State of Internet Freedom in Africa 2023

A Decade of Internet Freedom in Africa: Recounting the Past, Shaping the Future

10

CIPESA

Table of Contents

Essays

September 2023

State of Internet Freedom in Africa - 2023
A Decade of Internet Freedom in Africa: Recounting the Past, Shaping the Future

Introduction and Background

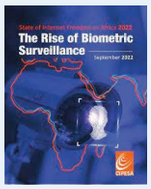
Over the years, CIPESA has been instrumental in defending and expanding the digital civic space to protect and promote human rights and enhance democratic governance. With a focus on disparate actors including government, the private sector, civil society, media, policy-makers and multinational institutions, CIPESA has consistently produced thought-evoking research on various facets of technology for the public good, which informs policy and practice around internet and ICT regulation and use. Some notable examples include various frameworks CIPESA has developed, such as one that fed into the Cost of Internet Shutdowns Tool (COST) for calculating the economic impact of internet disruptions, the Africa Media Freedom and Journalists' Safety Indicators for assessing the safety of journalists and media freedom, and Digital Accessibility Indicators for assessing compliance with ICT and disability rights obligations by governments and the private sector in Africa.

The State of Internet Freedom in Africa Report

CIPESA's work responds to a shortage of information, research, resources and actors consistently working at the nexus of technology, human rights and society. Indeed, CIPESA's establishment in 2004 was in response to the findings of the Louder Voices Report for DFiD, which cited the lack of easy, affordable and timely access to information about ICT-related issues and processes as key barriers to effective and inclusive ICT policy-making in Africa.

In line with this objective and towards the furtherance of its mission, CIPESA's flagship annual State of Internet Freedom in Africa Report documents trends in internet freedom in African countries and has remained a key reference point for various state and non-state actors on key issues of digital rights and those affecting the digital society and digital economy. The report has been instrumental in complementing the work of state and non-state actors including by providing contextual information and generating evidence to inform ICT policy-making and practice; creating awareness on internet freedom issues on the continent, and shaping conversations by digital rights actors across the continent.

The first edition of the report was published in 2014. Subsequently, eight annual regional reports and various country reports have been published. The regional reports, as summarised below, have covered a wide range of topics in the past decade:



2022 - The Rise of Biometric Surveillance: The report highlights the increasing risks in the use of biometric technologies by governments for surveillance and social control in Africa. The report raises concern that in the absence of adequate safeguards, biometric technologies such as facial recognition, fingerprinting, and iris scanning could be abused to monitor citizens' activities, track their movements, and limit their freedoms.

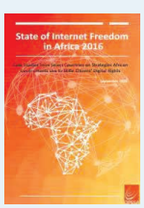
2021 - Effects of State Surveillance on Democratic Participation in Africa: The report documents how surveillance practices are becoming more pervasive in Africa, with governments using advanced technologies to monitor citizens' online activities and infringing on their right to privacy. These practices have had a chilling effect on freedom of expression, association, and assembly, and limited opportunities for civic participation and engagement.

2020 - Resetting Digital Rights Amidst the Covid-19 Fallout: The report focuses on the impact of the COVID-19 pandemic on digital rights and freedoms in Africa. It also highlights how the pandemic led to an increase in internet censorship, surveillance, and online violence against women, as well as the negative impact of internet shutdowns on access to information and public health messaging.

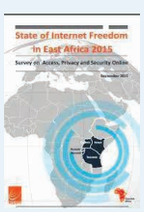
2019 - Mapping Trends in Government Internet Controls 1999-2019: The report provides an overview of the evolution of government internet controls in Africa over the past two decades. It highlights how African governments have increasingly adopted internet censorship and surveillance practices, implementing internet disruptions and arresting online activists, bloggers and journalists.

2018 - Privacy and Data Protection in the Digital Era: Challenges and Trends in Africa: The report highlights how African countries are lagging behind other regions in enacting data protection laws and regulations. It also highlights the increased risks of data breaches and other privacy violations and the impact on internet freedom.

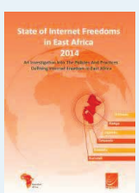
2017 - Intermediaries' Role in Advancing Internet Freedom in Africa: Challenges and Prospects: The report provides an overview of the role of intermediaries, such as Internet Service Providers (ISPs) and social media platforms, in promoting Internet freedom in Africa. It also highlights how African governments censor and control online content and the challenges faced by intermediaries in balancing their obligations under legal and regulatory frameworks and promoting internet freedom.



2016 - Case Studies from Select Countries on Strategies African Governments Use to Stifle Citizens' Digital Rights: The report provides an overview of the various strategies employed by African governments to restrict citizens' digital rights and examines case studies from a number of African countries, highlighting specific incidents of internet censorship, surveillance, and the persecution of online activists and journalists.



2015 - Survey on Access, Privacy and Security Online: The report surveyed internet users in six African countries and highlighted the challenges that they face in accessing the internet, protecting their privacy and security online, and accessing information. It also examined the role of governments in regulating the Internet, calling for greater transparency and accountability in their policies and practices.



2014 - An Investigation into the Policies and Practices Defining Internet Freedom in East Africa: The report provided an analysis of the policies and practices of governments and Internet Service Providers in Burundi, Ethiopia, Kenya, Rwanda, Tanzania, and Uganda. It also identified the key challenges facing internet users in these countries, such as censorship, surveillance, and online harassment.

Celebrating 10 years of the State of Internet Freedom in Africa Report

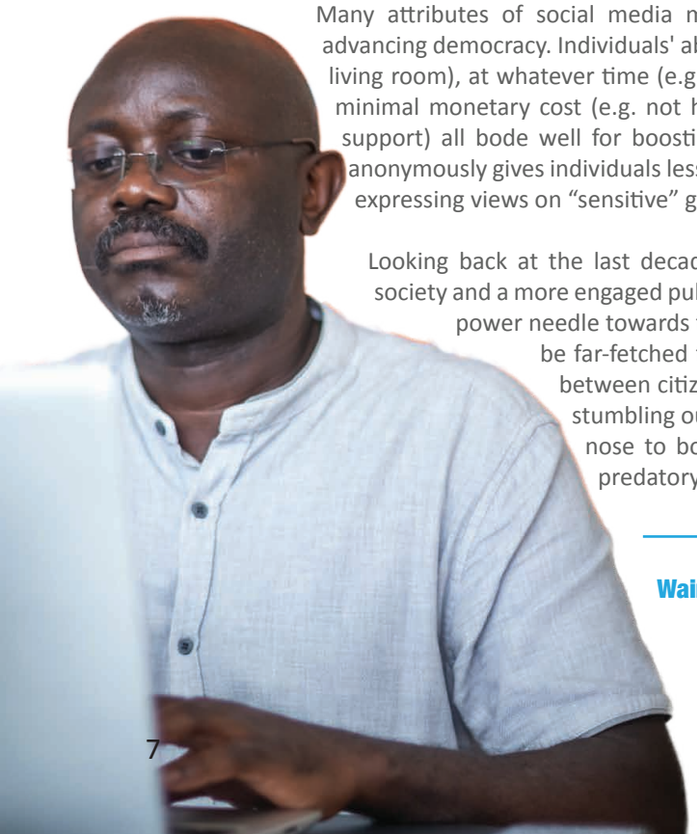
The year 2023 marks a decade since the first State of Internet Freedom in Africa report was produced. This also coincides with the 10th anniversary of the Forum on Internet Freedom in Africa (FIFAfrica). To celebrate these milestones CIPESA has produced this special edition to honour the efforts of various state and non-state actors in the promotion of internet freedom in Africa. It is also an opportunity to underline CIPESA's commitment to continue generating evidence-based research and strengthening partnerships and engagement through FIFAfrica.

The report and FIFAfrica 2023 will map the way ahead for digital rights in Africa and the role that different stakeholders need to play to realise the Digital Transformation Strategy for Africa and Declaration 15 of the 2030 Agenda for Sustainable Development on leveraging digital technologies to accelerate human progress, bridge the digital divide, and develop knowledge societies.

Digital Democracy Vs. [Digital] Authoritarianism: The Battle of Our Times

A decade ago, a common refrain went that Information and Communications Technology (ICT) would lead to more democratic systems and an engaged public, including in countries where open expression was proscribed. But there was also a niggling fear that autocratic governments would appropriate the power of technology to extend their stranglehold on civil liberties.

Optimism about technology's liberating power was not without basis. Digital technologies, such as social media, have functionalities that inherently render them a liberating technology in terms of the political relationships they enable, such as allowing ordinary citizens to speak out to or about those with power. Secondly, a decade ago there were handy examples to reference on how digital technology could be leveraged to challenge and weaken autocratic governments, in ways unfathomable before this technology proliferated.



Many attributes of social media make it amenable to boosting citizen participation and advancing democracy. Individuals' ability to participate from wherever they are (e.g. from their living room), at whatever time (e.g. engage in online political discourse at 02:00 am), and at minimal monetary cost (e.g. not having to travel to a rally to be able to mobilise political support) all bode well for boosting citizen participation. Moreover, the ability to engage anonymously gives individuals less fear of attracting reprisals for openly associating with and expressing views on “sensitive” governance matters.

Looking back at the last decade, has technology helped engender a more democratic society and a more engaged public? Has it helped to move the government-versus-citizens power needle towards the people and away from (autocratic) leaders? It may not be far-fetched to surmise that, in several countries, if this was a contest between citizens and their governments, it is the people that would be stumbling out of the boxing ring with their shirt in tatters and a bloody nose to boot. The authoritarians, well, they have a smirk on their predatory faces.

Wairagala Wakabi, PhD

Digital technology has thus turned out to be a double-edged sword, delivering some dividends for democracy but also handing autocrats new abilities to surveil their citizens and to repress dissenting views. Today, the encumbrances to citizens' online participation, and to digital democracy in general, are greater in range and more complex in nature than they were a decade ago. They are also more deliberate, the result of laws, financial investments, and dubious practices by governments, often aided by private entities and civic groups driven by profit motives.

Indisputably, technology has enabled cheaper and faster citizen organising, expression of dissenting views, swift mobilisation for democratic causes, and quicker generation and spread of diverse and pluralistic information. It has provided avenues for citizens to speak directly to power and enabled actors of limited power, or who would otherwise have had no platform, to get heard and sometimes to shape discourse on democracy. So, yes, digital technology has empowered citizens, civic actors and dissidents, and advanced pro-democracy causes.

However, no authoritarian African regime has been seated on its laurels. As technology handed citizens new tactics and mediums to challenge nepotism, authoritarianism, and corruption, the leaders adapted swiftly and steadily. The net result is that, today, several African governments boast a hefty stranglehold on technology's liberating power for democracy.

Methods of Authoritarian Control

Back in 2012, the methods of digital repression employed by authoritarian regimes in Africa were not as well understood as those in countries like Iran or China.[1] It was clear nonetheless that repression in the offline world would spread to the digital sphere. Back then, the tactics African governments were expected to adopt included curtailing citizens' access to ICT such as through censorship and filtering; surveillance; and efforts by regimes to shape online or social media content in their favour.[2]

This special issue of the State of Internet Freedom in Africa (SIFA) report presents 10 analytical and evocative essays that trace the trajectory of digital rights in Africa over the last decade, from the euphoria and optimism evoked by the Arab Spring to the deluge of retrogressive information controls that have been cast upon the region.

Authors in this special issue of SIFA explain that surveillance, propaganda, censorship, disinformation, infrastructure and access control have been prominent methods of repression. Admire Mare succinctly recounts how African countries have normalised and rationalised communications interception and surveillance. While charting four key trends, Mare notes that most smart surveillance technologies supplied to African governments by companies mostly from the USA, China, Europe, and Israel, have been used to monitor opposition politicians, human rights defenders, journalists, trade unionists, and civic activists. This has had a "chilling effect" on free expression and shrunk the civic space.

