Power, Control and the Promise of Technology

Rethinking Surveillance through a Democratic Governance Lens

Published by:

Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

Power, Control and the Promise of Technology

Rethinking Surveillance through a Democratic Governance Lens

November 2025

Authors:
Mable Barbara Amuron and Richard Ngamita,
Thraets Foundation.

The publication "Power, Control and the Promise of Technology" was commissioned by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, Sector Programme Governance, on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ).

Acknowledgements: We would like to express our sincere gratitude to the Competence Center 4C30, the Sector Program Human Rights, the Sector Project International Digital Policy for Sustainable Development, the Project Strengthening of the Civil Society in the Eastern Partnership and the Project Towards a Just(er) Digital Governance for their valuable contributions to this Policy Brief. Their insightful comments, critical feedback, and expertise have greatly enriched the analysis and helped shape the final outcome.

The contents of this publication do not represent the official position of neither BMZ nor GIZ.

Table of Contents

Executive Summary

Digital surveillance technologies are expanding globally, fueled by security justifications, public service goals, and datafication in public and private sectors. This trend varies across democratic, hybrid, and authoritarian regimes, shaped by institutional safeguards.

Over the past five years, nations such as Kenya, South Africa, Myanmar, Panama, Peru, Nigeria, Kazakhstan, Serbia, Ghana, Tanzania, and Uganda have rapidly adopted biometric systems, including fingerprint scans and facial recognition, for government, banking, elections, and border security. While China remains unmatched in the scale and sophistication of surveillance deployment, the pace and breadth of adoption across African contexts are exceptional. Promoted for efficiency, safety, and anti-fraud, these tools risk shifting into instruments of political control in the absence of robust legal and institutional safeguards, with lasting impacts on governance and civic freedoms.

When designed and implemented with appropriate safeguards, transparency, and accountability, AI and related technologies have the potential to improve governance, enhance service delivery, and strengthen citizen engagement. However, Governments are deploying these AI analytics and “Safe City” CCTV networks alongside biometric systems, often without transparency or public scrutiny and debate. These measures disproportionately impact civil society, journalists, and marginalised groups like women and persons with disabilities. Rather than enhancing governance, such technologies can also deepen inequalities, undermine political participation, and foster self-censorship. Digital surveillance is a major factor in shrinking democratic spaces and eroding accountability under the guise of security, particularly in transitional or hybrid democracies where activists and independent media experience increased harassment.[1]

Global power competition among Russia, China, other emerging economies, the United States (US), and the EU is reshaping technology supply chains and governance models. This competition is driven by overlapping economic, political, and strategic interests, including efforts to expand markets, secure geopolitical influence, and establish technological standards and alliances. Many Global South governments seek to leverage these global rivalries to gain financing and advanced technology. However, challenges like vendor lock-in, conditional partnerships and divergent regulations can lead to new dependencies that compromise digital sovereignty. The notion of digital sovereignty itself is contested: some states invoke it to justify tighter control over information and citizens, whereas a rights-based approach emphasises community empowerment, transparency, and democratic participation in shaping technologies and policies.

[1] Regulation of Digital Surveillance and Impact on Civil Society in South Africa, ICNL Report, August 2025. https://www.icnl.org/post/report/icnl-report/regulation-of-digital-surveillance-and-the-impact-on-civil-society-in-africa-experiences-from-south-africa

Finally, the effects of surveillance extend beyond borders. The repressive use of these technologies has transnational dimensions, including impacts on diaspora communities who may face monitoring, intimidation, or digital repression even when living abroad. This global dimension underscores the need for international cooperation and rights-based safeguards to prevent surveillance technologies from becoming entrenched tools of repression[2].

Addressing challenges from surveillance technologies requires context-specific regulations, capacity building, and inclusive governance that actively involve civil society.

Key Messages for Policymakers

- **Urgent risk:** Digital surveillance is rapidly outpacing the legal and oversight frameworks necessary to protect human rights. Weak institutions and limited accountability in many countries increase the risk of irreversible abuses. Most affected rights include privacy, freedom of expression, assembly, association, and non-discrimination. Unchecked surveillance leads to profiling, deepens inequalities, and fosters fear and self-censorship, undermining civic trust and democratic participation.
- **Strategic leverage:** Development cooperation can help shape global and regional norms by promoting standards of transparency, rights-based regulations, and governance models that are sensitive to local contexts and prioritise digital sovereignty.
- **Entry points:** Diplomatic engagement, multilateral forums (such as the EU, AU, and UN), and development funding should align with a partnership-based, risk-driven approach that uses minimum safeguards, sequencing, and incentives.

Key Messages for Practitioners and Project Implementers

- **Practical safeguards:** Utilise risk-assessment checklists before supporting digital or AI-related projects, ensuring that the vulnerabilities of marginalised groups and the intersectional impacts are explicitly considered.
- **Capacity building:** Promote institutional and regulatory capacity for accountable, transparent, and rights-based governance of surveillance and digital technologies. Where direct government oversight is constrained, efforts should prioritise independent institutions and inclusive dialogue with civil society to reinforce checks and balances.
- **Civil society empowerment:** Provide resources, training, and digital security tools to local organisations, youth groups, journalists, and human rights defenders. This support will enable them to monitor surveillance practices, raise awareness among citizens, advocate for rights, and foster resilient civic spaces.

The international development community, in collaboration with African and global partners, has a crucial opportunity to act. Without prompt intervention, surveillance technologies are becoming tools of control and repression. Focusing on democratic safeguards, inclusive governance, digital sovereignty, and human rights enables these technologies to enhance democratic resilience, social inclusion, and accountable governance in partner countries.

[2] Rising digital surveillance threatens Africa's democratic progress, ISS Africa, October 2023 https://futures.issafrica.org/blog/2023/Rising-digital-surveillance-threatens-Africas-democratic-progress

1 Introduction

1.1 Historical Context: From Analogue Surveillance to Digital Authoritarianism

Surveillance has always been part of governance, but today‘s modern digital tools represent a fundamental shift in scale, speed, and permanence. During the post-colonial era, African regimes relied on analogue methods, manual phone tapping, physical monitoring, and paper files, mainly to track political opponents and suppress dissent. The wave of liberalisation and the rise of the internet in the 1990s and 2000s introduced new telecommunications infrastructure, which created new opportunities for transparency and participation. Yet these same infrastructures have enabled governments to collect, store, and analyse personal data at an unprecedented pace. The most recent developments around AI have further accelerated this shift, automating surveillance at scale and lowering the cost of control.

Key Takeaway

Digitalisation has turned surveillance from a selective tool of control into a pervasive element of governance, fundamentally reshaping state-citizen relations.

1.2 Digital Surveillance Technologies and their Governance Relevance

Recent technological transformations have enabled governments to observe populations at unprecedented scale and speed. Over 30 African countries, alongside emerging economies such as India and Brazil, have introduced biometric identification systems. At least 15 African states now pilot or deploy facial-recognition technologies under Smart or Safe City initiatives, reflecting a broader drive toward digital transformation for governance efficiency and public safety.

In many countries worldwide, biometric national ID systems, AI-enhanced CCTV networks, mobile location analytics, and social media monitoring have become integral to public administration and security. Key technology providers (e.g., from China and Israel) play a crucial role in funding and supplying these systems. For example, the Ghana Card and Kenya’s Huduma Namba centralise data like fingerprints and facial scans to improve voter registration and welfare distribution. Major cities such as Lagos, Kampala, Addis Ababa, and Nairobi have implemented advanced CCTV networks with AI analytics for real-time monitoring. Serbia has also adopted Chinese-developed “Safe City” systems in Belgrade, raising concerns about surveillance and the impact on civic activism.

