Digital Authoritarianism and Democratic Participation in Africa

June **2022**

Introduction

Africa has registered remarkable growth in digitisation with increased internet penetration and use of Information and Communication Technologies (ICT). However, the proliferation of ICT and other new and emerging technologies has significantly expanded states' toolkit for repression and social control, deepening human rights challnges. Several African governments have embraced digital authoritarianism characterised by aggressive and sophisticated measures that curtail internet freedoms. These have included using digital technologies to surveil, repress and manipulate domestic and foreign populations.

Although state surveillance is not new, it has dramatically expanded with the increased digitisation. Further, surveillance has been digitalised and automated, making mass surveillance possible. Numerous countries across the continent have adopted policies and enacted laws that permit states and their respective agencies, especially security services, to use ICT to conduct surveillance; impose liability on telecommunication intermediaries to facilitate the interception of communication; stipulate the mandatory collection of biometric data; limit the use of encryption; require the localisation of personal data; and grant law enforcement agents broad search and seizure powers.

This brief discusses the key control measures adopted by some African states in enforcing digital authoritarianism and their effect on democratic participation.

Digital Authoritarian Control Measures

Legalising Surveillance and Interception of Communication

Countries have legalised state surveillance and the interception of communication on the pretext of fighting cybercrime, maintaining national security, and ensuring public order. The laws in themselves are not the main problem, as states have a duty to protect citizens against cybercrime and to ensure public order, including through enactment of laws. However, the laws are often fraught with loopholes which states can exploit. Common gaps include the lack of transparency and accountability mechanisms, such as robust independent oversight over surveillance, and the excessive powers handed to state security agencies.

For instance, in Lesotho, regulation 13 of the Compliance Monitoring and Revenue Assurance Regulations, 2021 requires licensees to allow the Lesotho Communication Authority or its representative to install and maintain "necessary equipment" on licensees' networks. Furthermore, the operators are required to facilitate the "installation of data transmission equipment between the Authority's monitoring system installed at their switch centers and the Authority's main operating center", a requirement which perpetuates privacy infringement by enabling real time monitoring, interception and surveillance.

In Zambia, under sections 29 and 30 of the Cyber Security and Cyber Crimes Act, 2021, an enforcement officer may intercept any communication and the request may be made orally to a service provider "on reasonable grounds to prevent possible or inflicted bodily harm, loss of life or threats to kill oneself, or damage to property or actual or possible cause of financial loss." Meanwhile, the Electronic Communications and Transaction Act, 2009 requires law enforcement officers to apply for an order to a judge or the Attorney General for permission to conduct interception. Such authorities may conduct communication interceptions for any offense, regardless of its nature.

In Mozambique, although article 68 of the 2004 Telecommunications Law provides for the secrecy of a user's communications, it stipulates grounds for exceptions, including in criminal investigations and in the interests of national safety and the prevention of terrorism. In addition, article 35 of the law on licensing and registration of telecommunications service providers (Decree No. 33/2001 of 6 November) obliges licensed providers to cooperate with the legal competent authorities regarding the legal interception of communications.

Uganda's Anti-Terrorism Act of 2002 permits the interception of communications on grounds such as safeguarding of the public interest; prevention of the violation of the fundamental and other human rights and freedoms of any person from terrorism; prevention or detecting the commission of any offence; and safeguarding the national economy from terrorism. Furthermore, section 8 of the Regulation of Interception of Communications Act, 2010 requires service providers to provide mandatory assistance that enables easy interception of communications.

In Tanzania, interception of communications is explicitly provided for in the 2002 Prevention of Terrorism Act and the 1996 Intelligence and Security Service Act. Under Section 31 of the 2002 Prevention of Terrorism Act, "a police officer may for the purpose of obtaining evidence of the commission of an offence under this Act, apply, ex parte, to the Court, for an interception of communications order." Section 31(4) of this Act allows for the use of any communications intercepted, including from outside of the country, to be admissible in proceedings for any offense under the Act.

The desire to entrench surveillance has seen the introduction of legal provisions requiring mandatory compliance by third parties with government interception requests. In several countries, intermediaries such as telecom companies and Internet Service Providers (ISPs) are required by law to facilitate surveillance including by installing equipment and software that enable governments to lawfully intercept communications on their networks. Failure to comply attracts hefty penalties.