Another flavour of the moment is disinformation, which many governments have added to their authoritarian arsenal, and which is undermining electoral integrity, the safety of human rights defenders and weakening democracy.[3] Blaise Pascal Andzongo Menyeng and Rima Rouibi take a deep dive into how disinformation is affecting digital rights, highlighting cases from Algeria, Cameroon, the Central African Republic, Libya, Morocco, and Tunisia.

The special issue of the State of Internet Freedom in Africa (SIFA) report presents 12 analytical and evocative essays that trace the trajectory of digital rights in Africa over the last decade, from the euphoria and optimism evoked by the Arab Spring to the deluge of retrogressive information controls that have been cast upon the region

1 *Laverty, A. R. (2012). The Missing Connection: ICTs and Democracy in Africa, https://escholarship.org/uc/item/3gp3v8zv*

2 *Greitens, S.C. Authoritarianism Online: What can we learn from internet data in nondemocracies? Political Science & Politics , Volume 46 , Issue 2, DOI: https://doi.org/10.1017/S1049096513000346*

3 *CIPESA, Disinformation Pathways and Effects on Democracy and Human Rights in Africa, https://cipesa.org/wp-content/files/briefs/Disinformation_Pathways_and_Effects_Case_Studies_from_Five_African_Countries_Report.pdf*

Censorship has for years remained front and centre in the authoritarian's playbook and shows no signs of abating. A lucid analysis by Victor Kapiyo states that Africa accounted for more than half of all global cases of social media restrictions implemented in 2021, with WhatsApp, Facebook Messenger, Facebook, Twitter (X) and Instagram the most targeted platforms. These restrictions, argues Kapiyo, are a common measure by authoritarian regimes to control public discourse, access to information and expression online; disrupt online association and assembly; and restrict political participation in democratic processes such as elections and protests.

Meanwhile, Richard Ngamita locates censorship within the broader, often "sophisticated", spectrum of actions by governments to suppress dissent and posits that struggles around censorship, surveillance and corporate or government control of the internet will persist. He analyses how some governments are embracing technologies like Artificial Intelligence (AI)-enabled surveillance, facial recognition and big data analytics to monitor and control citizens, and concludes that civil society advocates will need to keep pushing back against those limitations and promote progressive regulatory approaches.

The Arab Spring: A Watershed Moment for Digital Rights

The Arab Spring provided a watershed moment for digital rights in Africa. It exemplified that citizens had the power to challenge autocracy, including in countries where the state had enjoyed a monopoly over communication channels and narrative setting, often through punishing dissent. But authoritarian leaders were watching, getting scared, and learning. They eventually enacted laws to prescribe cyber crimes, to enable interception of communications, and instituted measures such as website blockages, censorship of short messaging services, and disruption of networks.

The Arab Spring wave of demonstrations and uprisings started in Tunisia in December 2010, and by February 2012 had forced the rulers of Tunisia, Egypt,Libya, and Yemen out of power. The dominant storyline claims social media played a big role in these uprisings. Notably, the Arab Spring demonstrated how social media could create safe communication channels for citizens to coordinate collective opposition and express their dissent in the public sphere;[4] gather and spread information to counter the propaganda and apparatus of the repressive state; and enable easy and fast ways of spreading information for instance on protests.[5] More recently, social media was credited for aiding mobilisation that led to the 2019 removal of the Sudanese president from power, and the prevention of Algeria's president from running for a fifth consecutive term that same year.

However, online activism has since hit some headwinds. Nanjala Nyabola explores the significant backlash from authoritarian governments threatened by a highly organised and active public sphere. She notes that regulations on the digital civic space passed by several African governments have focused on taxation and attempts to censor or block social media instead of protecting the rights of people to use the internet during times of political transformation. Furthermore, Nyabola points to growing concerns about platforms keeping users' data safely, not least given growing government requests for this data.

Concerns about the vast amounts of personal data being collected and attendant data privacy and security concerns are also explored by Prof. Bitange Ndemo, who argues that, as a result of the widespread use of digital services, digital platforms often use personal data for targeted advertising and other purposes, raising questions about the extent to which individuals are unwittingly participating in an economic system driven by

4 Tufekci, Z. and Wilson, C. (2012), Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square. Journal of Communication, 62: 363-379. https://doi.org/10.1111/j.1460-2466.2012.01629.x

5 Wairagala Wakabi, Motivating eParticipation in Authoritarian Countries, http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A902111&dswid=1880.

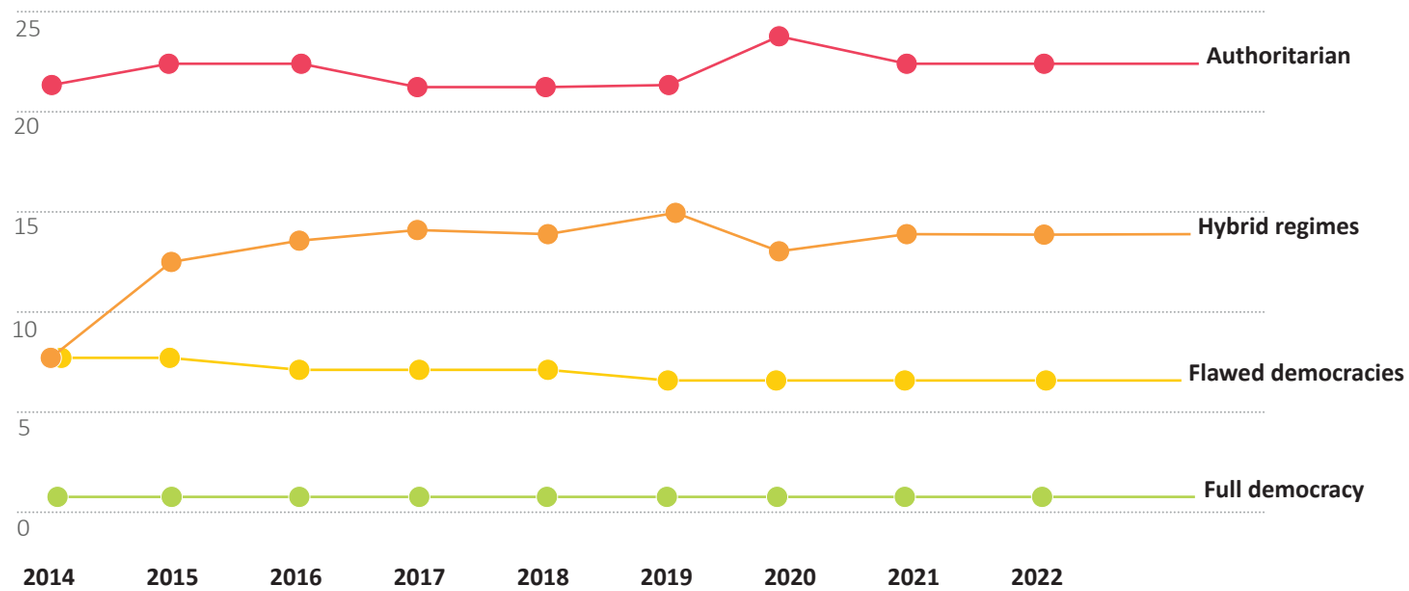
Delving into another dimension of this conundrum, Paul Kimumwe argues that governments have done little to ameliorate the problem, even as they are collecting huge amounts of data through mandatory SIM card registration, issuing national IDs, voters' cards and other exercises. In fact, Kimumwe contends that many government data collection programmes are implemented using weak and fragmented policy frameworks, limited dispute resolution mechanisms and inadequate remedies for privacy violations.

An enduring legacy from Egypt's revolution in 2011 is the practice of disrupting communication networks. Since Egypt cut off the internet 12 years ago, authoritarian governments across the continent have disrupted communications during protests and elections - a phenomenon brilliantly analysed by Felicia Anthonio. Anthonio writes that 37 out of Africa's 54 nations have imposed internet shutdowns. Up to 146 incidents of shutdowns have been registered in Africa since 2016, with authoritarian states taking the lead in imposing the disruptions.

When Offline Repression Escalates to the Digital Sphere

Democracy has been on retreat around Africa. Many leaders have held onto power for decades, elections are often not free or fair, political opponents are routinely harassed, media freedom is repressed, and public rallies by activists, social movements and political parties are often disrupted. According to the Economic Intelligence Unit's Democracy Index for 2022 - which measures electoral processes and pluralism, functioning of government, political culture, political participation, and civil liberties - half of the 44 countries assessed are authoritarian; most of the others are semi-authoritarian.[6]

Performance of African Countries on the Democracy Index



6 *Economist Intelligence Unit, Democracy Index 2022, https://www.eiu.com/n/campaigns/democracy-index-2022/*

Research has previously shown a link between longevity of leaders in power and their proclivity for digital repression, including ordering internet disruptions.[7] Accordingly, the digital authoritarianism being witnessed can not be divorced from the overall democratic regression and the longevity in power of authoritarian leaders. The last few years have seen many of the continent's longest-serving presidents leave the stage. Robert Mugabe was kicked out in 2017 after 37 years in power; Joseph Kabila exited in 2019 after 18 years; Omar Bongo died in 2019 after 41 years in the top seat; Omar al Bashir was deposed in 2019 after 30 years; Jose Eduardo dos Santos stepped down in 2017 after 38 years; and Idris Deby died in 2021 after 31 years as Togo's leader. Nonetheless, there is still a large crop of long-serving presidents, most of whose hold on power is credited to strong-arm tactics against opponents - and some tricks around the ballot box.

Africa's Longest-Serving Presidents

7 *CIPESA, Despots and Disruptions: Five Dimensions of Internet Shutdowns in Africa, https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/*

Censorship and repression are hallmarks of authoritarian regimes, as are limited pluralism, intolerance of opposition, and limited political participation. Other common features of authoritarianism include the existence of a single leader or small group of leaders with ultimate political authority, and belief in the supremacy of the authority of the state over all organisations in society and individuals' freedoms.[8] There are manifestations of these in numerous African countries, increasingly effected through "digital authoritarianism" - the use of technology tactics to advance repressive political interests.[9] As many essays in this issue demonstrate, the law is increasingly being weaponsided against digital rights and those that oppose authoritarianism. In numerous countries, the laws that regulate how citizens use digital platforms and exercise their digital rights are broadly worded, giving extensive powers to state agencies to interpret the laws and to interfere with citizens' rights.[10]

On the other hand, governments are failing to enact laws to address challenges that undermine many citizens' access to a safe internet. In Beyond the Screen: A Look at Gender and the Internet in Africa Over the Last Decade, Amanda Manyane illuminates the issue of online gender-based violence against women (OGBV), which is forcing many women to stay offline for fear of online abuse, thereby curtailing their participation in social, political, and economic spheres. Manyane writes that cybercrime laws being passed do not adequately address the full spectrum of the manifestations of OGBV. Further Manyana states, "Considering cybercrime from a gendered perspective is largely lacking, yet it is important in order to develop gender-sensitive crime prevention strategies and to ensure a more comprehensive approach to countering cybercrime and cyber violence."

Indeed, OVAW threatens to perpetuate the digital divide, a phenomenon which, Prof. Ndemo notes, prevents those without internet access from engaging in online civic spaces. Nonetheless, Prof. Bitange Ndemo charts the digitalisation path Africa has undertaken, from to AI, and provides insights into what the future is likely to hold for digitalisation and internet freedom in the region.

In Reflection on State Accountability for Digital Rights in the Past Decade: The Ups and Downs, Edrine Wanyama explains that states are mandated to ensure universal access to, and enjoyment of digital rights and freedoms, but "state accountability" for how governments are protecting and upholding these rights has had mixed results for internet freedom in Africa. He examines the role of the Universal Periodic Review (UPR) of United Nations Human Rights Council, special rapporteurs on freedom of expression and access to information, and regional courts in litigating network disruptions and digital rights issues in general, and offers recommendations on what needs to be done to leverage state accountability to better serve digital rights.

