How Enhanced State Surveillance is Hurting Digital Rights in Africa

June **2023**

Over the last few years, Africa has experienced a rapid increase in internet access, with millions of online users *engaging* on a wide range of issues on social media and other digital platforms. By the end of 2022, there were an estimated *570 million* internet users in Africa, more than double the number reported in 2015. However, despite this recent growth in internet usage, Africa continues to experience a steady decline in digital rights and a *shrinking civic space.*

The growth in internet penetration over the last few years has been matched with progressive developments such as the enactment of privacy and data protection laws, entrenching of the rights to online freedom of expression and access to information into national constitutions, and adoption of cybercrime laws. However, several other measures have undermined the progress.

In particular, several countries on the continent have weaponised technology against critics, opposition groups, journalists, and human rights defenders by deploying mass surveillance and interception of communications schemes that have undermined free speech and the rights to association and assembly.

This brief highlights trends in state surveillance in select African countries and how it is hurting rights online.

Redefining Digital Rights

Digital rights were firmly established in 2016 when both the *African Commission on Human and Peoples' Rights* (ACHPR) and the *United Nations* (UN) passed landmark resolutions affirming that the same rights that people have offline must also be protected online. In particular, the resolutions singled out the right to freedom of expression, access to information and privacy and personal data protection.

The ACHPR resolution particularly calls upon countries to respect and take legislative and other measures to guarantee, respect, and protect citizens' right to freedom of information and expression through access to internet services. On the other hand, the UN resolution calls upon "states to consider formulating, through transparent and inclusive processes with all stakeholders and adopting national internet-related public policies that have the objective of universal access and enjoyment of human rights at their core".

Although *state surveillance is not inherently* unlawful since governments can have legitimate reasons to undertake surveillance where necessary to prevent terrorism, monitor critical security threats, and investigate crime, several countries have enacted laws and policies to legitimise their surveillance practices through state agencies' interception of private communication with limited oversight, while the surveillance technologies being deployed have altered the nature and scope of how governments conduct surveillance.

Intermediary Liability in State Surveillance

Across the continent, there have been *reports* of strenuous and sometimes unclear demands by states on intermediaries, including facilitating interception of communication, disclosing communication data of their subscribers to state security agencies, and taking down content or shutting down the internet. In countries such as Mozambique, Tanzania, Uganda, Zambia, and Zimbabwe, legal provisions requiring mandatory compliance by third parties to government interception requests have been introduced, undermining civic freedoms.

In *Mozambique*, for example, Decree No. 33/2001 requires network operators to cooperate with the authorities regarding the legal interception of communications. And although article 68 of the 2004 Telecommunications Law provides for the secrecy of a user's communications, it makes exceptions, including in criminal investigations and in the interest of national safety and the prevention of terrorism.

In Tanzania, regulation 13(1)(d) of the repealed Electronic and Postal Communications (Online Content) Regulations, 2020 required Internet Café service providers to install surveillance cameras in their premises to monitor users' activities. In Uganda, section 28 of the Computer Misuse Act, 2011 and section 11 of Uganda's Regulation of Interception of Communications Act 2010 also require telecom companies to install systems that enable surveillance at their own cost.

In Zambia, *Section 38 of the Cyber Security and Cyber Crimes Act 2021* requires electronic communication service providers to use electronic communication systems that are technically capable of supporting lawful interceptions, install hardware and software facilities and devices that enable interception, provide services capable of rendering real-time and fulltime monitoring facilities for the interception of communications, and provide call-related information in real-time or as soon as possible upon call termination.

Zimbabwe's *Interception of Communications Act, 2007* requires telecommunications service providers to have, at their own cost, "the capability of interception" and ensure that their services are "capable of rendering real-time and full-time monitoring facilities for the interception of communications and storage of call-related information.

Enhanced Surveillance Capabilities

In addition to the legal regime around service provider assistance for surveillance, several African governments have enhanced their technical capacity to intercept and monitor electronic communications through procurement and installation of equipment and software that enables remote control hacking and eavesdropping, deployment of video surveillance systems, some of which have facial recognition capabilities, and roll-out of biometric data collection programs.

The use of spyware appears to be rising, with several countries increasingly being outed by *research* as among those who have acquired technology that allows governments to snoop on private communications and monitor, with precision, citizens' movements.

In 2021, the Ugandan government announced the *adoption* of the Intelligent Transport Management System (ITMS) that would involve the re-registration of all motor vehicles, motorcycles, and other vessels using an electronically activated device to be affixed to the motor vehicle, purportedly to curb insecurity and criminality. The move, which has since been *delayed* due to failure by the contractor to deliver on time, raised serious privacy questions as peoples' movement could be monitored and tracked in real-time, and the possible *misuse* of the system by security agencies.

In Zimbabwe, the government in July 2022 *launched* a USD 500 million Cybercity project which would result in the installation of surveillance cameras within the capital Harare for "purposes of security and similar initiatives." The project is expected to be rolled out in the rest of the country over the next few years. Like the Ugandan digital motor-vehicle number plates, the initiative has *raised* several privacy and data protection concerns, as the deployment and use of surveillance cameras in the country means that the government can quickly and with precision identify and target those with dissenting voices.