Example: Zambia's "Safe City"

Zambia's USD 200 million Safe City programme, developed with Chinese vendor ZTE, has raised governance concerns due to its opaque, single-sourced procurement and minimal public consultation. Civil society, journalists, and parliamentarians criticised the lack of transparency over the system's purpose and data handling. Debates on the CCTV Bill heightened fears of government access to surveillance data without judicial oversight, threatening privacy rights. In 2024, the Auditor-General reported that ZTE technicians retained control over key system components, exposing Zambia's dependence on foreign support and weak local capacity. While no direct misuse has been confirmed, the case illustrates how rapid technological deployment can outpace regulatory safeguards and heighten risks of abuse.

These technologies promise tangible benefits, reducing fraud, improving service delivery, and enhancing security, particularly in resource-constrained settings. Yet the centralisation of vast, sensitive datasets creates permanent digital records and grants governments unprecedented capacity to monitor citizens with precision, fundamentally shifting the balance of power between state and citizen.

Example: Nigeria's Bimodal Voter Accreditation System (BVAS)

During Nigeria's 2023 general elections, the Bimodal Voter Accreditation System (BVAS) and INEC Results Viewing Portal (IReV) were introduced to curb fraud and enhance transparency through biometric verification and real-time result publication. However, observers noted BVAS malfunctions, cybersecurity risks, disinformation, and human interference. The expansion of high-resolution CCTV networks and the use of National Identification Number (NIN) data in security operations further raised concerns about surveillance of protests and opposition activities, with implications for freedom of assembly and expression. These developments highlight how digital tools can either strengthen electoral integrity or enable control, depending on safeguards, transparency, and implementation.

Where legal protections and independent oversight remain weak, the deployment of these systems heightens the risk of political misuse. Long-term vendor contracts, proprietary software, and integrated databases make it costly and difficult to reform or dismantle surveillance systems once installed. In several countries, privacy laws are absent, unenforced, or circumvented, leaving citizens with limited means of redress. Without accountability, technological efficiency can entrench digital authoritarianism, where tools designed for service delivery or safety become mechanisms of control that erode trust, suppress dissent, and weaken democratic governance.

Key Takeaway

Africa's digital transformation illustrates both the promise and peril of technology-driven governance, offering efficiency gains while expanding the potential for unchecked state power.

1.3 Surveillance Expansion and Democratic Backsliding

Growing evidence suggests that the expansion of digital surveillance technologies is closely linked to democratic backsliding. While AI and data-driven tools hold potential for improving service delivery and sustainable development, they are increasingly used for targeted harassment, disinformation, and election interference. Once surveillance becomes normalised, reversing its reach is difficult, even after leadership changes, because systems and contracts are deeply embedded in state institutions.

Since 2015, more than 60% of African countries have experienced a decline in civil liberties, with digital surveillance frequently cited as a contributing factor.[3,4] Governments across the continent have employed internet shutdowns, digital monitoring tools, and biometric data systems to control or deter dissent. According to Access Now's #KeepItOn Data Dashboard (2024), recent shutdowns in countries such as Ethiopia, Senegal, and Sudan demonstrate how governments increasingly weaponise connectivity and surveillance infrastructure to control information during crises or elections.

In Tanzania, the late President Magufuli's administration curtailed online expression through social media restrictions and the arrest of critics. This pattern has largely continued under the current government, despite initial reform pledges. In Nigeria, surveillance and intimidation surrounding elections have further constrained civic space and undermined trust in institutions. Similarly, in Uganda, repeated internet blackouts during elections and the digital monitoring of opposition figures have restricted freedoms of expression and assembly. Together, these cases reflect a wider regional pattern: the routine use of digital technologies to suppress dissent, limit accountability, and consolidate executive power.

[3] https://www.africanews.com/2017/09/30/africa-lost-about-237-million-to-internet-shutdowns-since-2015-report/

[4] https://surfshark.com/research/internet-censorship

The challenge is not confined to autocratic settings. Even in democratic contexts, weak or broadly framed legislation can normalise intrusive surveillance. Recent EU debates on child protection, digital security, and AI regulation have raised concerns among rights groups that expansive exceptions for "public order" or "national security" could erode privacy protections and legitimise practices that authoritarian states readily adopt. Together, these developments show how global legal ambiguity and local authoritarian practices reinforce one another, shrinking civic space and undermining accountability.

Key Takeaway

Weak safeguards and broad legislative exceptions risk normalising surveillance across governance systems, accelerating democratic backsliding and eroding freedoms of privacy, expression, and assembly.

Azerbaijan's Digital ID and E-Governance Model

Azerbaijan's Asan İmza ("Easy Signature") system has become a regional benchmark for e-governance. The platform has streamlined public administration, reduced corruption opportunities, and expanded access to digital services across urban and rural areas by linking mobile-based digital IDs to tax, healthcare, and business services. Supported by the ASAN Service centres, the model showcases how strong institutional coordination and citizen-focused design can accelerate digital transformation. Despite its efficiency, the system operates within a limited oversight framework, raising concerns over data privacy, surveillance, and potential misuse of personal information for political purposes.

1.4 Importance for Development Cooperation

The rapid expansion of digital surveillance directly intersects with several development targets, especially SDG 16. Peace, Justice, and Strong Institutions depend on transparent governance and citizen trust, both of which are weakened by opaque or unchecked surveillance practices. Development cooperation actors following a human rights-based approach aim to support states in fulfilling their international obligations to respect, protect, and fulfil all human rights, including privacy, freedom of expression, and civic participation.

Surveillance technologies increasingly cut across sectors central to development policy, governance, digitalisation, urban development, and security reform, creating unavoidable exposure to related risks. If not managed responsibly, tools intended to improve service delivery or public safety may instead enable intimidation, repression, and exclusion. Yet development cooperation also has an opportunity to promote rights-respecting digital governance by supporting transparent procurement, institutional capacity, independent oversight, and inclusive policy dialogue, even in restrictive environments.

Unchecked surveillance erodes public confidence in institutions, fuels grievances, and risks instability and cross-border spillovers such as cybercrime or transnational repression. Conversely, governance models that embed safeguards for privacy, accountability, and non-discrimination strengthen institutional legitimacy and social cohesion.

Key Takeaway

Promoting rights-based and accountable digital governance is essential to achieving SDG 16 and to safeguarding long-term stability in partner countries.

2 Surveillance Technology – Current Trends and Risks

2.1 A New Digital Ecosystem

Across the Global South, governments are building interconnected digital ecosystems that merge biometric registries, telecom data, AI analytics, and cloud-based storage. These systems promise more efficient service delivery and inclusive governance, but also expand state capacity to monitor citizens continuously.

In Africa, this transformation mirrors global trends shaped by the Digital Silk Road, international development financing, and rapid private-sector innovation. Similar trajectories are evident in Myanmar, Kazakhstan, Peru, Serbia, Panama, and Cambodia, where governments adopt Chinese-backed digital ID and Safe City systems with limited transparency or oversight.

Serbia's Expanding Digital Surveillance Ecosystem

Serbia has rapidly developed an interconnected digital ecosystem integrating biometric registries, telecom data, AI analytics, and cloud infrastructure. Chinese-made "Safe City" systems with facial and license-plate recognition operate across Belgrade, Novi Sad, and Niš, supported by drones equipped with biometric monitoring. Although current law prohibits biometric public surveillance, repeated government attempts to legalise it have faced public backlash. In parallel, Serbia's authorities have reportedly deployed powerful spyware tools, including NSO Group's Pegasus, the domestic NoviSpy, and Cellebrite forensic software, to monitor journalists, activists, and civil society members. These practices, along with a national AI strategy and state data centre, show increased investment in digital governance and surveillance. Despite Serbia's EU integration goals, opaque surveillance tied to political interests fosters fear and repression in digital spaces.[5]

Key Takeaway

Surveillance capacity now grows through interlinked infrastructures that blur the boundaries between public and private oversight in many countries across the Global South.