Moreover, section 14 of the Intelligence and Security Service Act empowers the Tanzania Intelligence and Security Service (TISS) to collect, analyse, and retain "information and intelligence respecting activities that may on reasonable grounds be suspected of constituting a threat to the security of the United Republic or any part of it." Whilst the terms ``security" and "threats to the security of the United Republic'' are defined by the Act, their broadness is highly concerning and provides the TISS with extensive powers and minimal provisions for oversight over the agency.

The desire to entrench surveillance has seen the introduction of legal provisions requiring mandatory compliance by third parties with government interception requests. In several countries, intermediaries such as telecom companies and Internet Service Providers (ISPs) are required by law to facilitate surveillance including by installing equipment and software that enable governments to lawfully intercept communications on their networks. Failure to comply attracts hefty penalties.

In Uganda, the failure by intermediaries to comply with the requirement to support interception attracts a fine of not more than UGX 2.4 million (USD 641) or imprisonment for a period not exceeding five years, or both. In Zambia the penalty is a fine of 150,000 Kwacha (USD 6,643), imprisonment for up to five years, or both. Such a high penalty as stipulated in the Zambian legislation could compel service providers to render interception assistance even when they receive dubious or oral orders that lack judicial backing or any evidence justifying the interception.

In Zimbabwe, the government enacted the 2007 Interception of Communications Act, which 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. In addition, the interception law does not provide for judicial oversight in issuance of warrants, Instead, it grants the powers to the minister in charge of communications, or any other minister assigned by the president to issue such interception orders.

Enhanced Surveillance Capacity

Across the continent, governments have invested in building the technical capacity of their security agencies to carry out widespread surveillance and interception of communication through the acquisition of surveillance software, installation of Closed-Circuit Television (CCTV) systems and spyware, and skills building.

In 2016, the government of Mozambique began the installation of CCTV surveillance in the cities of Maputo and Matola, purportedly for security purposes. The project was allegedly awarded without a public tender. Also in 2016, there were reports that the Mozambican government was intercepting and surveilling citizens' online communications, with the support of a Chinese company - ZTE.

In April 2017, Tanzania signed an agreement with South Korea to enhance the country's cyber capabilities. Under the five-year Memorandum of Understanding (MoU), the Korea Internet & Security Agency (KISA) would offer Tanzania expertise, monitor the security of the cyber infrastructure, and put money into the sector. In March 2018, Israel and Tanzania signed a military training and intelligence gathering and sharing agreement. The countries agreed to intensify their collaboration in key defense and security matters, particularly in troops training, cyber and inter-territorial security as well as improved military technology.

In Uganda the government is reported to have, in 2012, enhanced its mass surveillance capacity using spyware, intrusion malware, and intelligent network monitoring systems. In July 2018, the Uganda communications regulator, UCC was reported to have installed an Intelligent Network Monitoring System (INMS) with the capacity to track all calls made on all networks, mobile money transactions, fraud detection and billing verification. In 2019, there were reports that Huawei staff aided Uganda's security agencies to spy on President Museveni's political opponents as they mobilised to oust him in the 2021 elections. According to the report, Huawei technicians helped Ugandan intelligence services infiltrate encrypted communications of Museveni's main challenger, Robert Ssentamu Kyagulanyi, a.k.a. Bobi Wine, and were as a result able to monitor his movements and scuttle his mobilisation rallies.

In January 2015, Zimbabwe's government was given various cyber-surveillance technologies, including the International Mobile Subscriber Identify (IMSI) catchers, from the Iranian government.[1] The equipment was said to aid the government to keep its foreign policy foes at bay, and ratchet up suppression and snooping on the political opposition and other organisations it considered a national security threat.

In 2019, Zambia initiated a "Safe City" Project under which Huawei mounted 24-hour surveillance cameras in public places and on the main road networks without adequate judicial oversight and monitoring to guard against possible abuse by law enforcement agencies. This video surveillance system was concerning, as a 2020 report by Citizen Lab, a global digital rights watchdog, for the second time identified Zambia as a possible customer of cyber espionage software. In 2019, Huawei technicians allegedly helped the government access the phones and Facebook pages of opposition bloggers behind a pro-opposition news site that had criticised President Edgar Lungu. The Huawei employees reportedly located the bloggers and were in contact with the police units deployed to arrest them.