Looking Ahead

The state of internet freedom in Africa is worrying. Yet while the essays in this series largely paint a grim picture of where Africa stands today, not all is doom and gloom. Each essay in this report offers suggestions for how these authoritarian roadblocks can be navigated to ensure that the great majority of citizens in Africa can enjoy their online rights and for digital democracy to flourish.

Governments have enacted regressive and draconian laws that empower state agencies to limit the digital civic space. As a result, rights such as freedom of expression, access to information, and data privacy continue to come under threat … Various laws are being used to arrest, persecute, detain and prosecute individuals over online communication, as witnessed in the Democratic Republic of Congo, Mozambique, Kenya, Rwanda, South Sudan, Tanzania, Uganda, Zambia, Zimbabwe and several other countries. - Digital Democracy in Africa: What Has the Law Got to Do With It?

Dr. Wairagala Wakabi is the Executive Director of CIPESA.

8 *Lauth, H. (2012). Authoritarian Regimes. Online Dictionary Social and Political Key Terms of the Americas: Politics, Inequalities, and North- South*

9 *Apolo Kakaire, Countering Digital Authoritarianism in Africa, https://cipesa.org/2022/11/countering-digital-authoritarianism-in-africa/*

10 *Edrine Wanyama, Digital Democracy in Africa: What Has the Law Got to Do With It?, https://cipesa.org/2023/04/digital-democracy-in-africa-what-has-the-law-got-to-do-with-it/*

Internet Shutdowns: A Threat to Human Rights and Democratic Values in Africa

Introduction

Over the last decade, governments across Africa have been tightening their grip on power by cracking down on human rights both online and off. With a growing demand for accountability and good governance, people across several countries in the region are speaking up against injustices, aided in part by the widespread access to the internet and social media platforms that have been effectively used to mobilise and organise the protests. In response to people's power, governments are disrupting the digital ecosystem through rights-harming practices like internet shutdowns, censorship, surveillance, and the introduction of stringent legislation targeting human rights defenders, political opponents and sexual minorities, among others.

Since the government of Egypt imposed[11] a nationwide complete internet blackout in the country during the Arab Spring to quell protests and silence dissent in 2011, the practice has become a go-to tool for governments, military juntas, third-party actors and warring parties to stifle dissent and restrict human rights. The weaponisation of internet shutdowns and the growing digital authoritarianism across the globe is a dangerous trend that needs to be tackled urgently by all stakeholders.[12] People's lives, including education, health, business, work, transportation, agriculture, entertainment, and politics are increasingly extending to the online space.

Consequently, the internet and digital communication platforms have become rights enablers and must be protected. Internet shutdowns have proven to violate a wide range of human rights while countering efforts to close the digital divide. At the height of the COVID-19 pandemic in 2020, several governments encouraged people to work from home. Without access to the internet and digital platforms, the world of work would have seen a complete shutdown resulting in serious repercussions for life and economies.[13] Yet, Access Now and the #KeepItOn coalition recorded 155 incidents of shutdowns in 29 countries across the globe during the pandemic.[14] In 2023, the coalition has already documented more than 80 incidents of shutdowns in at least 21 countries. These numbers are likely to increase significantly by the end of the year.[15]

Access Now and the #KeepItOn coalition – a network of over 300 organisations fighting against internet shutdowns since 2016 - have adopted the following definitions of internet shutdowns:

- Technical definition: "An internet shutdown is defined as an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information."[16]
- Non-technical definition: "An internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. Shutdowns are also sometimes called "blackouts" or "kill switches" or "network disruptions."

Felicia Anthonio

11 Five years later: the internet shutdown that rocked Egypt https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/

12 Weapons of control, shields of impunity: Internet shutdowns in 2022 https://www.accessnow.org/internet-shutdowns-2022/

13 Impact of Internet Use during COVID Lockdown https://horizon-jhssr.com/view-issue.php?id=64

14 #KeepItOn https://www.accessnow.org/keepiton/; Shattered Dreams and Lost Opportunities: A year in the fight to #KeepItOn

15https://www.accessnow.org/wp-content/uploads/2021/03/KeepItOn-report-on-the-2020-data_Mar-2021_3.pdf

16 Who is shutting down the internet in 2023? A mid-year update https://www.accessnow.org/publication/internet-shutdowns-in-2023-mid-year-update/#join-us See more at: https://accessnow.org/keepiton

Internet shutdowns are mostly ordered by governments or state actors. They can be in the form of "complete", "total" or "blanket" shutdowns, or partial. Partial shutdowns include slowing down or throttling internet speeds, and blocking access to specific digital communications platforms such as websites or social media platforms.

Over the years, governments have also increasingly resorted to shutting down mobile internet connections, while sparing fixed cable connections for the privileged few. The impact of shutting down mobile internet connection, particularly in Africa, can be detrimental as a majority of the population in the region rely on this medium to access the internet. Internet shutdowns have also been implemented to target a whole nation, region or a group of people in identified communities. Some governments have turned to implementing more than one or all of the above types of shutdowns in response to escalating national crises.

Internet shutdowns violate the national constitutions of African countries, and regional and international frameworks including the African Charter on Human and People's Rights,[17] the Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019[18] and the International Covenant on Civil and Political Rights (ICCPR).[19] These frameworks uphold fundamental human rights including freedom of opinion and expression, access to information, right to assembly and social, economic, cultural and political rights. Also, shutdowns have gained a place on the global agenda with several governments, human rights experts[20] and heads of high-level institutions such as the UN, the African Union, the Freedom Online Coalition and the G7, denouncing internet shutdowns and urging governments to stop imposing them.

Yet, governments and powermongers struggle to justify these unjustifiable acts of repression — plunging their citizens into digital darkness. Authorities continue to cite "national security", "precautionary measures", the need to "prevent the spread of misinformation or hateful content online" or to stop "cheating" in school exams to justify shutdowns. On some occasions, no explanation is given by authorities for the shutdowns imposed.

There is no credible evidence to show that internet shutdowns have solved any of the above-listed 'problems'. If anything, shutdowns enable those in power to continue exerting control over the flow of information, provide them a shield to perpetrate human rights violations with impunity, deny people access to critical information, and amplify the spread of misinformation as shutdowns block access to alternative sources of verification.

17 *African Charter on Human and People's Rights https://www.achpr.org/legalinstruments/detail?id=49*

18 *Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019 https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf*

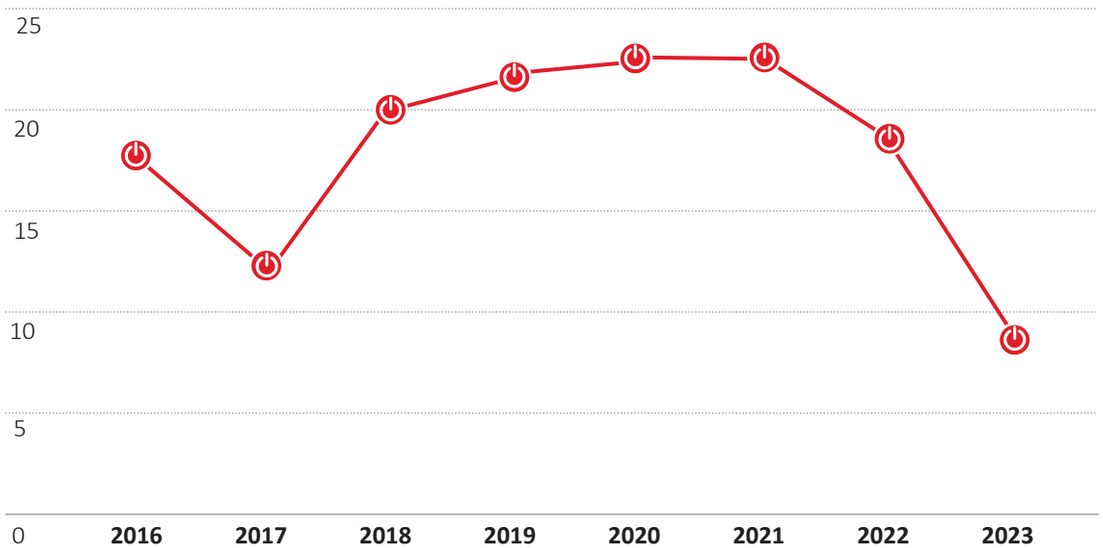
19 *International Covenant on Civil and Political Rights (ICCPR) https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf*

20 *Joint Declaration on Freedom of Expression and Responses to Conflict Situations https://www.osce.org/fom/154846*

Internet Shutdown Trends and Emerging Issues in Africa

Internet shutdowns have increasingly become a part of governments' information control playbook in Africa and around the globe, in democratic and authoritarian regimes alike. Access Now and the #KeepItOn coalition have recorded at least 1,118 shutdowns in about 76 countries worldwide since 2016. The coalition has documented at least 146 incidents of shutdowns in 37 countries in Africa between January 2016 and June 2023, as seen in chart 1 below. Over the years, the shutdowns are lasting longer, affecting more people and spreading across Africa.

Chart 1: Number of shutdowns in Africa from January 2016 to - June 2023



The region has also seen the weaponisation of internet shutdowns during the conflict in Ethiopia and Sudan. Africa has also seen the highest number of nationwide shutdowns affecting an entire country or more than one region at a time. Governments in Africa are also increasingly imposing mobile internet shutdowns and service-based shutdowns. Normalising the use of mobile internet shutdowns in particular could become dangerous for human rights. It is crucial to note that most people in Africa still rely on mobile devices to access the internet and only a handful can afford fixed cable connections which are usually spared by governments in some cases. Thus, the impact of mobile internet shutdown is huge.

Incidents of Shutdowns Documented in Africa from January 2016 to June 2023

Ethiopia is the leading perpetrator of internet shutdowns in Africa with at least 26 incidents of shutdowns followed by Sudan and Algeria with 15 and 13 shutdowns respectively, as shown in Chart 2 below. Other countries like Uganda and Chad had seven and six incidents respectively. Authorities in Cameroon, the Democratic Republic of Congo, Mali, and Mauritania, among others, have also imposed shutdowns on some occasions. Across Africa, internet shutdowns are ordered during major national events including elections, protests, and conflicts. Governments in the region have shut down the internet 59 times during protests, 25 times during elections, 11 incidents during conflict and six shutdowns in times of military coups. Other triggers of shutdowns include school exams and terrorism claims.

17
18

19
20

Impact of Shutdowns on Internet Freedom in Africa

Internet shutdowns violate human rights, widen the digital divide and enable those in power to evade accountability for human rights violations. Shutdowns also endanger people's lives during crises and cost national economies billions of dollars. In 2022, the UN Office of the High Commissioner for Human Rights (OHCHR) issued its first dedicated report on internet shutdowns, Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights, shining a spotlight on the devastating impact the disruptions have on human lives.[21] The report underscored that shutdowns directly counter efforts to close digital divides and the promise of the accelerated economic and social development that universal connectivity would bring, thus threatening the realisation of the Sustainable Development Goals.[22]

Internet Shutdowns Harm Elections and Democratic Tenets

The internet and digital communication tools have enhanced the rights to access to information, freedom of opinion, expression and assembly. They also enable people to actively participate in democratic processes like elections, scrutinise policies put forward by political candidates and provide opportunities for people to hold those in power to account.