[5] https://bezbednost.org/en/publication/digital-surveillance-in-serbia/

2.2 Core Technologies and Deployment Patterns

The surveillance landscape rests on four interlinked technological pillars that are now widely deployed across Africa and other regions in the Global South

Biometric Digital IDs

National ID programmes, such as Kenya's Huduma Namba, Nigeria's and Uganda's National Identification Number, Ghana's Card, and Mexico's CURP, collect extensive biometric and demographic data, often linked to SIM registration to create single digital identities. Governments justify these systems through the promise of faster and more inclusive service delivery, a narrative that powerfully legitimises mass data collection. Yet this framing of efficiency masks the risk of "function creep", where personal data is repurposed for surveillance or political control. In contexts where data sharing is culturally viewed as communal rather than individual, such narratives are easily exploited by both state and corporate actors, weakening privacy protections and normalising intrusive governance.

Mexico's National Digital Identity and Expanding Surveillance

Mexico is rolling out a mandatory biometric digital ID system called the CURP (Unique Population Registry Code), which collects biometric data like photos, fingerprints, and iris scans. This system links personal data across government and private services to improve inclusion and service delivery. However, civil society groups warn that it risks mass surveillance and data misuse, especially as new laws broaden access to personal data for security and intelligence purposes, raising concerns about privacy erosion and intrusive governance. The cultural context of data sharing in Mexico further complicates efforts to protect privacy.[6]

CCTV and "Safe City" Networks

Urban centres such as Nairobi, Kampala, Accra, and Lusaka deploy high-resolution camera systems increasingly enhanced with AI for real-time facial recognition, acoustic analysis, and vehicle tracking. Frequently financed or supplied by large vendors (e.g., Huawei, ZTE), these projects can reach costs in the hundreds of millions of USD per city and often outpace robust data-protection and oversight frameworks.

AI-Driven Monitoring and Predictive Policing

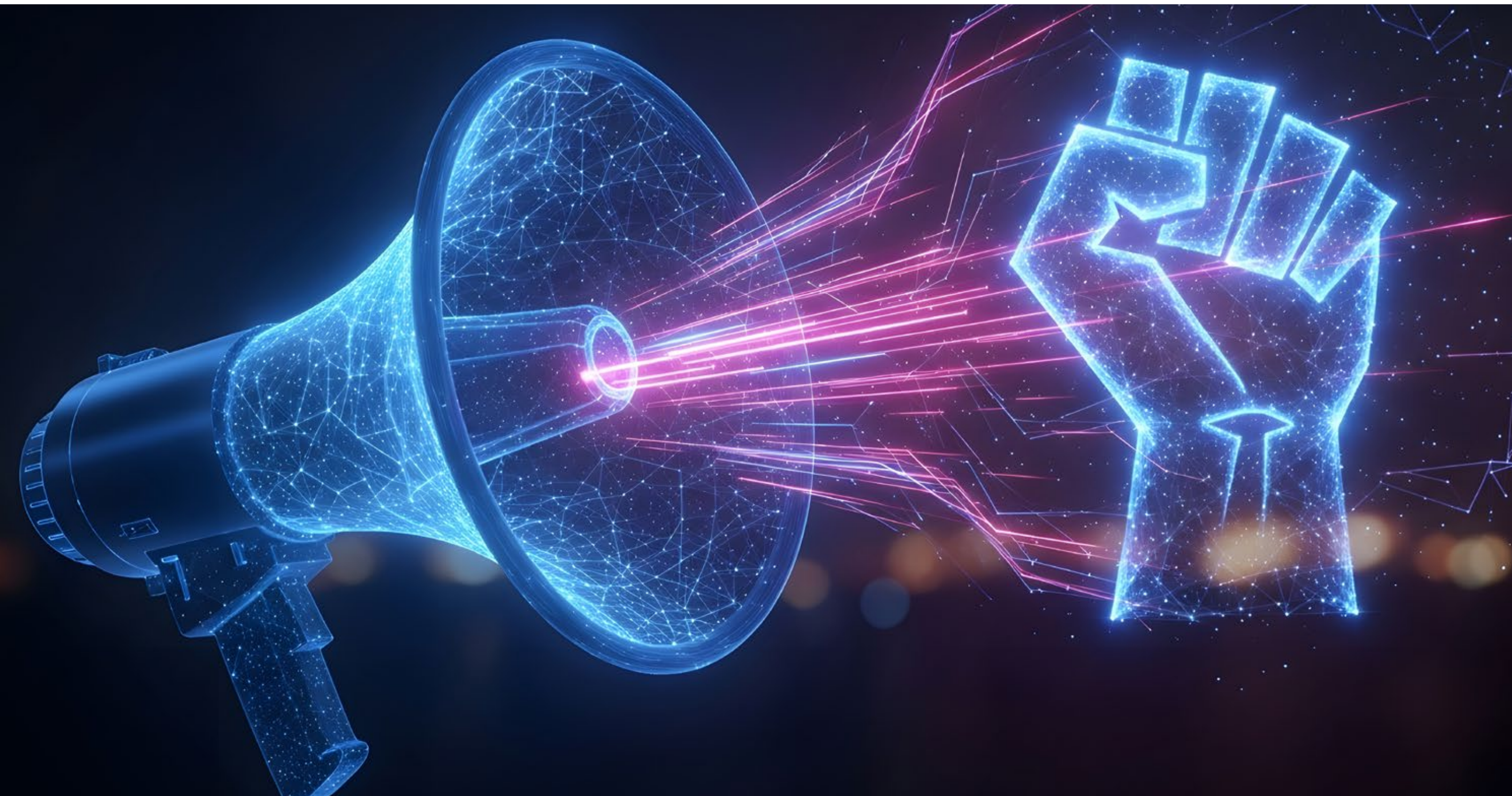
Governments in the Global South are increasingly using AI models to analyse social-media content, call records, and online activity. Predictive policing systems claim to anticipate crime or unrest but often replicate existing biases, disproportionately affecting marginalised or politically active groups.

[6] https://www.eff.org/deeplinks/2025/09/mexican-allies-raise-alarms-about-new-mass-surveillance-laws-call-international

Kazakhstan's Expanding AI Surveillance and Biometric Control System

Kazakhstan's TargetEYE facial recognition system, operated by the Ministry of Internal Affairs' anti-extremism department, enables real-time identification and detention of individuals based on AI matches, including reported cases of wrongful arrests, such as that of a political blogger misidentified by the system. In 2024, the government announced a national biometric authentication system to become mandatory for banking services, including online loans, by August 2025. A data breach in mid-2025 exposed the personal data of millions of citizens, revealing significant vulnerabilities in the centralised biometric infrastructure. Chinese and Russian vendors supply much of Kazakhstan's surveillance hardware and software, embedding foreign technological influence into the country's governance architecture. Experts warn that this growing dependence, coupled with weak privacy protections, risks enabling unchecked state monitoring, data misuse, and transnational surveillance collaboration under the guise of digital modernisation.[7]

[7] https://timesca.com/kazakhstan-confronts-major-data-leak-in-high-stakes-security-crackdown/



Serbia: AI Surveillance and Predictive Policing in Protest Crackdowns

In Serbia, student-led protests began in November 2024 after a train station canopy collapsed in Novi Sad, killing 15 people. This incident highlighted government corruption under President Aleksandar Vučić. The movement grew into a nationwide call for accountability and transparency, peaking in March 2025 with over 300,000 demonstrators in Belgrade. Since the protests erupted, Serbian authorities have intensified digital surveillance to suppress dissent. AI-driven monitoring systems, integrated into over 8,000 Chinese-made cameras from Huawei, Dahua, and Hikvision, use facial and behavioural recognition to identify, track, and predict protest activity in real time. These tools, combined with drones and predictive policing algorithms analysing crowd data and individual profiles, enable preemptive targeting of activists and journalists. Investigations by the Share Foundation and Amnesty International have exposed the use of Pegasus spyware, NoviSpy, and Cellebrite forensic tools to hack phones and extract data from protesters and reporters, including two BIRN journalists targeted in February 2025.

Integrated Data Fusion Platforms

The most ambitious projects combine biometric IDs, CCTV, telecom metadata, and financial data into central command centres capable of real-time monitoring and automated decision-making. These opaque systems, often hosted offshore, can map population movements and behaviours, with few avenues for redress or appeal.