Earlier in January 2015, the Zimbabwean government was reported to have *acquired* various cyber-surveillance technologies from the Iranian government. The equipment is said to have been used to aid the government in ratcheting up suppression and snooping on the political opposition and other organisations the government considered a national security threat.

In 2020, several countries, including Botswana, Equatorial Guinea, Kenya, Nigeria, Zambia, and Zimbabwe, were *reported* to be using the surveillance platform Circles to exploit flaws in telecom systems and to access telephone calls, SMS messages, and location services. The investments in communication monitoring systems, including the installation of closed-circuit television (CCTV) systems, have become key components of the increasing state surveillance within the region.

In addition, several countries have criminalised the provision of encryption services that would guarantee anonymous communication. For example, countries like Tanzania and Zambia have penalties for offering cryptographic services without licensing, registration, or authorisation. Interception of communications provisions in various countries' laws often require service providers to decrypt any encrypted information they may intercept when offering assistance to lawful interception. In Tanzania, the law requires the encryption services providers to disclose the encryption technologies they plan to use upon registration with the authorities.

While there has been some progress in the enactment of privacy and data protection laws that require an interception warrant or order from a judicial officer, countries such as Tanzania, Zambia, and Zimbabwe fall short of the provisions of the Africa Union's Declaration of Principles of Freedom of Expression and Access to Information in Africa (the Declaration) such as manner and scope of surveillance, and transparency on the surveillance activity, including notification requirements.

Impact on Digital Rights and Civic Spaces

The right to privacy

The *right to privacy* online has become critical due to its intricate connection with and being the foundation for the protection and realisation of other rights, including the rights to freedom of expression, information, assembly, and association. However, the pervasive nature of state surveillance in Africa has directly impacted digital rights and civic spaces, as it affects an individual's right to privacy and, by extension, the freedom to express themselves, associate, and assemble. While there has been a surge in the number of countries that have enacted privacy and data protection laws in Africa, many of them contain *retrogressive provisions* that leave scope for intrusion, including enabling state surveillance without sufficient safeguards and oversight.

The lack of comprehensive data protection laws exacerbates concerns about the potential for the misuse of such data. The absence of independent data protection authorities, poor enforcement of data privacy laws where they exist, and the loopholes in the regulation of interception of communication laws, present additional concerns.

Freedom of Expression and Access to Information

Access to the internet has become fundamental to the enjoyment of digital rights, particularly the right to freedom of expression and access to information. Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR) emphasises that the right to freedom of expression applies regardless of frontiers and through any media of one's choice. Principle 3 of the *African Declaration on Internet Rights and Freedoms* notes that "everyone has the right to hold opinions without interference and the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds."

However, several *studies* in various countries have found that surveillance practices cause human rights defenders, including journalists and online users, to self-censor and refrain from exercising their rights due to easy identification and ease of traceability. The *ability* to remain anonymous when communicating or expressing oneself without fear of government interference or public retaliation is critical to expanding any democratic dispensation. However, collecting, processing, and sharing personal data has become a critical component in facilitating surveillance and the identification of surveillance targets, with several countries *enforcing* mandatory Subscriber Identification Module (SIM) registration laws that require all communications users to link their electronic communications to their legal identities.

The extensive information collected under SIM card registration and other biometric data collection programs has *enabled* governments to easily identify and track citizens and their communications. *Researchers* have noted that many African states are deploying Artificial Intelligence (AI) surveillance technologies to monitor citizens for various purposes, but seldom in rights-respecting or privacy-respecting ways.

Conclusion

Respect for digital rights and civic space has become a *cornerstone* of functioning democracies as it enables citizens and justice actors to meaningfully participate in key decision-making processes as they can access information and freely express themselves without fear of reprisals from state agencies. Unfortunately, many citizens and civil society actors are not *equipped* with the right skills, knowledge, and tools to respond to the increasing and more sophisticated government surveillance tactics. There is also limited awareness among citizens of their privacy rights.

Recommendations

- As governments become more sophisticated and emboldened in their approach to digital surveillance, it is critical that civil society actors strengthen their capacity and enhance their organisational practices, especially the implementation of security and safety measures related to digital and social media platform usage by the organisations and their staff. More specifically,

- Governments should repeal, amend or review existing laws, policies, and practices on surveillance, interception of communication, biometric data collection, and limitations on the use of encryption to ensure compliance with the established international minimum standards on human rights and communications surveillance.
- Civil society actors should partner with the media to investigate, document, and expose data and privacy breaches such as unauthorised access, surveillance, and non-compliance by data collectors, controllers, and processors.
- The media should strive to continuously expose and report all cases of unlawful surveillance and interception of communications through various platforms so as to push for accountability and transparency against the key perpetrators.
- Telecom companies, including internet service providers, should challenge laws, policies, and directives that place on them undue intermediary liability obligations through utilising litigation in national and regional courts and other quasi-judicial processes such as tribunals.
- Intermediaries should regularly publish, update and widely disseminate privacy policies and transparency reports and inform users about the collection, use, handling, sharing and retention of their data and the measures taken to protect their right to privacy.

CIPESA
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place (Off Semawata Road) Ntinda, Kampala
programmes@cipesa.org
@cipesaug facebook.com/cipesaug Linkedin/cipesa
www.cipesa.org