25 of the 146 shutdowns imposed since 2016 by African governments have been during elections. Elections, particularly in growing democracies, are a critical time of transition and active citizen participation in the process contributes significantly to credible democratic outcomes. Shutdowns also make it extremely difficult for journalists, human rights defenders, election observers, and other key players to effectively monitor and report on electoral processes. Denying internet access to these actors hinders their ability to participate in and scrutinise the electoral processes and brings to question the credibility of election outcomes. According to a 2019 study by CIPESA, governments who want to hold on to power are likely to impose shutdowns at times that favour them most.[23]

Case Study: Uganda A Repeat Offender of Election-Related Shutdowns in Africa

Uganda is known for flipping the kill switch whenever the country is going to the polls. As early as 2011, the government of Uganda shut down access to social media platforms during elections.[24] Similarly, in 2016 and 2021, authorities in Uganda shut down the internet during elections and other key national events while cracking down on opposition politicians offline. On the eve of elections in January 2021, the Uganda Communication Commission (UCC) ordered ISPs across the country to completely shut down internet access and social media applications citing "'national security concerns".[25] Although the government ended the shutdown after about five days, as of September 2023 it has refused to unblock access to Facebook.

Internet Shutdowns in Times of Protests, Political Turmoil and Conflict

Another trigger of internet shutdowns in Africa are turbulent moments such as protests, political turmoils and conflicts. Authorities tend to shut down access to the internet and electronic communications when access to information is critical in order to control the flow of information. Internet shutdowns silence dissent and quell protests. Since 2016, there have been at least 59 shutdowns documented during protests, 11 during conflict and six during military coups across Africa. The governments of Sudan, Ethiopia, Guinea, Mauritania, Eswatini, Niger, Chad, Somaliland, Sudan, Senegal and Zimbabwe have imposed shutdowns during these key national moments.

21 *Internet shutdowns: UN report details 'dramatic' impact on people's lives and human rights https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human*

22 *The Sustainable Development Goals Report 2023: Special Edition https://unstats.un.org/sdgs/report/2023/*

23 *Despots and Disruptions: Five Dimensions of Internet Shutdowns in Africa https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/*

24 *Uganda shuts down social media; candidates arrested on election day https://edition.cnn.com/2016/02/18/world/uganda-election-social-media-shutdown/index.html*

25 *Uganda Eases Internet Shutdown Imposed Over Election https://www.capitalfm.co.ke/news/2021/01/uganda-eases-internet-shutdown-imposed-over-election/*

The internet and digital platforms have facilitated dissent and provided an avenue for people to mobilise and coordinate during protests. In times of conflict, lack of information can be a matter of life and death as people struggle to find safe routes and gather information about the whereabouts of their loved ones.[26] Shutdowns during conflict worsen the delivery of humanitarian and emergency aid to affected populations while access to healthcare, education and businesses is heavily hit.

Case Studies: Lead Perpetrators of Shutdowns in Africa During High Tension Moments

In Ethiopia, a majority of the 26 incidents of shutdowns imposed by authorities since 2016 are usually to crack down on protests or in response to communal violence or conflict. Ethiopia is also known to have imposed one of the longest internet shutdowns during an active conflict in Africa.[27] When conflict broke out between the government and the Tigray People's Liberation Front in November 2020, the internet and other communications platforms were shut down for over two years. The blackout enabled warring parties to commit human rights abuses including mass rape, mass murder, and violent abuse against civilian populations and refugees with impunity.

Additionally, since August 2023, authorities blocked internet access in the Amhara region following clashes between local ethnic militia and federal security forces.[28] Earlier in April 2023, the region had been cut off as violent protests erupted in several parts of the region against the federal government's decision to disintegrate regional special forces.[29] In February 2023, when the leadership of the Ethiopian Orthodox Church called for protests, the government imposed a nationwide social media blackout lasting over five months.[30]

In Sudan, authorities, mainly the military junta, have imposed at least 15 shutdowns since 2016 – mostly to quell protests and most recently during the armed conflict. When fighting between the Sudanese Armed Forces (SAF) and Rapid Support Forces (RSF) began to escalate in April 2023, access to the internet was disrupted[31] on April 16 for about 10 hours as well as on April 23.[32] The military regime that ousted Omar Al Bashir three years ago has weaponised shutdowns to squash protests. In October 2021, the junta shut down both mobile and fixed cable connections throughout the country for 25 days. According to reports, at least 17 people were reportedly killed and over 250 injured during the shutdown as a result of police brutalities. On June 3, 2019, the Transitional Military Council (TMC) shut down the internet for over a month, blocked foreign media and instituted a brutal crackdown on protesters, resulting in over 100 deaths, over 700 injuries, and at least 70 raped people by the notorious Janjaweed militia.

Other countries including Senegal,[33] Mauritania, [34] Eswatini[35] and Guinea have also imposed internet shutdowns during protests and unrest. In July and June 2023, the government of Senegal cut access to social media apps and mobile internet services in the country following unrest.[36] The government justified the shutdown claiming it was "necessary to prevent" the spread of "hateful and subversive" messages online.[37]

26 *Stranded, suffocated, and in pain: 15 stories from Tigray's internet siege https://www.accessnow.org/15-stories-from-tigrays-internet-siege/*
27 *After years in the dark, Tigray is slowly coming back online https://www.accessnow.org/tigray-shutdown-slowly-coming-back-online/*
28 *Ethiopia's Amhara region requests federal help over militia unrest https://www.reuters.com/world/africa/mobile-internet-outages-ethiopias-amhara-amid-fighting-residents-say-2023-08-03*
29 *Gun battles erupt in Ethiopia as PM axes Amhara region's security force https://www.theguardian.com/global-development/2023/apr/12/gun-battles-erupt-in-ethiopia-as-pm-axes-amhara-regions-security-force*
30 *Ethiopia restores social media access after five months https://t.ly/rGUWf*
31 *Sudanese telecoms provider MTN blocks internet services, MTN officials say https://www.reuters.com/article/sudan-politics-internet/sudanese-telecoms-provider-mtn-blocks-internet-services-mtn-officials-say-idINS8N35N0D8*
32 *Cloudflare Radar https://twitter.com/CloudflareRadar/status/1648054950159605762*
33 *Stop the internet shutdowns: Senegal authorities must end censorship https://www.accessnow.org/press-release/internet-shutdowns-senegal/*
34 *Mauritania: Protests and clashes possible in areas across country through at least early June following recent death of individual in police custody https://crisis24.garda.com/alerts/2023/05/mauritania-protests-and-clashes-possible-in-areas-across-country-through-at-least-early-june-following-recent-death-of-individual-in-police-custody*
35 *#KeepItOn: Eswatini authorities shut down internet to quell protests, ask people to email grievances https://www.accessnow.org/press-release/keepiton-eswatini-protests/*
36 *Senegal government cuts mobile internet access amid deadly rioting https://www.reuters.com/world/africa/senegal-government-cuts-mobile-internet-access-amid-deadly-rioting-2023-06-04/*
37 *#FreeSenegal: 'Our people are literally suffering!' due to intermittent internet shutdowns https://technext24.com/2023/06/05/internet-shutdown-in-senegal/*

Reflections on the Future: All Hope is Not Lost

Best Practices: Keeping It On In Africa

Despite the spread of internet shutdowns and their growing threat to internet freedom in Africa, it is important to highlight some key successes and best practices in the fight against shutdowns. According to Access Now's STOP database, 37 out of Africa's 54 nations have imposed internet shutdowns meaning 17 countries in the region have not done so. Ghana and Kenya are among the countries that have publicly committed to not imposing internet shutdowns during critical national events like elections. In 2023, Nigeria and Sierra Leone lived up to their commitments to keep internet access on throughout elections in February and June respectively. Ahead of the general elections in June 2023, the government of Sierra Leone committed to keeping internet access on during a closed meeting with stakeholders. In February 2023, authorities in Nigeria responded to public pressure[38] by assuring the people of Nigeria that internet access would not be disrupted.[39] Similar public commitments were also documented in Kenya during the 2022 elections.[40] Other countries, like Benin and The Gambia, which have disrupted internet access in the past, kept it on during elections in 2021.

Civil society actors and other stakeholders continue to play a crucial role in holding authorities accountable. Through the #KeepItOn Election Watch – a campaign that seeks to push back against election-related shutdowns globally - the #KeepItOn coalition has mobilised various stakeholders to prepare, prevent and respond to shutdowns during elections.[41] The #KeepItOn coalition has engaged with governments, private companies, internet service providers, Big Tech and other actors through open letters, joint statements and stakeholders' dialogues as well as capacity-building training across countries to ensure unfettered access to the internet during elections. The coalition has provided training on shutdowns for journalists, civil society activists, election observers and individuals to prepare and equip them with relevant resources like circumvention and digital safety tools to bypass shutdowns.

Another important milestone worth mentioning is that Africa has recorded several successes in public interest litigation against internet shutdowns at both national and regional levels. On July 14, 2022, the Community Court of Justice of the Economic Community of West African States (ECOWAS Court), declared the seven-month Twitter blocking in Nigeria unlawful and incongruent with the African Charter on Human and People's Rights as well as the UN Charter.[42] Earlier in June 2020, The ECOWAS Court made a similar finding against the government of Togo following a lawsuit by civil society actors, journalists and individuals after the government shut down the internet to quell protests in September 2017.[43]

In Zambia, litigation by Chapter One Foundation (Ltd), a civil society group successfully ended an internet shutdown ordered by the Zambia Information and Communication Authority (ZICTA) during the August 2021 elections. Subsequently, in March 2022, the High Court of Zambia adopted a consent judgement in which ZICTA agreed "not to act outside its legal authority to interrupt access to the internet in future" and to give the public a 36-hour prior notice and reason for any disruption to internet access.[44]

38 *#KeepItOn in Nigeria: social media, internet must stay connected during elections https://www.accessnow.org/press-release/keepiton-nigeria-elections/*

39 *Nigerian Communications Commission Says No Network Shutdown During General Elections https://saharareporters.com/2023/02/24/nigerian-communications-commission-says-no-network-shutdown-during-general-elections*

40 *Matiang'i: Kenya will not shut down internet during 2022 elections https://nairobinews.nation.africa/matiangi-kenya-will-not-shut-down-internet-during-2022-elections/*

41 *2023 Elections and Internet Shutdowns Watch https://www.accessnow.org/campaign/2023-elections-and-internet-shutdowns-watch/#Pakistan*

42 *ECOWAS Court victory: Twitter ban in Nigeria declared unlawful https://t.ly/JYrRF*

43 *ECOWAS Court upholds digital rights, rules 2017 internet shutdowns in Togo illegal https://www.accessnow.org/press-release/internet-shutdowns-in-togo-illegal/*

44 *Chapter One Foundation v. Zambian Information and Communications Technology Authority https://globalfreedomofexpression.columbia.edu/cases/chapter-one-foundation-v-zambian-information-and-communications-technology-authority/*

Similarly, courts in Sudan have issued several judgements ending shutdowns and upholding people's rights. In 2021, the Sudanese Consumer Protection Organisation and others sued Internet Service Providers (ISPs) and telecom companies operating in Sudan for breach of contractual agreements after they implemented a shutdown ordered by the military.[45] The general court of Khartoum ordered the ISPs to restore internet services to the complainants and subsequently to all subscribers. In response, the Sudanese Telecommunication and Postal Regulatory Authority (TPRA) rejected the court ruling and ordered ISPs to continue the shutdown. However, the court rejected the TPRA's directive and issued an arrest warrant for the CEOs of the ISPs.[46] As a result, the internet was partially restored with some restrictions on social media sites.[47] A similar legal battle was noted following the June 2019 internet shutdown by the military junta.[48]

While the legal successes in some African countries have not prevented shutdowns from recurring, these court rulings serve as precedents for activists and other stakeholders to explore in pushing back against internet shutdowns.

Looking Forward, Recommendations for Governments and Stakeholders

Africa is still on the route to digitalisation yet it is also one of the continents with widespread incidents of shutdowns. Such acts contradict the goals of regional initiatives such as the African Union's Digital Transformation Strategy for Africa which seeks to ensure that every individual, business and government in the region is digitally connected or enabled by 2030.[49] Regional and subregional bodies including the African Union, ECOWAS, Southern African Development Community (SADC) and the East African Community (EAC) must also adopt mechanisms against internet shutdowns as well as concrete measures to bolster digital economic growth in Africa.