Key Takeaway

Combined, these technologies give governments and private actors unprecedented power to observe, profile, and influence citizens in real time.

Examples of CCTV Usage

- Ghana has rolled out a multi-phase CCTV programme in Accra and other urban centres, pairing thousands of cameras with video analytic software to support crime-prevention goals. But this has raised significant privacy concerns, including risks of data misuse, inadequate protection under existing laws, and potential government overreach in surveilling citizens for non-security purposes
- Zambia's national Safe City project, developed with ZTE for over USD 200 million, has faced scrutiny for its opaque procurement and the continued control of core infrastructure by the vendor. Civil society groups warn that without clear legal safeguards or local technical oversight, such projects risk embedding permanent surveillance capacity beyond democratic control.
- Nigeria is expanding city-scale CCTV networks in Lagos and other metropolitan areas while trialling AI analytics for public-safety monitoring. These initiatives have sparked alarms over privacy breaches, ethical dilemmas in data handling, and the use of surveillance tools to target activists, journalists, and political opponents, potentially stifling dissent and violating human rights.
- South Africa (Johannesburg and Cape Town) combines AI-enabled tools such as ShotSpotter (gunshot detection) with citywide CCTV feeds and predictive mapping to identify hotspots; critics highlight disproportionate impacts on low-income or racialised communities. The Protection of Personal Information Act (POPIA) aims to regulate such data use, but concerns over bias and lack of transparency remain.
- Kazakhstan has developed one of the most sophisticated surveillance networks in Central Asia, integrating AI-driven monitoring, biometric databases, and centralised data systems. Nationwide, over 1.36 million cameras, including 310,000 linked directly to police command centres, continuously monitor public spaces using AI to detect faces, license plates, and "suspicious behaviour."
- Georgia has expanded CCTV deployment in public areas, including government buildings, to counter disinformation and maintain social order. However, this extensive surveillance coincides with restrictive media laws that suppress independent journalism and civil society. These CCTV systems, often enhanced with digital analytics, are part of state strategies to monitor opposition and control political narratives, contributing to democratic erosion and media self-censorship.
- Belarus has greatly expanded its CCTV infrastructure, with around 60,000 cameras monitoring citizens under President Alexander Lukashenko. The country also has a surveillance system that covers all its forests for fire detection and environmental monitoring. This push for "digital sovereignty" emphasises control over digital infrastructure, aligning with the increased surveillance aimed at state control over the population.

Table 1: Core Technologies and Governance Risks.

Core Technology	Primary Purpose / Justification	Key Governance Risks	Example Contexts / Cases
Biometric Digital IDs	Streamline service delivery, reduce fraud, enhance inclusion	"Function creep", where data is repurposed for surveillance or political control; permanent biometric identifiers increase vulnerability to misuse or breaches	Kenya's Huduma Namba, Nigeria's NIN, Uganda's national ID, Ghana's Ghana Card, Mexico's CURP
CCTV and "Safe City" Networks	Strengthen urban security, deter crime, and improve law enforcement responsiveness	Pervasive surveillance, lack of oversight, data-sharing with vendors, and potential targeting of activists	Ghana (Accra CCTV), Zambia's ZTE Safe City, Nigeria (Lagos pilot), South Africa (ShotSpotter, predictive mapping)
AI-Driven Monitoring and Predictive Policing	Anticipate crime or unrest, optimise policing and resource allocation	Algorithmic bias, profiling of marginalised or politically active groups, and chilling effects on civic participation	Serbia (AI-assisted protest monitoring), South Africa (predictive mapping), Nigeria (AI-enabled safety systems), Kazakhstan's TargetEye
Integrated Data Fusion Platforms	Enable real-time coordination across agencies via combined biometric, telecom, and financial data	Centralised control without transparency; potential for mass profiling and abuse; weak legal recourse for citizens	Huawei/ZTE command centres in Nairobi, Lusaka, and Belgrade
Spyware and Forensic Tools	Support lawful interception and digital forensics for security investigations	Arbitrary targeting of journalists, activists, and opposition; no due process or oversight	Serbia (Pegasus, NoviSpy, Cellebrite); Mexico (state spyware deployment); various NSO-linked cases globally

2.3 Democratic Risks

Unchecked surveillance systems present significant dangers to democratic governance and human rights:

- **Erosion of the Civic Space:** Governments can monitor the activities of journalists, civil rights activists, and political opponents with relative ease and minimal expense. This surveillance often leads to a chilling effect where individuals may self-censor for fear of retribution. This effect is particularly strong among already marginalised communities, such as LGBTIQ+ or ethnic or religious minorities.

- **Diminished Privacy and Due Process:** The reliance on centralised biometric systems creates permanent digital records that individuals cannot control or erase. Unlike passwords or ID cards, biometric identifiers like fingerprints and facial features are immutable; once compromised, they cannot be changed. This makes misuse and data breaches far more severe. In many countries, citizens lack mechanisms to understand how their data is used or to seek redress for wrongful surveillance. Centralised storage heightens risks, as a single breach can impact millions. Without strong legal safeguards and oversight, biometric systems risk converting everyday interactions into continuous surveillance, eroding privacy and due process.

- **Gaps in Accountability:** The deployment of artificial intelligence and algorithmic decision-making tools tends to produce results and conclusions that are not easily understood or scrutinised. Most jurisdictions in Africa, particularly those with limited technical resources, struggle to audit these systems for data bias, discrimination, or exploitation, resulting in a significant lack of accountability for decisions made by these algorithms – eroding public trust and the perceived legitimacy of democratic institutions**.**

- **Manipulation through Disinformation and Social Control:** When surveillance data is combined with advanced analytics, it allows for precision targeting of individuals with specific narratives or information. This manipulation can undermine constructive public discourse and political dissent, compromising the integrity of elections by shaping the perceptions and attitudes of the electorate based on tailored disinformation campaigns.

Example: Data-Driven Manipulation and Digital Authoritarianism in the Philippines

In the Philippines, surveillance data and social-media analytics have been weaponised to micro-target voters and shape political narratives. Since 2016, networks linked to political consultancies and state actors have used harvested Facebook data and coordinated "troll farms" to amplify pro-government messaging and attack critics. The fusion of SIM registration, national ID data, and social-media monitoring blurs the line between governance and surveillance, enabling what civil society groups call "digital authoritarianism by stealth."

2.4 Supply Chains and Cost Pressures

Behind every camera and database lies a global network of suppliers and financiers that shape governance outcomes.

- Chinese vendors (e.g., Huawei and ZTE) are major providers of telecoms and “Safe City” infrastructure, often bundling financing, equipment, software, and long-term service contracts. This vertical integration can embed vendor-specific technical standards and limit interoperability, and lead to potential foreign control of sensitive data.

- US and European firms supply AI analytics, cloud hosting, and compute hardware that underpin large-scale data processing and storage. Hyperscale cloud agreements and proprietary algorithms can raise data-transfer and jurisdictional questions that complicate accountability and public oversight.

- Israeli companies export spyware and digital forensic tools used by law enforcement and intelligence agencies; their deployment has raised recurring questions about human rights safeguards and oversight.

Fiscal and governance implications:

- Hidden debt from opaque vendor-financed surveillance projects and offshore data hosting arrangements can undermine fiscal transparency and national sovereignty.

- Proprietary standards hinder interoperability and accountability.

- Competing geopolitical interests, such as China‘s state-led model and Western human rights-based approaches, influence local governance norms.

The human-rights implications of these global supply chains are well established. The UN Guiding Principles on Business and Human Rights (UNGPs) provide the international benchmark for ensuring that both states and companies exercise due diligence to prevent, mitigate, and remedy human-rights abuses linked to business activities –including those involving surveillance technologies. These principles have been operationalised for the technology sector, clarifying that suppliers of surveillance tools and governments procuring them share responsibility for identifying and addressing risks of misuse. Germany, as a UNGP signatory, has embedded these standards in its National Action Plan on Business and Human Rights and Supply Chain Due Diligence Act, which also apply to digital and security-related exports and procurements.