Massive Collection and Processing of Personal Data

Several governments are undertaking rapid data collection and digitisation initiatives, including e-government services, digital identity, biometric voters' cards, drivers' licenses, and SIM card registration. Unfortunately, most of the data collection programs are done without adequate data protection laws, amidst limited oversight mechanisms and inadequate remedies. While many have recently passed data protection laws and policies, implementation is not effective, and the safeguards are not watertight as required under international human rights law.

In 2012, the Zambian government issued a new policy requiring citizens to register their mobile phone SIM cards, using their real identities. The Zambia Information and Communication Technology Authority (ZICTA) stated that citizens must register their SIM cards by December 31, 2013, or they will begin to lose certain services. In addition, phones will be fully deregistered by February 15, 2014 if owners did not comply with the registration order.

1 *An 'IMSI catcher' is a device that locates and then tracks all mobile phones that are connected to a phone network in its vicinity, by 'catching' the unique IMSI number.*

In addition, mandatory SIM card registration is further provided for under section 39 of the Cyber Security and Cyber Crimes Act 2021 requires electronic communication service providers to collect personal data from individuals including names, residential addresses and identity numbers contained in identity cards before entering a contract for provision of any service.

Several governments are undertaking rapid data collection and digitisation initiatives, including e-government services, digital identity, biometric voters' cards, drivers' licenses, and SIM card registration. Unfortunately, most of the data collection programs are done without adequate data protection laws, amidst limited oversight mechanisms and inadequate remedies.

In Tanzania, SIM card registration has been ongoing since 2009, and currently it is not possible to register a SIM card unless the biometric information collected is verified against the National Identification Authority (NIDA) database, which was created under the Registration and Identification of Persons Act. Increasingly, public institutions in Tanzania have moved to make the National ID or National Identification Number (NINs) the "primary/mandatory requirement for identification for service provision, including institutions like the Higher Education Loans Board, the Tax Revenue Authority, Business Registration, Licensing Authority and the Government Recruitment Agency."

Zimbabwe introduced compulsory SIM card registration in 2013 through the Postal and Telecommunications Regulations Statutory Instrument 95 of 2014 (Subscriber Registration), which also created a centralised subscriber database of all users that is managed by the communications industry regulator. Regulation 8(2)(c) of the Postal and Telecommunications (Subscriber Registration) Regulations, 2014 provides that, through this database, the regulator shall, among others, assist law enforcement agencies in safeguarding national security.

In Uganda, mandatory registration of SIM cards was introduced in 2012 following a campaign by the UCC to fulfill its mandate under the Regulations of Interception of Communications Act (2010). The commission stated that the exercise was necessary to curb crime by enabling the tracking of criminals and identification of mobile phone SIM card owners. During the 2016 elections, the Electoral Commission extracted data from the National Identification and Registration Authority (NIRA) national ID database to compile the national voter register. Fraught with inconsistencies and errors, the electoral body was called out by a team of activists for flaunting the voter register with 20,000 ghost voters. The unfettered access to the national ID database by different bodies, including security and law enforcement and private sector corporations such as telecom and technology service providers raised questions on the ability of arbitrary actors to abuse very sensitive personally identifiable information during electoral cycles.

In 2011, the government of Lesotho passed the National Identity Cards Act 2011, which paved the way for establishing a national digital identity register and issuing national identity cards . In 2013, the register, managed by the Department of National Identity and Civil Registry in the Ministry of Home Affairs, was established based on this law. The Act requires that all eligible persons use the national ID card to "access all services."

Effects on Digital Rights and Democratic Participation

Digital authoritarianism tools such as surveillance and the interception of communication undermine the privacy of communications and the right to anonymity. Consequently, they can lead to self-censorship and the withdrawal of some individuals and groups from the online public sphere.

In addition, on a continent where most countries are experiencing increasing degrees of democratic regression, disinformation campaigns have added to the arsenal of tools and tactics used by governments to stifle digital rights, distort the truth, advance propaganda, sway public opinion, manipulate the online sphere and consequently undermine the respect for human rights and democracy participation. Yet others have deployed digital taxation, internet disruptions, arrests and prosecution of social media users, mandatory registration and licensing of online content creators, and criminalisation of online speech, particularly "false information"

In addition, on a continent where most countries are experiencing increasing degrees of democratic regression, disinformation campaigns have added to the arsenal of tools and tactics used by governments to stifle digital rights, distort the truth, advance propaganda, sway public opinion, manipulate the online sphere and consequently undermine the respect for human rights and democracy participation. Yet others have deployed digital taxation, internet disruptions, arrests and prosecution of social media users, mandatory registration and licensing of online content creators, and criminalisation of online speech, particularly "false information".