Moreover, ISPs, Big Tech companies, tech industry players and private entities should push back against government-mandated internet shutdowns in their countries of operation. New market entrants must take the necessary due diligence to ensure that contracts for licences do not require them to normalise shutting down the internet or infringing on human rights online at governments' request. Companies must also undertake periodic human rights impact assessments to improve upon the delivery of services while centering human rights throughout their operations.

Civil society actors must continue to prioritise monitoring, documentation and advocacy against shutdowns. The #KeepItOn coalition must continue to mobilise people and communities impacted by shutdowns and closely engage with relevant policy-makers to bring an end to shutdowns. Through lobbying, leveraging mechanisms like the Universal Periodic Review (UPR), and spaces like the Internet Governance Forum (IGF), in-person stakeholder dialogues and capacity-building workshops, members of the coalition should continue to highlight the threats and dangers these shutdowns pose. Civil society must also begin to push for more stringent international laws and frameworks that could potentially make it difficult for governments to arbitrarily shut down the internet.

Moreover, the fight against internet shutdowns requires strong collaborations, collective efforts and action-oriented commitment from all stakeholders. To effectively advocate against shutdowns, stakeholders must move away from just denouncing perpetrators of internet shutdowns to taking concrete steps including strategic litigation and demanding firm commitments in practice from governments to protect and promote internet freedom.

Felicia Anthonio is the #KeepItOn Campaign Manager at Access Now. She is also co-author of a number of publications on internet shutdowns and a host of The Kill Switch podcast.

45 *Sudan court orders end to internet shutdown https://www.aljazeera.com/news/2021/11/9/calls-for-strike-and-civil-disobedience-in-sud*
46 *SMEX https://twitter.com/SMEX/status/1459086911931363329?s=20*
47 *Internet connection restored in Sudan https://www.africanews.com/2021/11/18/internet-connection-restored-in-sudan/*
48 *Sudan court orders company to end military-ordered internet blackout: lawyer https://www.reuters.com/article/us-sudan-politics-internet-idUSKCN1TO0FV*
49 *Digital Transformation Strategy for Africa https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf*

Social Media & Content Regulation

Introduction

The early forms of social media platforms emerged in the 1980s and 90s as discussion boards, online forums, email and chat rooms.[50] However, these platforms were limited to the elite few who had access to the internet. As internet connectivity spread across the continent, from the mid-2000s, mainstream social media platforms such as Meta (Facebook), X (Twitter), YouTube and more recently TikTok have gained popularity. The mobile revolution has further reinforced this adoption. The early 2010s saw increased adoption of smartphones, the expansion of internet infrastructure and cheaper internet access.[51]

Today, social media is significant given its utility as a platform for the realisation of rights to freedom of expression, association, assembly and democratic participation. It has become a useful avenue for cultural expression, creativity, entertainment, communication and connectivity across diverse communities. Many people today earn a living from multimedia content shared on social media platforms either as content creators, influencers or businesses. Social media has also become a new digital public square where human rights activists, the political opposition, government officials and the public can engage, mobilise and debate on critical issues affecting our society.[52]

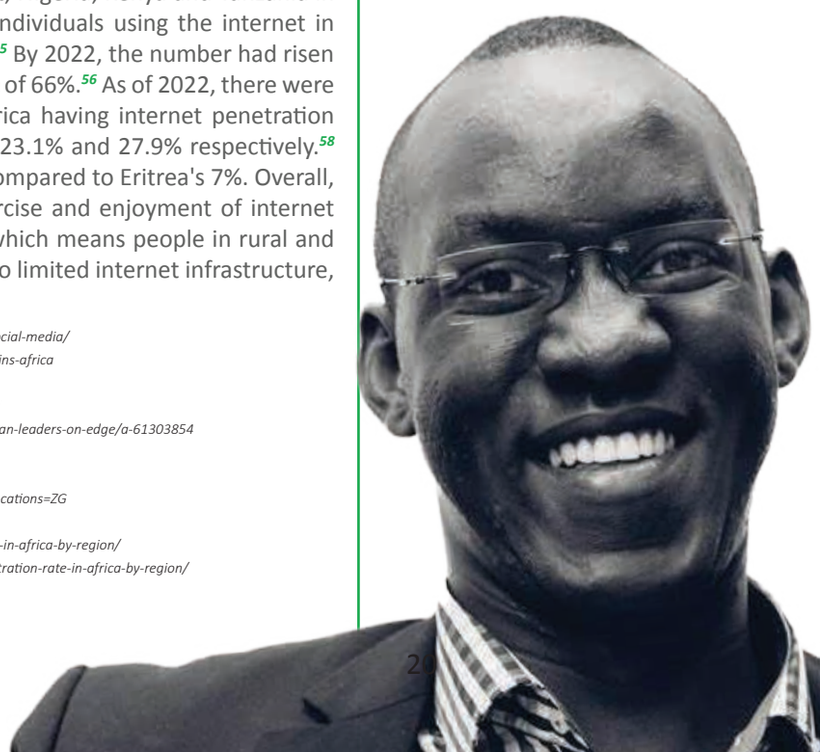
It is this last use that was exemplified in the Arab Spring that has remained of concern to some governments across the continent, whose officials are intolerant of criticism and demands for accountability by the public. As a result, such governments have in the past decade implemented various legislative measures to prohibit, punish, curtail and censor information online. According to SurfShark, Africa is the most restricted region in the world, accounting for 53% of all global cases of social media restrictions implemented in 2021.[53] The main platforms targeted include websites and social media platforms such as WhatsApp, Facebook Messenger, Facebook, X (Twitter) and Instagram. Unfortunately, these restrictions are becoming a popular measure by authoritarian regimes to control public discourse, access to information and expression online; disrupt online association and assembly; and restrict political participation in democratic processes such as elections and protests.

Victor Kapiyo

Overview of the Trends in Africa

Increasing connectivity to the internet

Internet use across the continent has been on a steady rise, growing four-fold between 2011 and 2021. In 2000, there were 4.5 million internet users in Africa, with South Africa, Egypt, Nigeria, Kenya and Tanzania in the top five countries.[54] According to the World Bank, the percentage of individuals using the internet in Sub-Saharan Africa rose from 1% in 2000 to 6% in 2010, and to 36% in 2021.[55] By 2022, the number had risen to 40% (566 million users) across Africa, which is still below the global average of 66%.[56] As of 2022, there were significant variances across the continent, with Northern and Southern Africa having internet penetration rates of 66% and 71% respectively,[57] while East and Central Africa stood at 23.1% and 27.9% respectively.[58] Among the countries, Morocco recorded an internet penetration of 84.1%, compared to Eritrea's 7%. Overall, the increased access to the internet has had a profound effect on the exercise and enjoyment of internet freedom. Yet these figures show that a significant digital divide still exists, which means people in rural and marginalised areas including informal settlements remain unconnected due to limited internet infrastructure, high cost of digital devices and low digital skills.



50 *The Evolution of Social Media: How Did It Begin, and Where Could It Go Next? https://online.maryville.edu/blog/evolution-social-media/*
51 *A social media boom begins in Africa https://www.un.org/africarenewal/magazine/december-2010/social-media-boom-begins-africa*
52 *Digital technologies and the new public square: Revitalising democracy? https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-09/digital_technologies_and_the_new_public_square.pdf*
53 *Increased social media use puts African leaders on edge https://corporate.dw.com/en/increased-social-media-use-puts-african-leaders-on-edge/a-61303854*
54 *How Africa achieved the world's highest growth in Internet users between 2000 and 2017 https://enitiate.solutions/africa-experienced-the-highest-growth-in-internet-users-between-2000-and-2017/*
55 *Individuals using the Internet (% of population) - Sub-Saharan Africa https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZG*
56 *Internet use https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-internet-use/*
57 *Social media penetration in Africa in 2023, by region https://www.statista.com/statistics/1190628/social-media-penetration-in-africa-by-region/*
58 *Internet penetration rate in Africa as of January 2023, by region https://www.statista.com/statistics/1176668/internet-penetration-rate-in-africa-by-region/*

Increasing use of social media

Social media use has also been on the rise in the past decade. People across the continent are using social media platforms to build communities where they can express themselves, share information, communicate, collaborate, advocate, participate in democratic processes and engage in economic activities. In 2022, there were at least 384 million social media users in Africa,[59] with Facebook leading in market share with 271 million users, followed by WhatsApp (200 million),[60] YouTube (180 million) and Twitter/X (24 million). TikTok is also growing in popularity with a reach of 28 million users in North Africa alone in 2022.[61] The highest social media usage as of January 2023 was recorded in Northern and Southern Africa with 49% and 41.3% of the population respectively using social media. The lowest rate was recorded in Central Africa with only 7% of the population using social media, which is also the lowest regional share globally. These user bases are expected to grow in the next five years as more people get connected online, digital devices become more readily accessible and populations become more tech-savvy.

Use of repressive laws to silence dissent

In a number of countries, repressive laws have been widely used to stifle internet freedom during critical events and in particular to target, threaten, arrest and detain bloggers, journalists, whistle-blowers and critics of the government in various countries. Of concern, has been the use of cybercrime, insult, hate speech, criminal defamation, false news and COVID-19 laws to muzzle free speech.[62] Some of these actions have been in response to legitimate concerns regarding problematic user behaviour or conduct on social media platforms. However, their enforcement in practice has not always targeted criminal elements on social media but people expressing their opinions online. For example, criminal defamation laws have been used to target people in Botswana, Kenya, The Gambia, and Uganda; while false news and cybercrime laws with punitive sanctions have been deployed in the Democratic Republic of Congo (DRC), Ethiopia, Kenya, Nigeria, Tanzania and Zimbabwe to achieve the same effect.

Likewise, during the COVID-19 pandemic, countries such as Algeria, Burkina Faso, Côte d'Ivoire, Cameroon, Egypt, Ethiopia, Kenya, Morocco, Niger, Nigeria, Senegal, South Africa, Tanzania, Zambia and Zimbabwe introduced new or enforced existing laws with repressive provisions to curtail freedom of expression regarding the Corona virus or government actions around the pandemic.[63] Whereas some of these laws have been reviewed or repealed, those that are in force remain potent threats to internet freedom and can be arbitrarily applied to muzzle speech.

Blocking of access to the internet and social media platforms

Africa has in the past decade witnessed rising internet shutdowns and restrictions to social media access across various countries. According to the #KeepItOnCampaign, 146 internet shutdowns were documented in 37 (68.5%) of African countries[64] Ethiopia, Sudan, Algeria, Chad, DRC and Uganda account for 50% of all the shutdowns implemented between 2016 and 2023. Blocking of social media access is becoming more sophisticated and has been more rampant in authoritarian regimes with long-serving presidents, during times of protests, elections and national examinations.[65] Blocking has also been implemented in retaliation for content moderation as was the case in Nigeria which suspended Twitter in June 2021 for deleting a post made from the president's account.[66] These restrictions continue and are aided by various laws, with at least 30 countries having a law that can facilitate the implementation of an internet shutdown. Often, laws developed to safeguard national security, and prevent terrorism, cyber crimes, hate speech and fake news have been deployed to enforce internet shutdowns and social media restrictions.