Key Takeaway

Surveillance infrastructure embeds long-term economic and geopolitical dependencies that constrain local digital sovereignty.

2.5 The Rise of Non-State Surveillance

Surveillance has increasingly expanded beyond government functions, with private companies playing a significant role in the collection of personal data. This trend, known as surveillance by proxy, allows social media platforms and data brokers to track user behaviour for advertising, often granting governmental access to this data without standard legal protocols. Telecommunications and internet service providers maintain detailed records of communications, which can be shared with authorities for real-time monitoring. Additionally, spyware vendors may target journalists and political opposition, exploiting regulatory gaps.

When States Borrow the Platform

Several African governments, including Nigeria, Kenya, South Africa, Egypt, and Sudan, have been documented as frequently requesting user data from social media and telecom companies under 'legal' grounds. Nigeria, for example, has made numerous requests for user account information, with some compliance reported. These requests often involve law enforcement or national security investigations and highlight the increasing use of digital platforms for surveillance by proxy through private companies.

These practices can cross borders, creating accountability challenges for both governments and companies. Without clear regulations, states can gain surveillance powers without proper oversight, while private firms manage personal data, complicating privacy and security issues. The implementation of the UN Guiding Principles (UNGP) is crucial as technology providers take on roles traditionally held by the state. Under the UNGP framework, corporations must respect human rights, while governments should regulate corporate actions to prevent abuses. This approach supports human rights due diligence in digital trade and cross-border data governance, helping to bridge accountability gaps.

Implications for Development Cooperation

For development actors, early engagement is essential given the potential political and fiscal risks of technical projects like urban security and digital ID systems. Donors and implementation agencies should assist partner countries by promoting transparent procurement, vendor due diligence, and budget planning that ensures data sovereignty. Adhering to the UN Guiding Principles on Business and Human Rights, donors can integrate due diligence into digital cooperation, e.g., assessing human rights risks in supply chains and ensuring vendor compliance with Germany's Supply Chain Due Diligence Act. (Lieferkettensorgfaltspflichtengesetz).

Table 2: Comparative Overview of AI-Driven and Biometric Governance Practices.

Country/Region	Political Context	Key Technologies Adopted	Primary Justifications	Notable Risks/ Impacts	Institutional Safeguards Status
Kenya (Africa)	Emerging democracy with expanding digital infrastructure	Biometric IDs (Huduma Namba), facial recognition in elections	Efficiency in services, fraud reduction	Self-censorship among activists, data breaches	Emerging data protection laws, but weak enforcement
South Africa (Africa)	Constitutional democracy with strong legal institutions	National ID biometrics, CCTV networks	Public safety, border security	Marginalised groups targeted, inequality amplification	Constitutional privacy rights, ongoing parliamentary debates
Myanmar (Asia)	Authoritarian regime post-2021 military coup	Facial recognition for security, AI analytics	Counter-insurgency post-2021 coup	Heightened repression of ethnic minorities, civic space erosion	Minimal oversight amid authoritarian shift
Panama/Peru (Latin America)	Hybrid democracies with fluctuating institutional trust	Biometric registries for banking/elections	Anti-corruption, service delivery	Political intimidation of journalists, bias in profiling	Hybrid systems with judicial reviews, but inconsistent
Nigeria (Africa)	Federal democracy with contested digital governance	BVAS for voter accreditation, Safe City CCTV	Electoral integrity, urban safety	Election harassment, diaspora monitoring	Data laws exist, but opaque contracts undermine
Kazakhstan (Central Asia)	An authoritarian regime with strong state control over ICT	Biometric borders, social media monitoring	National security	Suppression of dissent, transnational effects on exiles	Authoritarian controls with limited civil input
Ghana/Tanzania/ Uganda (Africa)	Mixed democracies experimenting with surveillance-led governance	Ghana Card IDs, urban CCTV, predictive policing	Fraud combat, crime reduction	Youth/women vulnerabilities, self-censorship	Varied; AU frameworks aiding, but local gaps persist
Serbia (Europe)	Hybrid regime with democratic institutions under pressure	Facial recognition "Safe City" systems, biometric IDs	Crime prevention, EU alignment on digital modernisation	Targeting of activists and journalists, chilling effect on dissent	Weak data protection enforcement; limited transparency in surveillance contracts
Moldova (Europe)	Emerging democracy under EU-oriented reforms	Digital ID rollout, biometric border systems, expanded CCTV in Chişinău	EU integration, public safety, anti-corruption	Risk of data centralisation and third-party access; limited public debate on surveillance scope	Partial GDPR alignment; oversight bodies under-resourced

3 How the Global Surveillance Ecosystem Works

3.1 Transparency, Oversight, and Rule-of-Law Gaps

In many Global South countries, surveillance systems are implemented without public knowledge or discussion, leading to minimal debate and weak legislative oversight. Confidentiality clauses in contracts obscure technical details and data practices. Regulatory bodies, often underfunded, struggle to enforce privacy laws. This lack of transparency can result in data collected for public services being repurposed for policing or political repression, making it hard for individuals to assert their rights. Such practices pose significant risks for development cooperation, as funded digital systems may be used to silence critics or interfere in elections.

Uganda's Intelligent Transport Monitoring System (ITMS)

Uganda's deployment of digital license plates was integrated into a surveillance system installed by Global Security, a private Russian contractor. While publicised as infrastructure modernisation, the project has raised concerns about transparency, governance, and potential misuse. Critics highlight the lack of public discussion on data access, storage, and safeguards, fearing the technology will facilitate real-time tracking of vehicles used by journalists, opposition supporters, and activists.

3.2 The Expanding Role of Private Tech Companies

Private companies are actively shaping who has power over surveillance. Social media platforms and advertising companies collect massive amounts of data about people‘s behaviour. Governments can purchase such data or compel disclosure through lawful process, enabling surveillance by proxy. Telecom and cloud companies hold sensitive communications and metadata (e.g., who contacts whom and when). They often have to build in “lawful intercept” systems that allow security agencies to access communications under legal process. Security and surveillance vendors from Israel, Europe, China, the US, and elsewhere market sophisticated tools such as facial recognition, network hacking software, and phone data extraction systems. Operating across borders, these companies often navigate regulatory gaps or exploit weak export controls. Their business priorities – making recurring profits, gaining market share, and protecting proprietary technology – often conflict with transparency, accountability, and human rights safeguards.

Surveillance by Proxy

Another stark example of surveillance by proxy is the use of Pegasus spyware, developed by Israel's NSO Group and sold to more than 65 governments under the pretext of "law enforcement." Pegasus can infiltrate smartphones through zero-click exploits, granting access to encrypted messages, emails, location data, and even cameras, often by harvesting information from social media and data brokers. In Saudi Arabia, Pegasus was reportedly used to monitor journalist Jamal Khashoggi's communications before his 2018 assassination, while in Hungary, authorities targeted over 300 journalists, lawyers, and opposition figures ahead of elections. Both cases expose how commercial spyware exploits weak export controls and private data flows to enable political surveillance without oversight.[8]

Armenia: Spyware and Political Surveillance

Between October 2020 and December 2022, at least 12 Armenian public figures, including journalists, human rights defenders, and officials, were targeted with Pegasus spyware amid tensions with Azerbaijan over Nagorno-Karabakh. These attacks coincided with key political crises and peace negotiations following Armenia's 2020 defeat, suggesting spyware was used to monitor dissent and influence political discourse. Victims included journalists covering security issues and civil society activists, highlighting the weaponisation of surveillance tools against democratic oversight. Human rights groups, including Amnesty International, have called for a global ban on such spyware due to its grave risks to privacy, free expression, and civic space. Civil society in Armenia continues to press for greater transparency and legal safeguards against misuse of digital surveillance technologies.[9]

[8] https://carnegieendowment.org/posts/2021/07/governments-are-using-spyware-on-citizens-can-they-be-stopped?lang=en

[9] https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/

3.3 Geopolitical Competition and the “Digital Cold War”

Surveillance technology has become a battleground for strategic competition between China, the US, and the European Union. China offers comprehensive “Safe City” packages with easy financing options. These packages are attractive to governments that want quick results without political strings attached. As of 2025, 20 countries in the Global South have implemented these Safe City Projects. United States companies control cloud infrastructure, smartphone operating systems, and online advertising markets, giving US regulators and tech firms significant influence over global data. The EU promotes privacy-focused standards (like the General Data Protection Regulation and the AI Act) and export controls, but European companies still sell surveillance tools through complicated supply chains. [10] Governments in the Global South are balancing competing models to secure financing, technology transfer, and political flexibility. This has led to a fragmented regulatory environment with conflicting standards and legal regimes, risking long-term technological dependencies that hinder interoperability and weaken accountability, making oversight and democratic control more challenging.

