112

Da Vinha, L. (2024). Smart for whom? Africa's smart cities and digital authoritarianism. International Journal of Intelligence and CounterIntelligence, 37(3), 941–959. https://doi.org/10.1080/08850607.2023.2284629

Das, D. K., Aiyetan, A. O., & Mostafa, M. M. H. (2026). Advancing smart cities in Africa: Barriers, potentials, and strategic pathways for sustainable urban transformation. Smart Cities, 9(2), 38. https://doi.org/10.3390/smartcities9020038

Datta, A. (2023). The digitalising state: Governing digitalisation-as-urbanisation in the global south. Progress in Human Geography, 47(1), 141–159. https://doi.org/10.1177/03091325221141798

Dorostkar, E., & Najarsadeghi, M. (2026). The digital city and the struggle for urban public spaces: A pragmatic rethinking of public space and digital rights in a postliberal urban future. Urban Governance, 6(2), 255–264. https://doi.org/10.1016/j.ugj.2026.05.004

Egba, V. N., Ukeje, I. O., Ayanwale, M. A., Robinson, D. F., Ojogbane, R. S., & Akonye, J. E. (2026). Smart urban governance for sustainable cities: Integrating artificial intelligence, digitalization, and renewable energy technologies in Nigeria's public service transformation. Frontiers in Sustainable Cities, 8, 1739482. https://doi.org/10.3389/frsc.2026.1739482

Gabrielli, G. (2025). The use of facial recognition technologies in the context of peaceful protest: The risk of mass surveillance practices and the implications for the protection of human rights. European Journal of Risk Regulation, 16(2), 514–541. https://doi.org/10.1017/err.2025.26

Gikay, A. A. (2023). Regulating use by law enforcement authorities of live facial recognition technology in public spaces: An incremental approach. The Cambridge Law Journal, 82(3), 414–449. https://doi.org/10.1017/s0008197323000454

Kim, E.-S., & Chung, J.-B. (2025). Toward a more contextual approach to predictive policing: Systematic literature review. Sociology Compass, 19(8), e70102. https://doi.org/10.1111/soc4.70102

Lang, K., Sanford, J., & Murtagh, C. (2025). Assessing CCTV in preventing and reducing property crime. Justice Evaluation Journal, 8(2), 263–283. https://doi.org/10.1080/24751979.2025.2474706

Lin, B. (2024). Beyond authoritarianism and liberal democracy: Understanding China's artificial intelligence impact in Africa. Information, Communication & Society, 27(6), 1126–1141. https://doi.org/10.1080/1369118x.2023.2239322

Maatallah, R., Abdessamad, A., & Khatori, Y. (2026). Smart cities in Africa: A systematic literature review of challenges and development strategies. City and Environment Interactions, 30, 100365. https://doi.org/10.1016/j.cacint.2026.100365

Mhlanga, D. (2026). Artificial intelligence in smart cities: Implications for urban governance in Africa. Frontiers in Sustainable Cities, 8, 1835768. https://doi.org/10.3389/frsc.2026.1835768

Olajide, O. A., & Lawanson, T. (2025). Claiming the right to the city: The politics of urban reform coalitions in Lagos. Environment & Urbanization, 37(1), 57–75. https://doi.org/10.1177/09562478251318231

Sen, S., Rasmussen, J., & Kimari, W. (2026). Dialectics of informality in the smart city: Between antagonism and interdependence. Urban Studies, 63(14), 3278–3290. https://doi.org/10.1177/00420980261435846

Tedeschi, M. (2024). Datafication and urban (in)justice: Towards a digital spatial justice. Geography Compass, 18(6), e12763. https://doi.org/10.1111/gec3.12763

© IIARJournal. All rights reserved.

van Riet, G. (2023). Topology, scene and asymmetries in security provision in a small South African city. Critical Studies on Security, 11(1), 14–23. https://doi.org/10.1080/21624887.2022.2060062

Widmark, J. (2026). Crime prevention in residential areas: A systematic review and meta-analysis of environmental design approaches. European Journal on Criminal Policy and Research, 32(3), 943–971. https://doi.org/10.1007/s10610-026-09659-y

Yang, C., Wong, U. K., Cai, J., Wang, C., Hu, H., Ho, W. I., & Yin, Y. (2026). Bridging the socio-technical lag: A systematic literature review of regulation, collaboration, and inclusive governance in smart city infrastructure. Frontiers in Sustainable Cities, 8, 1897229. https://doi.org/10.3389/frsc.2026.1897229

Yigitcanlar, T., Shaamala, A., Marasinghe, R., Liu, K., Hossain, S. T., & Xu, Y. (2026). Surveilled urban futures: How AI shapes power, privacy, and participation in smart cities. Urban Studies. Advance online publication. https://doi.org/10.1177/00420980261461440

Zalnieriute, M. (2025). Facial recognition surveillance and public space: Protecting protest movements. International Review of Law, Computers & Technology, 39(1), 116–135. https://doi.org/10.1080/13600869.2023.2295690

© IIARJournal. All rights reserved.