59 *Social media in Africa - statistics & facts https://www.statista.com/topics/9922/social-media-in-africa/?#topicOverview*

60 *Africa's WhatsApp economy is on the rise https://it-online.co.za/2023/03/02/africas-whatsapp-economy-is-on-the-rise/#:~:text=We%20live%20in%20a%20WhatsApp,plug%20into%20the%20global%20economy.*

61 *Potential advertising reach of TikTok in Africa as of 2022, by region https://www.statista.com/statistics/1323769/tiktok-potential-advertising-reach-in-africa-by-region/*

62 *Mapping Trends in Government Internet Controls, 1999 - 2019, State of Internet Freedom in Africa Report, CIPESA, https://cipesa.org/wp-content/files/State-of-Internet-Freedom-in-Africa-2019.pdf*

63 *Resetting Digital Rights Amidst the COVID-19 Fallout, State of Internet Freedom in Africa Report, CIPESA, https://cipesa.org/wp-content/files/briefs/report/State-of-Internet-Freedom-in-Africa-2020.pdf*

64 *#KeepitOn Stop Data https://docs.google.com/spreadsheets/d/1DvPAuHNLp5BXGb0nnZDGNoilwEeu2ogdXEIDvT4Hyfk/edit#gid=111443934*

65 *Study on Internet Shutdowns in Africa, https://aira.africa/wp-content/uploads/2022/04/STUDY-ON-INTERNET-SHUTDOWNS-IN-AFRICA-2021.pdf*

66 *Inside Nigeria's decision to ban Twitter https://restofworld.org/2021/inside-nigerias-decision-to-ban-twitter/*

Rise of disinformation, hate and harmful content

Disinformation has become increasingly widespread and sophisticated in several countries across the continent, driven by several factors. Social media platforms have become the primary vehicle for spreading disinformation, hate, extremist views, and propaganda which has in some cases led or fuelled polarisation, conflict and violence, given the ease of use, the wide audiences and the gaps in content moderation in the region. The ability to use targeted advertisements, manipulated digital content,[67] armies of paid influencers and communication firms[68] and the contribution of media houses[69] has amplified the magnitude and sophistication of the disinformation industry. These continue given the lack of access to credible and factual information, gaps in content moderation practices, weak oversight of platforms, and low levels of digital and media literacy affecting the ability of social media users to fact-check information and use social media responsibly.

Investigations in DRC, Ethiopia, Kenya, Sudan and Uganda show the main sponsors of disinformation campaigns are the African diaspora, politicians, political parties and governments seeking to influence public opinion and sway political discourse.[70] Pro-Russia entities are reported to be leading purveyors with disinformation campaigns reported in 16 countries in Africa.[71] In the past decade, the continent has witnessed widespread disinformation, especially around the COVID-19 pandemic, politics and national elections such as, in Senegal, Kenya and Zimbabwe, and on social issues and conflict such as in DRC and Ethiopia. In several countries, for instance, Kenya and Ethiopia,[72] civil society and media organisations have faced coordinated smear campaigns through hashtags geared towards tarnishing their reputations for doing their work. Likewise, individual journalists and fact-checkers have faced online bullying, including being labelled as traitors leading some to flee Ethiopia. In addition, TikTok has been used to fuel harassment and incite violence against LGBTQ+ individuals.[73]

Progressive Jurisprudence from Regional Courts and Mechanisms

In the past decade, there have been landmark decisions from national and regional courts that have significantly advanced internet freedom in the continent by setting standards that are cascaded to the national level. In 2013, the African Court on Human and Peoples' Rights (African Court) faulted Burkina Faso over its defamation laws that were found to be in violation of the African Charter on Human and Peoples' Rights (ACHPR), the International Covenant on Civil and Political Rights ICCPR), and the Economic Community of West African States (ECOWAS) treaty.[74] Similarly, the East African Court of Justice (EACJ) in 2016 found numerous provisions of Tanzania's Media Services Act in violation of the Treaty for the Establishment of the East African Community.[75] In 2021, the Community Court of Justice of the ECOWAS ruled that the Nigerian government, by suspending the operation of Twitter, had violated Article 9 of the ACHPR and Article 19 of the ICCPR.[76] A similar finding was made by the court against Togo for implementing an internet shutdown during protests in September 2017, with the court stating that access to the internet was a "derivative right" as it enhanced the exercise of freedom of expression.[77]

The ACHPR adopted the Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019 which establishes or affirms the principles for anchoring the rights to freedom of expression and access to information in Africa.[78] In its judicial capacity, it held in 2021, that Rwanda's criminal defamation laws are not compatible with Article 9 of the Charter since they restrict journalists' freedom of expression and the public's right to access valuable information.[79] The Commission has also adopted resolutions affirming that "the same rights that people have offline must also be protected online".[80] In the same vein, the Special Rapporteur on Freedom of Expression and Access to Information in Africa has also condemned internet and social media shutdowns on the continent for violating the ACHPR.[81]

67 *Robot wars: How to build a bot to subvert elections https://disinfo.africa/robot-wars-how-to-build-a-bot-to-subvert-elections-9f739411aa39*

68 *Inside the Shadowy World of disinformation for Hire in Kenya https://assets.mofoprod.net/network/documents/Report_Inside_the_shadowy_world_of_disinformation_for_hire_in_Kenya_5._hcc.pdf*

69 *South African newsroom uses fake journalist to spread disinformation https://disinfo.africa/south-african-media-outlet-uses-fake-journalist-to-spread-disinformation-67cccae8aa9f; State of Kenya's Media in 2020 https://africacenter.org/spotlight/mapping-disinformation-in-africa/ https://mediacouncil.or.ke/sites/default/files/downloads/State%20of%20Kenya%27s%20Media%202022%20Report.pdf*

70 *Domestic Disinformation on the Rise in Africa https://africacenter.org/spotlight/domestic-disinformation-on-the-rise-in-africa/*

71 *Mapping Disinformation in Africa https://disinfo.africa/smear-campaign-target-journalists-and-fact-checkers-covering-the-ethiopia-tigray-war-346121c1b8e5*

72 *Journalists covering Ethiopia-Tigray war targeted https://disinfo.africa/smear-campaign-target-journalists-and-fact-checkers-covering-the-ethiopia-tigray-war-346121c1b8e5*

73 *TikTok fuels LGBTQ+ harassment in Ethiopia https://disinfo.africa/tiktoks-role-in-fuelling-lgbtq-harassment-and-violence-in-ethiopia-6d74698575d5*

74 *Lohé Issa Konaté v. The Republic of Burkina Faso https://globalfreedomofexpression.columbia.edu/cases/lohe-issa-konate-v-the-republic-of-burkina-faso/*

75 *Media Council of Tanzania v. Attorney General https://globalfreedomofexpression.columbia.edu/cases/media-council-of-tanzania-v-attorney-general/#:~:text=The%20Court%20found%20that%20the,on%20Human%20and%20Peoples'%20Rights.*

76 *SERAP v. Federal Republic of Nigeria https://globalfreedomofexpression.columbia.edu/cases/serap-v-federal-republic-of-nigeria/*

77 *Amnesty International Togo and Ors v. The Togolese Republic https://globalfreedomofexpression.columbia.edu/cases/amnesty-international-togo-and-ors-v-the-togolese-republic/*

78 *Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019 https://achpr.au.int/en/node/902*

79 *Agnes Uwimana-Nkusi v. Rwanda https://globalfreedomofexpression.columbia.edu/cases/agnes-uwimana-nkusi-v-rwanda/*

80 *Resolution ACHPR/Res.362 (LIX) 2016 on the Right to Freedom of Information and Expression on the Internet in Africa, adopted during the 59th Ordinary Session, held from 21 October to 04 November 2016 http://www.oas.org/en/sla/dil/docs/acceso_informacion_desarrollos_UA_ACHPR-Res_362_LIX_2016.pdf*

81 *Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africahttps://achpr.au.int/en/news/press-releases/2019-01-29/press-release-special-rapporteur-freedom-expression-and-access-0*

Impact on Internet Freedom in Africa

The use of laws, policies and practices to restrict access to the Internet and social media goes against international human rights standards, which are well established in regional and international instruments, and domesticated in national constitutions across several countries. The restrictions curtail digital rights, but also the ability of people to freely assemble, associate and participate in democratic processes. In many African countries, the restrictions are arbitrary, unwarranted, excessive, discriminatory and implemented with limited transparency to serve political or other purposes. Also, they do not satisfy the three-part cumulative test under international human rights law, which requires that any restriction to freedom of expression must be provided by law, pursue a legitimate purpose, and be proven as a necessary and least restrictive means to achieve the purported aim. Perpetuating such practices also embeds impunity in governance and if sustained, could render the rule of law and good governance meaningless.

By restricting access to the internet and social media, states are directly interfering with not only civil and political rights but also economic, social and cultural rights. States have an obligation to respect, protect and remedy the violation of these rights within their jurisdictions. These restrictions often target bloggers, civil society, journalists, human rights defenders, online activists, the political opposition and the wider citizenry, and serve to restrict civic space. Whereas governments often justify the restrictions as necessary to maintain public order, and national security or to prevent the spread of hate speech and disinformation, this is not usually the case. Overall, the effect of these measures is the restriction of the free flow of information, undermining democracy and electoral processes, covering up human rights violations and consequently denying the public opportunities to exercise their democratic rights and participate in governance. They also threaten investor confidence and harm the business environment, by denying access to essential services or discouraging transactions that are increasingly reliant on the internet and social media.

In the coming years, the regulation of content on social media platforms and efforts to hold companies accountable for human rights violations that occur on their platforms will be important. There are documented risks regarding the structural conception of social media platforms, whose business models and algorithms mostly prioritise profit and content based on engagement value rather than its accuracy or truth.[82] Whereas platforms are making attempts to regularise their content policies and standards, there are various ongoing efforts that are aimed at developing regulatory solutions at the national, regional and global levels. These include the development of Guidelines for Regulating Digital Platforms,[83] multistakeholder oversight efforts such as those under UNESCO's Social Media 4 Peace Project,[84] and regional laws such as the European Union's Digital Services Act. As African governments consider regulating digital platforms, it will be critical for them to learn from existing models and consider regulatory approaches that are relevant to the context in this region. More importantly, multi-stakeholder engagement will be critical, as well as the delineation of the roles of the various actors, mainstreaming of international human rights standards, ensuring independent oversight, and entrenching due diligence practices by companies.

Reflections on the future of internet freedom

The ongoing conflicts across the continent, coupled with recent coup d'etat in several countries, have provided fertile ground for increased hate and disinformation online. These conflicts are driven by ideological and political differences among leaders, corruption, poor governance and the resource curse. They have also been exacerbated by famine arising from climate change effects, food shortages due to the Ukraine-Russia conflict, and the economic hardships in the aftermath of the COVID-19 pandemic, leaving individuals and nations in distress. The continuation of these multiple crises could fuel increased conflict, hate and disinformation online. Therefore, averting their potential consequences and addressing the root causes of conflict should be prioritised.

82 *Disinformation and freedom of opinion and expression https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/085/64/PDF/G2108564.pdf?OpenElement*
Safeguarding freedom of expression and access to information: guidelines for a multistakeholder approach in the context of regulating digital platforms

83 *https://unesdoc.unesco.org/ark:/48223/pf0000384031.locale=en*

84 *Social media 4peace: taking stock of progress achieved, project activities & visibility https://unesdoc.unesco.org/ark:/48223/pf0000383696*

However, the increasing discontentment with leadership across various countries means that the affected governments are likely to increase their attempts to control information on digital platforms and repress opponents. As has been witnessed before, as activists, government critics and opponents ramp up disapproval of governments, autocratic incumbents have strengthened their stranglehold on power and are increasingly asserting themselves on digital platforms and could thus turn social media into a conflict zone or digital battlefield.

Therefore, courts and legislative bodies at the national and regional levels have an important role to play in preventing the escalation of restrictions on internet freedom including abolishing problematic laws and outlawing repressive practices. As the excesses of national executives increase, these two critical arms of government which are already battling for their independence in some countries, should seize the opportunity to escape executive capture and defend and protect human rights online in the face of emerging threats to internet freedom in Africa.