Table 3: Comparison of China-US-EU Models of Surveillance Governance.

	China Model	US Model	EU Model
Core Focus	Export of comprehensive surveillance packages like "Safe Cities" with integrated hardware, software, and financing for rapid deployment in public safety and urban management.	Dominance through private sector control of cloud, operating systems, and advertising ecosystems, enabling data leverage for economic and security influence.	Emphasis on human rights and privacy via regulatory frameworks, with export restrictions on high-risk tools to prevent misuse.
Approach to the Global South	No-conditionality aid and tech transfer via the Belt and Road Initiative, appealing for quick infrastructure gains.	Influence through market dominance and regulatory pressures, often tied to alliances and trade deals.	Promotion of standards like GDPR for data protection, with conditional support and complex supply chains for tools.
Key Risks/ Dependencies	Potential for data access by Chinese entities and long-term tech lock-in.	Vulnerability to US sanctions and private firm decisions affecting global access.	Slower adoption due to stringent rules, but risks from indirect exports bypassing controls.

Key Takeaway

Fragmented systems across the Global South, driven by divergent standards and legal regimes, undermine interoperability and hinder regional governance initiatives and safeguards, deepening asymmetries of power in digital governance.

[10] https://www.realinstitutoelcano.org/en/analyses/the-us-china-technology-war-and-its-the_effects-on-europe/

3.4 Digital Inequalities and the Quest for Digital Sovereignty

Many countries in the Global South face structural disadvantages that hinder their control over digital futures, such as limited local research and development capabilities, weak negotiating power in international agreements, and a heavy reliance on foreign cloud and satellite services. Capacity gaps complicate their ability to assess surveillance technology or ensure data remains within their borders. Financial constraints often lead governments to engage in vendor-financing arrangements, resulting in long-term debt and dependency on specific technologies. Additionally, civil society organisations often lack the resources needed to address surveillance abuses or advocate for human rights-based alternatives – leaving little space for open, critical public debate on these issues.

How to navigate the ecosystem in partner countries: For countries in the Global South, these challenges can deepen dependencies on foreign technology providers and surveillance-based governance models, making it harder to pursue inclusive and rights-based digital development. For development cooperation, it is crucial to help build local technical capacity, strengthen independent regulatory authorities free from political or private-sector interference, and promote international norms that safeguard human rights and data protection.

4 Opportunities and Strategic Entry Points for German Development Cooperation

Despite the rapid spread of surveillance technologies and the governance risks they pose, development cooperation has multiple pathways to promote democratic resilience and rights-respecting digital governance. These entry points combine policy engagement, capacity building, and practical safeguards that benefit both governments and civil society.

Guiding Principles for Implementation

- **Human Rights Due Diligence:** Apply the UN Guiding Principles on Business and Human Rights (UNGPs) and Germany's Supply Chain Due Diligence Act across all digital projects.

- **Do No Harm:** Integrate risk assessments to ensure that support for digital governance or civil society does not unintentionally expose activists or marginalised groups to surveillance or retaliation.

- **Independence and Accountability:** Strengthen oversight bodies that are free from political or private-sector interference.

- **Local Ownership and Participation:** Empower partner-country institutions, National Human Rights Institutions (NHRIs), and civil society to co-create digital policies that reflect national priorities and social realities.

4.1 Strengthen Institutional Oversight and Regulatory Frameworks

- **Legal Reform Support:** Provide technical assistance and peer-learning exchanges to help partner countries draft or update context-specific data protection, privacy, and AI governance laws aligned with international human rights standards (e.g., GDPR, African Union Convention on Cyber Security and Personal Data Protection).

- **Independent Regulators:** Support the creation or strengthening of data protection authorities, parliamentary oversight committees, and ombudspersons with genuine investigative powers, budgetary autonomy, and protection from political and commercial influence.

- **Regional Coordination:** Facilitate African regional dialogues (through the AU, ECOWAS, SADC, EAC) to harmonise surveillance safeguards and share best practices. This reduces regulatory fragmentation and prevents countries from competing by lowering standards.

Good Practice: Ghana’s Data Protection Commission (DPC)

Ghana’s DPC, established in 2012, offers an example of gradual institutional strengthening through multi-donor support. With technical assistance from the EU and the Council of Europe, the DPC improved complaint-handling, public awareness, and coordination with telecom regulators. Donors in development cooperation could support similar multi-stakeholder capacity-building models elsewhere in Africa.

4.2 Empower Civil Society and National Human Rights Institutions

- **Capacity Building:** Fund training in digital security, forensic auditing, and legal advocacy for watchdog NGOs, journalists, youth groups, and NHRIs, both domestically and in exile.

- **Participatory Mechanisms:** Apply the Do No Harm principle to ensure that consultation processes do not endanger participants already under surveillance. Where feasible, use secure digital participation platforms or trusted intermediaries.

- **Support for NHRIs:** Provide targeted funding and technical assistance to independent National Human Rights Institutions so they can collect evidence of surveillance-related abuses, issue early-warning reports, and coordinate protection for at-risk individuals.

- **Grassroots Innovation:** Offer small grants for open-source civic tech solutions that monitor procurement, audit AI systems, and report rights violations safely and anonymously.

4.3 Promote Technology Transparency and Ethical Standards

- **Procurement Safeguards:** Embed open-contracting principles, human-rights impact assessments (HRIAs), and UNGP-based due diligence into all digital infrastructure projects supported by implementing agencies.

- **Vendor Accountability:** Require vendors to disclose data-handling practices, AI decision-making logic (where possible), and submit to independent audits. Financial support should be contingent on such transparency.

- **Export-Control Dialogue:** Use influence within the EU and OECD to promote stricter export controls and mandatory public reporting for surveillance technologies that risk enabling repression.

Good Practice: EU Dual-Use Export Controls

The EU’s revised Dual-Use Regulation introduced human-rights criteria for export licensing of surveillance technologies. EU countries can leverage this framework to support capacity building for partner-country regulators and ensure ethical technology transfers.

4.4 Support Inclusive, Participatory AI and Surveillance Governance

- **Multi-Stakeholder Platforms:** Facilitate citizen assemblies, expert panels, and youth consultations on AI and surveillance governance to ensure diverse voices shape national policies.
- **Ethical AI Pilots:** Co-finance demonstration projects that integrate algorithmic transparency, explainability, and fairness benchmarks, creating positive examples for partner governments.
- **South-South Knowledge Sharing:** Sponsor exchanges between African regulators, technologists, and civil society groups to share lessons on ethical AI deployment and rights-protective surveillance management.

Key Takeaway

Development cooperation actors can utilise a”dual-track” strategy. First, they should engage in policy dialogue and norm-setting by leveraging both bilateral and multilateral forums to promote rights-based standards and coordinate with EU initiatives, such as the AI Act and discussions on GDPR adequacy. Second, it is essential to integrate project-level safeguards by incorporating risk-assessment checklists, ensuring procurement transparency, and requiring civil society engagement in every digital or AI-related program.