Undermining the Right to Freedom of Expression and Access to Information

The inability to freely express oneself has a direct impact on democratic participation since it limits an individual's engagement in political discussions and the capacity to influence others, especially during periods of political contestation. Political censorship continues to be used to block content that is critical of governments. In addition, the fear of repercussions leads to self-censorship, as many individuals now exercise restraint, are less vocal, and limit their comments and opinions especially in political conversations or debates online and offline - including on social media, phone conversations, public meetings and in interactions with government officials. Media sources are also placed at risk due to the surveillance and interception of journalists' communication. This is because the deployment of surveillance technologies and large-scale data collection and retention pose risks in terms of reprisals against media workers and their sources, thereby affecting the free exercise of journalism.

Relatedly, disinformation campaigns have also been used to perpetuate hate speech, and hand autocratic governments an excuse to crack down on legitimate expression by critics and dissenters and to generally muzzle an open and free internet. Several governments have weaponised disinformation laws to silence critical voices, undermine political discourse, and hamper free expression.

Infringing on the Right to Privacy of Communications

The right to privacy is associated with the rights to freedom of expression, access to information, freedom of movement, freedom from discrimination and the principle of government accountability. Surveillance and the interception of communication intrude on the privacy of individuals as they involve tracking and monitoring their communication and activities.

Surveillance and hacking compromise citizens' rights to privacy of their communication. For the media, the exposure of information gathered by journalists, including from whistle-blowers, violates the principle of source protection, which is universally considered a prerequisite for freedom of the media and is enshrined in UN Resolutions. In addition, surveillance may harm the safety of not only journalists but also "netizens" by disclosing sensitive private information, which could be used for arbitrary judicial harassment or attack.

The fear of surveillance has forced many journalists, political actors, and ordinary citizens to keep a low profile online, to significantly reduce their online activities, and to become reluctant to use social media platforms and digital communication channels. Many potential targets of surveillance tend to be more cautious with their digital communications and some constantly adapt the latest tools that secure the privacy of their communications, such as setting chats to disappear after conversations, regularly changing communication channels, and encrypting communications. They avoid discussing, or sharing over their mobile devices, sensitive information such as activism plans, meeting details, and information sources.

Curtailing Freedom of Assembly and Association

Freedom of assembly and association has a direct link with freedom of expression and access to information. The ability to organise and mobilise for activities, especially political meetings, has been adversely affected by state surveillance. The deployment of digital technologies gives regimes the power not only to react to online actions, but also to carry out online tracking and to prevent actions such as mobilisation and protests against bad governance.

By forcing the victims of surveillance to be mistrustful of both strangers and even some of their own associates, surveillance has severely affected the ability of such individuals to do their work (in the case of journalists and HRDs) or to mobilise for causes they are passionate about (for HRDs and opposition politicians).

Undermining Civic Participation

One of the distinguishing features of democratic societies is the ability of the citizens to participate in decision-making processes actively and meaningfully, and the extent to which governments open up to citizen involvement and the space for citizens to hold the government accountable. This includes the ability to express dissent, support parties opposed to the government, and hold those in power accountable.

However, there are prerequisites to citizens' meaningful participation, such as safe and trusted mediums for participation, confidence that their participation will be meaningful, and that there shall be no sanctions or reprisals for expressing their opinions and choices.The various digital control measures that have been deployed by states have eroded many of these prerequisites, with the sum effect that the ability and proclivity of citizens to participate is now at its lowest.In addition, when citizens are unable to enjoy an unfettered right to access and impart information, civic space is constrained, various rights and freedoms are hindered, and democracy suffers.

Conclusion

The rise of digital authoritarianism has greatly undermined citizens' rights to enjoy the benefits of digital technology. Several of the tools and control measures that states have employed include the surveillance and interception of communications, poorly regulated collection and processing of personal data including biometrics, as well as the weaponisation of laws that have fundamentally undermined the enjoyment of fundamental freedoms such as freedom of expression, assembly and association. Collectively, these controls measures have continued to undermine citizens digital rights and democratic participation and cement authoritarians' hold on political power.

CIPESA

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

+256 414 289 502

programmes@cipesa.org

@cipesaug facebook.com/cipesaug Linkedin/cipesa

www.cipesa.org