In addition, UNESCO's Guidelines for Regulating Digital Platforms which are still under development, provide a useful standard which if adopted, could provide guidance for states in the development of regulation of social media platforms. They also provide guidance for platforms in the implementation of content moderation processes in ways that safeguard freedom of expression, access to information and other human rights.[85] It is crucial that these guidelines gain wide acceptance and adoption in the face of growing technological changes such as artificial intelligence, increased use of the internet and social media platforms, and new legislative proposals targeting digital platforms across several countries.

Lastly, if the internet and social media are to remain the digital public square, then the role of multi-stakeholders will be of the utmost importance. All stakeholders have a role to play and a responsibility to safeguard human rights online. It will therefore be critical to expand internet infrastructure, lower the cost of digital devices and internet connectivity and enhance digital and media literacy across the continent to ensure citizens can utilise the power of the internet and social media to better their lives. Over and above the technological aspects, it is equally crucial for states to address the underlying social, political, cultural and economic challenges across the continent in order to reap the full dividends of technology.

Potential Solutions/strategies

- Governments should amend, review and abolish laws that permit internet disruptions, and enact laws that are in line with international human rights standards.
- Governments should provide an enabling environment for internet use, including by investing universal service funds towards promoting internet access and lowering barriers to internet connectivity.
- National and regional human rights institutions should invest more in investigating cases relating to digital rights violations and take steps to hold states and companies accountable.
- Civil society should monitor, report and push back against laws, policies and practices which could adversely affect digital rights such as internet disruptions.
- Civil society should partner with government, business, media and the tech community to build capacity and deepen public awareness of media and information literacy and digital rights.
- Civil society should pursue strategic Public Interest Litigation to challenge laws, policies and practices that perpetuate internet disruptions and information controls.
- Social media companies should invest more resources in content moderation, and effective redress mechanisms and provide more statistics and disaggregated data regarding social media use and harmful content targeting African users.
- Telecoms and internet services providers should invest more in internet infrastructure and promote access to affordable digital devices.

Victor is a human rights lawyer and Researcher at CIPESA. He is also a Trustee of the Kenya ICT Action Network (KICTANet).

85 *Safeguarding freedom of expression and access to information: guidelines for a multistakeholder approach in the context of regulating digital platforms https://unesdoc.unesco.org/ark:/48223/pf0000384031.locale=en*

Enhancing Digitisation and Data Governance in Africa

Introduction

Over the last decade, digitisation in Africa has increased, with many countries adopting digital technologies to improve service delivery and enhance public participation. Digital technologies are now critical to the enjoyment of rights and the improvement of livelihoods in Africa. Many African governments have embarked on rapid data collection and digitisation initiatives – e-government services, digital identity (digital ID), biometric voters' cards, driver's licences, and SIM card registration. However, there are several counter steps that weaken the potential of digital technologies to catalyse free expression and civic participation or to drive innovation.

Africa's digital journey is characterised by the adoption of various data collection programmes, many of which are implemented under weak and questionable legal frameworks that compromise the protection of personal data by facilitating surveillance.[86] Other concerns about digital rights include personal data breaches, increased surveillance, and the proliferation of laws and regulations that undermine technology's potential to promote political and socio-economic development. They also hinder the citizen's readiness to apply these transformative technologies in a meaningful way.

According to a 2018 report by the United Nations High Commissioner for Human Rights (UNHCR), the mere generation and collection of data relating to a person's identity, family or life already affect the right to privacy, as through those steps an individual loses some control over information that puts their privacy at risk.[87] While state surveillance is often justified as necessary for strengthening national security and public order, fighting terrorism and cybercrime, different African governments are increasingly using it to enhance their political control by targeting and spying on critical and dissenting voices including activists, human rights defenders, journalists, and political actors.[88]

Enhanced Data Collection Programs

Several countries have taken steps to strengthen their data collection programmes, by enacting legislation that requires the compulsory collection of a wide variety of personal data for purposes of registering SIM cards, voter registration, and the issuance of national digital identity cards, driving licences and birth or death certificates. They have also embarked on the acquisition of technologies that facilitate the collection of biometric data such as installation of CCTV cameras in major cities.[89] These laws enacted provide for the collection of fingerprints, photos and signatures before official documents such as IDs and passports are issued. Laws in countries like Kenya, Nigeria and Zambia also mandate the collection of iris scans.[90] In many countries, telecommunications companies are required by law to carry out mandatory registration of subscribers' SIM cards. Applicants must provide proof of identity such as a valid residence permit, national ID, biographical and biometric data and in some cases, the International Mobile Identity (IMEI) of their device.

Paul Kimumwe

86 *Defined as the monitoring, interception, collection, storage, and retention of information transmitted, transmitted, or created to a recipient group over communicati networks by a third party*

87 *Right to Privacy https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx#:~:text=Even%20the%20mere%20generation%20and,%2 2C%20para.*

88 *State of Internet Freedom in Africa 2022 https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_2022.pdf*

89 *State of Internet Freedom in Africa 2022 https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_2022.pdf*

90 *Ibid*

For example, article 6 of Regulation No. 2015/3759 on the identification of subscribers in Cameroon obliges the subscriber of a telecommunications SIM card to present an original national identity card, a valid residence permit of a foreigner, or another document that replaces it, as well as the exact address, including a location map. Kenya's Information and Communications Act (Registration of SIM cards) Regulations, 2015 under rule 4 requires all mobile network providers to register all SIM card subscribers. In Mozambique, the Regulation for the Registration and Activation of Mobile Subscriber Identification Modules Decree of 2015 requires all communications operators to register all SIM cards with data such as name and address of customers. In Rwanda, licensed operators are required under article 4 of the 2017 Regulation Governing SIM card registrations to register all subscribers and SIM card holders.

Several reasons have been advanced for implementing these biometric data collection programmes, including the creation of central databases such as those in Cameroon[91] and Kenya,[92] as including, promoting national security, identifying, stabilising, and effectively managing identity information. Other reasons given include strengthening a country's digital transformation efforts, eliminating identity theft, fraud and falsification of official documents, and improving tax collection.

Several countries have also adopted the use of Biometric Registration and Biometric Verification (BVVS) systems with the aim of ensuring voter equality and protecting the integrity of the electoral process. While biometrics have raised expectations of election integrity, they have not averted electoral fraud with many reported cases of vote manipulations, leading to accusations and counteraccusations among political contestants.[93]

Weak Legislative Framework

Unfortunately, many of the initiatives are not anchored on robust laws. They therefore fall short of water-tight safeguards, including independent oversight bodies, that would safeguard data rights and promote data protection rights and principles. In countries where the laws are present, they are weak, fragmented, outdated, poorly enforced, and do not provide strong and independent oversight mechanisms for data privacy protection or effective remedies, yet governments have intensified the deployment of data collection technologies such as CCTV with automated facial recognition technology.[94] These laws tend to facilitate access to data without adequate safeguards. Laws such as Personal Data Protection Law No. 18-07 of 2018 of Algeria, Data Protection Law of 2019 in Kenya, Angola Data Protection Law of 2011, Ivory Coast Data Protection Act of 2013 and the Uganda Privacy and Data Protection Act 2019 provide circumstances in which personal data, including sensitive information, may be processed.

In most of the countries where SIM card registration is mandatory, there is concern that service providers may be compelled under existing communication interception laws to aid state surveillance activities by providing information about subscribers to state security agents. The assistance rendered by intermediaries is used to facilitate internet disruptions, access to users' data with ease, content removals, decryption of users' data, and state surveillance.[95]

In addition, many governments lack proper procedures or safeguards for the sharing of data between state institutions or with third parties such as banks and telecom companies. In Tanzania, the data-sharing agreements between the National Identification Authority (NIDA) and other agencies are not disclosed to the public. Similarly, in Senegal, the lack of transparency around the unified biometric card used as a national identity card and a voter's card has fuelled speculation over possible abuse by politicians to target voters in specific areas. It is not uncommon to read reports of cases where flawed laws are used to ease access to the personal data of individuals to identify and target them. The main categories of targeted individuals include human rights defenders, political activists, dissidents, and government opposition actors.[96]

91 *10 Questions to understand the biometric redesign of electoral rolls in Cameroon https://www.camerlex.com/10-questions-pour-comprendre-la-refonte-biometrique-des-listes-electorales-au-cameroun-12559/*

92 *Benefits https://www.hudumanamba.go.ke/benefits/*

93 *The productive failures of biometric voting in Africa https://democracyinafrica.org/the-productive-failures-of-biometric-voting-in-africa/*

94 *CIPESA (2022) State of Internet Freedom in Africa https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_2022.pdf*

95 *Compelled Service Provider Assistance for State Surveillance in Africa: Challenges and Policy Options https://cipesa.org/2023/04/compelled-service-provider-assistance-for-state-surveillance-in-africa-challenges-and-policy-options/*

96 *CIPESA (2022) State of Internet Freedom in Africa https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_2022.pdf*

Limited Transparency by governments

Despite the intrusive nature of biometric data collection, there has been a notable lack of transparency and public awareness, engagement, and consultations about the objectives, applications, design, and implementation of biometric data collection programmes in many countries. Particularly, issues of data protection principles, data subjects' rights, and risk for data misuse are rarely emphasised in nations where public campaigns were conducted, such as Ghana, Kenya, and Uganda. Instead of putting the emphasis on public involvement and consultation, which are essential to the success of such projects, governments appear to have been in a rush to establish biometric data-gathering programmes and celebrate registration statistics.

In several countries, including Angola, Kenya, Liberia, Nigeria, Mozambique, Tanzania, and Zambia, research shows that there has been limited public discussion of the concerns surrounding personal data gathering programmes, their aims, and any associated hazards.[97] Due to this and the power disparity between states and data subjects, the public is forced to provide biometric data without their knowledge or informed consent or due to fear of not being able to obtain essential services or official documents like passports, national identity cards, voter identification cards, or driver's licences.

Across the continent, biometric data registration programmes are contingent on an individual's possession of the most basic forms of official identification, such as national identity cards, birth certificates, and driver's licences. In addition, several programmes are not universally implemented particularly in rural areas leaving many citizens non-registered. And because possession of the IDs has become a prerequisite for service delivery, there have been reports of citizens being denied access to basic services such as adult suffrage, financial services, work, education, health, social services, travel, registering a company, SIM card ownership, and subsequently internet access if they lack such documents.[98] In addition, the appetite for public participation has been dulled for many citizens because there is a high perception of surveillance and mistrust of government-initiated (digital) programmes.

Increased Data Localisation Legislation

Several African countries have also adopted data localisation policies that require local storage of data and forbid unauthorised cross-border data transfers. The countries have specified the conditions for authorising transfer, mostly where the data subject has offered consent and where an adequate level of protection is assured in the recipient country or international organisations.[99] These include Algeria (article 44 of data protection law, article 10 of the Post and Electronic Communications Regulatory Authority [ARPCE] directive on cloud computing, and the 2018 law on e-commerce); Gabon (article 94 of the Law No. 001/2011 on the protection of personal data); Niger (article 24 of the data protection law); Morocco (articles 43 and 44 of the law No. 09-08 on Processing of Personal Data, 2009); Angola (article 34 of the data protection law); Benin (article 391 of the Benin Digital Code); Burkina Faso (article 42 of the law No. 001-2021 / AN); and Cape Verde (article 19 of the Data Protection Act).