5 Recommendations

5.1 Policy-Level

Make Human Rights and Democratic Principles the Benchmark for Surveillance Policies and Agreements

Development cooperation should prioritise rights-respecting governance by promoting transparency, accountability, and data protection. Thereby, development actors must support regional initiatives like the African Union's Malabo Convention and align with global standards such as GDPR and UNESCO's Recommendation on the Ethics of AI. Bilateral dialogues should focus on enhancing governance and human rights in partner countries' digital ecosystems, even in restrictive contexts, by incorporating international norms into national strategies and ensuring effective implementation.

Promote Multi-Stakeholder Engagement and Accountability Frameworks

Inclusive participation is critical for legitimate and sustainable surveillance governance. Development cooperation should support the creation and strengthening of multi-stakeholder platforms that bring together governments, civil society, academia, independent media, and the private sector. This includes funding for civil society participation in technology assessments and legislative reviews, as well as peer learning between data protection authorities across regions. Such frameworks improve oversight, transparency, and accountability, especially in countries with limited democratic space.

Support Inclusive Regulatory Development Reflecting Local Contexts and Rule of Law Maturity

Recognising varying political and institutional contexts, development cooperation should promote context-sensitive regulatory approaches. Technical assistance, such as provided through GIZ's Digital Transformation Centres (e.g. Kenya) and the Digital Democracy 4 All project (for example, Serbia), can help partner governments and institutions implement privacy and data protection laws aligned with international standards. Where government ownership may limit genuine oversight, support should prioritise independent regulators, judicial review mechanisms, and parliamentary capacity to ensure the rule of law. Development partners should also mainstream Human Rights Impact Assessments (HRIAs) across all digital transformation projects to identify surveillance risks early and strengthen digital sovereignty based on accountability and rights.

Advance Open Government and Transparent Procurement Standards

To address opaque contracting and vendor lock-in risks, development cooperation should embed open contracting and transparency principles within broader Open Government approaches. This includes supporting governments to adopt open data and public procurement standards across their digital and security portfolios. Mainstreaming transparency measures in public contracting, such as in existing Open Government projects (e.g., Ecuador), is essential for donors to effectively prevent misuse, enhance accountability, and foster public scrutiny of surveillance-related procurements.

5.2 Operational-Level

Integrate Surveillance Governance in Digital, Public Sector Reform and Civil Society Programming

Surveillance governance should be mainstreamed across all relevant public-sector reforms – including public administration modernisation, security sector reform, and justice system strengthening – and across digital projects. Building on the risks highlighted in Chapter 3 (bias, opacity, vendor lock-in, cross-border spillovers), each initiative should include rights-by-design measures: DPIAs, data minimisation and retention limits, open standards and exit clauses, algorithmic testing, and independent oversight. In parallel, civil-society programming should fund watchdog capacity, strategic litigation, and community digital security, and provide accessible channels for complaints and redress (see Chapter 4 entry points).

To identify whether surveillance-related risks may arise in a specific project context, the Self-Risk-Assessment Checklist (Annex 1) provides an initial screening.

Strengthen Institutional Capacity for Oversight, Enforcement, and Redress

Technical assistance should focus on building the institutional capabilities of oversight bodies, such as parliaments, judiciaries, and data protection authorities, to review procurement, monitor implementation, and enforce compliance with human rights and data protection standards. Strengthening the rule of law is essential: this includes supporting access to justice mechanisms, enabling individuals to file criminal complaints or seek civil remedies in cases of unlawful surveillance, spyware abuse, or data misuse. Partner countries should be supported to establish independent grievance and redress mechanisms, accessible to both individuals and civil society organisations, to ensure that surveillance-related rights violations can be investigated and remedied.

Civil Society Empowerment

Parallel to state-focused measures, civil society organisations should receive targeted support to monitor surveillance practices, document human rights abuses, and advocate for transparency and accountability. This includes investments in digital rights training, awareness-raising campaigns, and public dialogues that highlight the social and political impacts of surveillance. Funding for community-based monitoring tools, such as open data platforms or participatory mapping of surveillance infrastructure, can help citizens and watchdogs hold authorities accountable.

Enhance Digital and AI Literacy Targeted at Marginalised Groups and Journalists

Capacity building must prioritise marginalised populations (women, youth, minorities, human rights defenders, people with disabilities) and independent media actors who are disproportionately affected by surveillance risks. Digital literacy programs should empower these groups to identify surveillance technologies, understand their rights, and employ secure tools (e.g., training journalists to detect deepfakes and disinformation). This fosters a more informed and active citizenry advocating for reforms.

Foster Cross-Sector Safeguards in Social Protection and Urban Technologies

Given that surveillance is embedded in digital ID systems, social protection, and smart cities, safeguards must be integrated across sectors. The cooperation should fund project assessments that incorporate human rights impact evaluations, data protection by design principles, and community consultation before deployment. This includes advocating for transparent procurement, data minimisation, and user consent mechanisms within biometric and urban development projects to ensure public accountability.

Risk Assessment Checklist for Surveillance Technologies in Projects (RACS-Tech)

Category	Key Questions	Mitigation Measures
Legal & Regulatory	□ Is the technology compliant with national privacy/data laws? □ Are independent oversight/judicial review mechanisms in place? □ Are there safeguards against secondary misuse of data?	» Condition support on legal compliance. » Require independent audits. » Insert contractual restrictions on secondary use.
Democratic & Human Rights	□ Could the technology shrink civic space or target journalists/activists? □ Does it chill free speech, protest, or political participation? □ Could it be used in discriminatory ways?	» Demand human rights impact assessments. » Apply transparency and accountability clauses. » Support civil society monitoring.
Technical & Operational	□ How secure is the system against hacking/misuse? □ Is there a risk of vendo lock-in? □ Are there interoperability gaps?	» Require security certification and regular audits. » Encourage open standards and multiple vendors. » Build in exit/transition clauses.
Geopolitical	□ Who is the supplier (China, US, EU, Israel, etc.)? □ Does the project create dependency or erode digital sovereignty? □ Is there alignment with EU/German standards?	» Diversify suppliers. » Promote EU-aligned procurement guidelines. » Include digital sovereignty benchmarks.
Social & Ethical	□ Have marginalised groups been consulted? □ Could the technology reinforce bias (e.g., profiling)? □ Was public consent or transparency ensured?	» Conduct social impact assessments. » Mandate community consultation. » Introduce safeguards for groups in vulnerable situations.

Project/Measure Name:

Partner Country:

Technology/System Assessed:
(e.g., Smart City CCTV, Biometric ID, Social Protection Algorithm)

Assessment Date:

					Risk Level			
Area	Criteria / Question	Yes	No	N/A	High	Med.	Low	Required Mitigation Measure & Owner
A. Project & Technology Overview	A.1 Is the technology component strictly necessary and proportionate to achieve the stated legitimate public goal? (i.e., less rights-intrusive alternatives were considered and rejected)	□	□	□	□	□	□	
	A.2 Is the system's function clearly defined, limited to a specific scope, and non-modifiable for new, unapproved functions without a new assessment?	□	□	□	□	□	□	
	A.3 Does the technology or its use pose risks to populations identified as marginalised (e.g., women, youth, ethnic minorities), journalists, or human rights defenders?	□	□	□	□	□	□	
B. Legal & Governance Basis	B.1 Is there a clear, publicly accessible national legal framework (e.g., privacy law, data protection authority) authorising and regulating the specific type of surveillance technology?	□	□	□	□	□	□	
	B.2 Does the procurement contract explicitly prohibit the vendor from sharing data with third parties (including foreign security agencies) or altering functionality without host/partner country authorisation?	□	□	□	□	□	□	
C. Human Rights & Social Impact	C.1 Has a Human Rights Impact Assessment (HRIA) specific to the local context and target group been conducted and made publicly available before procurement or deployment?	□	□	□	□	□	□	

Area	Criteria / Question	Yes	No	N/A	Risk Level			Required Mitigation Measure & Owner
					High	Med.	Low	
	C.2 Does the system employ or have the capacity for biometric recognition (e.g., facial, gait, voice) in public spaces or for mass identification?	□	□	□	□	□	□	
	C.3 Are there mechanisms to prevent discriminatory outcomes (e.g., bias in AI/algorithm) and allow for an individual's right to challenge an automated decision with meaningful human review?	□	□	□	□	□	□	
	C.4 Is there a clear, accessible, and safe grievance and redress mechanism for individuals harmed or negatively affected by the technology's operation?	□	□	□	□	□	□	
D. Data Protection & Security	D.1 Does the project adhere to Data Protection by Design (DPbD) principles, ensuring data minimisation and anonymisation/pseudo-anonymisation?	□	□	□	□	□	□	
	D.2 Is the data stored locally or in a jurisdiction that provides an equivalent level of legal data protection and digital sovereignty for the partner country?	□	□	□	□	□	□	
	D.3 Is there a documented and robust security protocol for data lifecycle management (collection, storage, access, retention, deletion) that meets international best practices?	□	□	□	□	□	□	
E. Transparency & Accountability	E.1 Has the project disclosed key information to the public regarding the technology's capabilities, purpose, and the rules governing its use?	□	□	□	□	□	□	
	E.2 Is there a requirement for mandatory, regular public auditing of the system's operational effectiveness, human rights compliance, and data security?	□	□	□	□	□	□	
	E.3 Does the project include a specific "sunset clause" or defined review period after which the system must be re-authorised or decommissioned?	□	□	□	□	□	□	

Area	Criteria / Question	Yes	No	N/A	Risk Level			Required Mitigation Measure & Owner
					High	Med.	Low	
F. Peace and Conflict	F.1. Could the surveillance technology (e.g., CCTV in disputed areas) intensify ethnic or political conflicts	□	□	□	□	□	□	
	F.2 How does the project align with local peacebuilding needs?	□	□	□	□	□	□	
G. Responsible AI Use	G.1 Does the algorithm risk discriminatory outcomes (e.g., biased facial recognition against certain ethnic groups)?	□	□	□	□	□	□	
	G.2 Are the decision-making processes in the surveillance system explainable to affected users?	□	□	□	□	□	□	
	G.3 Who is liable for misuse, and how is oversight enforced?	□	□	□	□	□	□	

Risk Scoring Guidance

Use the following definitions to complete the "Risk Level" column. Any High risk requires mandatory and time-bound mitigation.

Risk Level	Definition
High (H)	The project activity or technology component poses a severe and likely threat to human rights (e.g., freedom of assembly, life, non-discrimination) or democratic principles (e.g., electoral integrity, rule of law). The risk is highly probable, potentially irreversible, and requires immediate, substantial intervention.
Medium (M)	The project activity poses a moderate threat to human rights or democratic principles. Mitigation measures are necessary to reduce the probability or impact of harm, but the risk is controllable or reversible with reasonable effort.
Low (L)	The project activity or technology component poses a minimal or unlikely threat to human rights or democratic principles. Standard project safeguards are generally sufficient, but the activity still warrants documentation and monitoring.
Not Applicable (N/A)	The question is irrelevant to the technology or project component being assessed (e.g., a question about biometrics when no biometric data is collected).

Stakeholder Engagement Guide

Effective governance of surveillance technologies requires input from a broad range of actors. This guide provides steps to structure meaningful engagement.

A. Identifying Stakeholders

- Government bodies: regulators, ministries of justice/interior, data protection agencies.
- Civil society: human rights organisations, journalists' associations, digital rights groups.
- Academia/experts: legal scholars, technologists, data ethicists.
- Private sector: technology vendors, telecom operators
- Target Groups: Groups that will be impacted directly or indirectly, including those to be disproportionately affected (e.g. women, activists, marginalised groups)

B. Principles for Engagement

- Transparency: share project objectives, technology details, and risk implications openly.
- Inclusivity: ensure representation of affected groups, including marginalised voices and those without digital access.
- Protection: guarantee confidentiality or anonymity for sensitive participants.
- Iterative dialogue: consultations should not be one-off but continuous throughout the project cycle.

C. Methods of Engagement

- Public hearings and policy roundtables.
- Participatory workshops with community representatives.
- Anonymous digital surveys for sensitive stakeholders.
- Joint risk-mapping exercises combining government, civil society, and experts.

D. Outcomes & Accountability

- Document stakeholder concerns and integrate them into project design.
- Establish feedback loops (e.g., periodic reports to consulted groups).
- Set up grievance mechanisms for communities impacted by surveillance projects.

Stakeholder Engagement Guide

Step	Details	Examples
Identify Stakeholders	Include government regulators, civil society, media, academia, vendors, and marginalised groups.	Data protection agencies, journalists' unions, women's rights groups, and digital rights NGOs.
Apply Principles	■ Transparency: share project goals. ■ Inclusivity: ensure diverse representation. ■ Protection: safeguard sensitive voices. ■ Iteration: engage throughout the project cycle.	Use accessible language; allow anonymous contributions; repeat consultations at key milestones.
Engagement Methods	Combine participatory formats to reach different groups.	Public hearings, workshops, digital surveys, and joint risk-mapping exercises.
Ensure Accountability	Establish clear mechanisms to document, respond to, and act upon stakeholder input.	Publish consultation reports, disclose changes made based on feedback, set up grievance mechanisms, and provide ongoing feedback loops.

As a federally owned enterprise, GIZ supports the German Government
in achieving its objectives in the field of international cooperation for
sustainable development.

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn

Division Global Policy, Governance
Section Governance, Human Rights
Sector Programme Governance

Friedrich-Ebert-Allee 36
53113 Bonn, Germany
T +49 228 44 60-0
F +49 228 44 60-17 66

Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Germany
T +49 61 96 79-0
F +49 61 96 79-11 15

E info@giz.de
I www.giz.de

Responsible:
Sector Programme Governance

Authors:
Mable Barbara Amuron
Richard Ngamita

Contact:
sv-governance@giz.de

Design und Layout:
Barbara Reuter | Oberursel | Germany | barbarareuter-grafik@web.de

Photo credits:
Photo on the cover and backpage © AdobeStock, dadakko – AI
Photo on page 9 © AdobeStock, William – AI | on page 10 © AdobeStock, Dream – AI |
on page 13 © AdobeStock, felasteri - AI | on page 14 © AdobeStock, Engineer Jahid – AI |
on page 16 © AdobeStock, Rashid – AI | on page 24 © AdobeStock, nikomsolftwaer – AI |
on page 30 © AdobeStock, buraratn – AI

URL links:
This publication contains links to external websites. Responsibility for the content of the listed external sites always lies with their respective publishers. When the links to these sites were first posted, GIZ checked the third-party content to establish whether it could give rise to civil or criminal liability. However, the constant review of the links to external sites cannot reasonably be expected without concrete indication of a violation of rights. If GIZ itself becomes aware or is notified by a third party that an external site it has provided a link to gives rise to civil or criminal liability, it will remove the link to this site immediately. GIZ expressly dissociates itself from such content.

Maps:
The maps printed here are intended only for information purposes and in no way constitute recognition under international law of boundaries and territories. GIZ accepts no responsibility for these maps being entirely up to date, correct or complete. All liability for any damage, direct or indirect, resulting from their use is excluded.

On behalf of
German Federal Ministry for Economic Cooperation and Development (BMZ)
Division G12: Governance
Bonn, Germany

GIZ is responsible for the content of this publication.

Eschborn/Bonn November 2025

Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn

Friedrich-Ebert-Allee 36 + 40
53113 Bonn, Germany
T +49 228 44 60-0
F +49 228 44 60-17 66

Dag-Hammarskjöld-Weg 1 - 5
65760 Eschborn, Germany
T +49 61 96 79-0
F +49 61 96 79-11 15

E info@giz.de
I www.giz.de

On behalf of

Federal Ministry
for Economic Cooperation
and Development