96 *Global Report Biometrics and Digital Identity: Trend Analysis and Comparative Assessment https://internews.org/wp-content/uploads/2023/09/Global-BDI-Trend-Analysis-Geographical-Assessment-Final-Approval-06.09.2023.pdf; Towards the Evaluation of*

97 *Socio-Digital ID Ecosystems in Africa https://researchictafrica.net/wp/wp-content/uploads/2021/11/Comparative-Report_5.11.21-2.pdf*

98 *Global Report Biometrics and Digital Identity: Trend Analysis and Comparative Assessment https://internews.org/wp-content/uploads/2023/09/Global-BDI-Trend-Analysis-Geographical-Assessment-Final-Approval-06.09.2023.pdf; Towards the Evaluation of Socio-Digital ID Ecosystems in Africa https://researchictafrica.net/wp/wp-content/uploads/2021/11/Comparative-Report_5.11.21-2.pdf*

99 *Mapping and Analysis of Privacy Laws and Policies in Africa https://cipesa.org/wp-content/files/reports/Mapping-and-Analysis-of-Privacy-Laws-and-Policies-in-Africa.pdf*

There are divergent views on the need and the benefits of data localisation, with advocates often arguing that data localisation is critical in safeguarding national security, promoting the local digital economy, and ensuring adequate data security and users' privacy. On the other hand, critics have opined that hosting data locally could grant state surveillance apparatus easier access to data for surveillance purposes, as they would not need to go through foreign countries or intermediaries' data management protocols to access this data.[100] There are also fears that the localisation of privacy of personal data may be used as an excuse to withhold public sector data that could be made open for citizens to advocate for better public services, hold governments accountable and tackle public sector corruption. However, there is limited evidence of how various countries have implemented their legal provisions on data localisation. And as with other barriers to full implementation of other laws, data protection bodies established by national data protection laws are fairly young, ill-resourced and oftentimes not operational. In others, there is limited evidence as to how - if at all - they enforce the legal provisions relating to data localisation.[101]

Reflections for the Future

There is no doubt that digitisation including the collection and processing of personal data is a crucial aspect in development, particularly how the database once consolidated can be used in various ways to facilitate service delivery through applications in areas such as digital identification and verification, voter registration and identification. In Africa however, concerns remain about privacy and data protection, as many of the current government data collection programmes are being implemented using weak and fragmented policy frameworks, limited dispute resolution mechanisms and inadequate safeguards and remedies for privacy violations. Indeed, as discussed, various reports show that the extensive amount of personal data collected under the SIM card registration by itself has enabled governments to identify and track a vast number of citizens with ease, and yet, several governments are steadily pushing to link such data to the national ID and voters' registration databases, as well as to various other government databases for services delivery.

To benefit from the digitisation dividends, countries must undertake deliberate efforts to ensure that the adoption of any data collection programmes is inclusive and empowering; as well as respect for digital rights, including the rights to privacy and personal data protection, access to information, non-discrimination, and free expression.

- *More specifically, governments should work towards reviewing and or enacting robust data governance frameworks to harness the benefits of data through multi-stakeholder efforts informed by evidence-based research.*
- *In addition, governments should undertake capacity-building programmes for their officials particularly those responsible for biometric data collection programmes, including data protection bodies, law enforcement, prosecution, regulators, and the Judiciary in effective data protection.*
- *Civil society and social justice actors should work together with other stakeholders including the government, private sector, technical community, media and the public to promote understanding of biometrics such as through awareness raising and capacity building of key players on privacy and data protection.*

Paul Kimumwe is a Senior Programme Officer - Research and Advocacy at CIPESA with expertise in media, communications and research.

100 *How Surveillance, Collection of Biometric Data and Limitation of Encryption are Undermining Privacy Rights in Africa, https://cipesa.org/2021/07/how-surveillance-collection-of-biometric-data-and-limitation-of-encryption-are-undermining-privacy-rights-in-africa-2/*

101 *Which way for data localization in Africa? https://cipesa.org/wp-content/files/briefs/Which_Way_for_Data_Localisation_in_Africa___Brief.pdf*

Online Activism and Civic Space in Africa in the Age of the Privatised Internet

Introduction

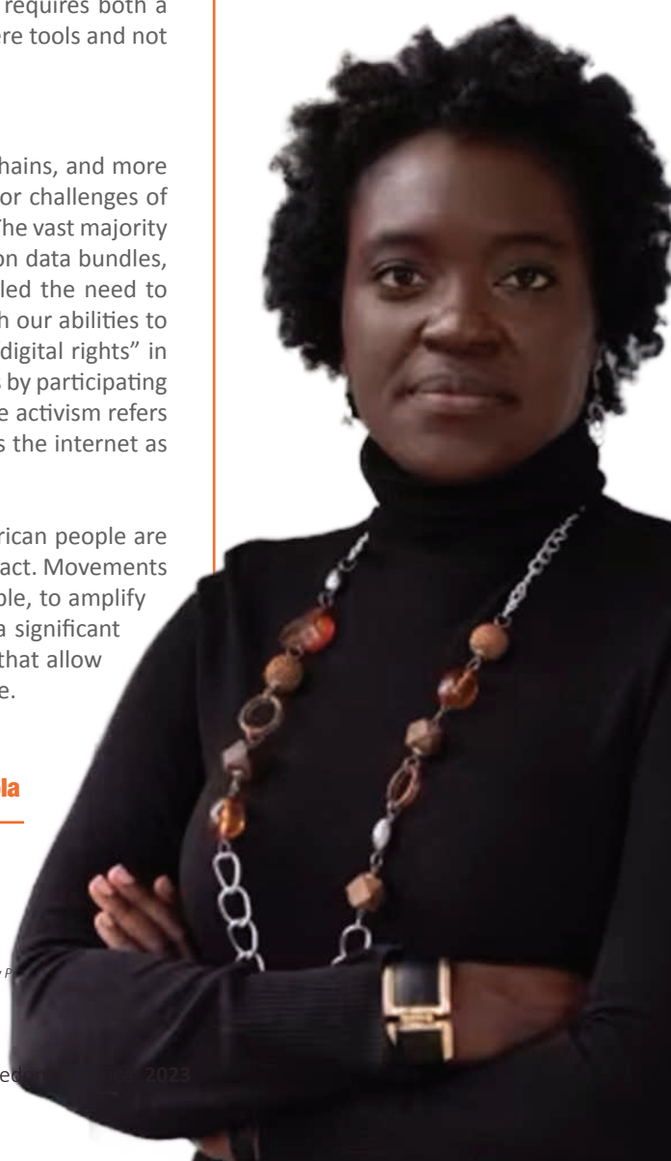
The idea of civic space is often cited in politics, even while there is arguably no consensus on what it means. The Office of the United Nations High Commissioner for Human Rights (OHCHR) defines civic space as the environment that makes it possible for people and groups to contribute towards the governance of their societies and to participate in the social and economic life of their communities.[102] Civic space could be a physical space, that is, any place that allows individuals and groups to gather to participate in the governance processes, like underneath an acacia tree within a village, or at a public protest site. But more often than not, when we say "civic space," we are referring to the conditions that enable this participation or the rights, duties, and liberties that are afforded to the individual or the group within a community to participate in the governance or shaping of their society.

From the moment the internet became more freely accessible to the general public, it has been utilised by people to create and protect civic space. Whichever way you define it, Africans are using the internet and digital technologies to expand the civic space. The internet contributes to activism; that is, people can and do use the internet in support or in the pursuit of actions to increase or protect the civic space as part of their activism. The work conducted online can also be a form of activism in itself, depending on the objectives at hand.[103] In instances where raising awareness is the main goal for activism, the use of digital technologies to amplify messages can constitute a complete activist action. But in cases where the cause requires both a message and tangible action, activists must view the internet and digital technologies as mere tools and not an end in themselves.[104]

Africans Online

Across Africa, the rise of digital technologies like social media, mailing lists, text message chains, and more have become integral to the processes of advocacy and organising. This is despite the major challenges of connectivity, including limitations on infrastructure and the high cost of digital connectivity. The vast majority of Africans online are connecting through their mobile phones and are dependent mostly on data bundles, and sometimes zero-rated websites, for their internet experiences. This has similarly fuelled the need to understand and promote a whole new set of rights, duties, and liberties that pertain to both our abilities to access the internet and to use the internet to organise our political lives. The concept of "digital rights" in 2023 includes both the rights to access and use the internet, as well as the rights a person has by participating online, including freedoms of expression, association, and opinion.[105] This means that online activism refers both to the ability of people to advocate for various issues online and to the right to access the internet as well.

Despite the challenges of lack of infrastructure and the high cost of digital connectivity, African people are using the internet to advance and protect the civic space within their societies to varying impact. Movements like #EndSars[106] and #RhodesMustFall[107] have made effective use of social media, for example, to amplify their calls for accountability and social change. Today, digital technologies are integral to a significant portion of political action across the continent, conducted on or through online platforms that allow people to circumvent the legal or political restrictions on their participation in the civic space.



Nanjala Nyabola

102 *OHCHR. 'OHCHR and Protecting and Expanding Civic Space'. Accessed 2 August 2023. https://www.ohchr.org/en/civic-space*
103 *Nyabola, Nanjala. Digital Democracy, Analogue Politics: How the Internet Era Is Transforming Kenya. London: ZED, 2018.*
104 *Nyabola, Nanjala. Digital Democracy, Analogue Politics: How the Internet Era Is Transforming Kenya. London: ZED, 2018.*
105 *Dragu, Tiberiu, and Yonatan Lupu. "Digital authoritarianism and the future of human rights." International Organization 75, no. 4 (2021): 991-1017.*
106 *Uwazuruike, Allwell Raphael. "# EndSARS: the movement against police brutality in Nigeria." Harvard Human Rights Journal (2020).*
107 *Kwoba, Brian, Roseanne Chantiluke, and Athinangamso Nkopo, eds. Rhodes must fall: The struggle to decolonise the racist heart of empire. Bloomsbury P*

At the same time, there has been significant backlash against these developments from governments threatened by a highly organised and active public sphere. Civic space around the world is under threat from rising authoritarianism, and Africa is not exempt from these trends. Groups challenging civic space in defence of xenophobia, racism, misogyny, and other social ills are on the rise across the world, including in Africa. African social media is as gendered as in other parts of the world, and wherever feminist counter-publics have mobilised to protest violence against women, some young men have equally organised and mobilised along misogynist lines.[108] Overall, while online activism remains a crucial part of the activist's toolkit in Africa, Africa is not abstract to the rest of the world, as there have been enough significant transformations in the global context to reshape the opportunities and challenges that face African online activists as well.

Against the Odds

Can online activism and civic space thrive on an internet that is increasingly held by the interests of private capital? This is arguably the main question that faces activists who depend on these platforms to conduct their political action. Between 2013 and 2023, many African social movements turned to social media as a way of amplifying their causes in the context of a repressed public sphere. X (Twitter) has been by far the most popular site for such organising, favoured by movements like #LuchaRDC,[109] #BalaiCitoyen[110] #MyDressMyChoice and more. For African activists facing some of the world's highest costs of connectivity, the relatively low barriers to entry and a critical mass of public-facing communication made Twitter an attractive choice, even if rival Meta managed to have its flagship product, Facebook, zero-rated in many countries through its Facebook Free Basics programme. This ease of access also makes it possible for movements of transnational solidarity to work together on specific campaigns and to build in-person networks like #Africtivistes from that.

Under its previous management, X (Twitter) made concerted efforts to deepen its foothold on the continent by opening an African office and liaising directly with social movements on the continent. But 2022 was a reminder that the dramatic expansion in our concepts of digital rights and online activism occurs alongside an inflexion point for digital technologies more broadly. After Twitter was acquired by Elon Musk in October 2022 there was a raft of changes in the way its platform operates, who it presumes its target audience is, and, indeed, where the company viewed its future. Many of the guarantees that digital rights advocates had organised for on the site, including the creation of dedicated regional offices and a Trust and Safety team that oversaw the protection of the digital rights of users, were quickly overturned.[111]

Experts noted a significant increase in hate speech across the platform after the Musk acquisition, presumably because many of the checks and balances against such speech were eliminated, turning the platform into yet another unmoderated haven for misinformation, extremism, and hate.[112] The Twitter Africa team was fired,[113] the Trust and Safety Council dissolved[114] and only a small core group of policy workers in the organisation left focused on three major markets – the US, the EU, and India.

108 *Trott, Verity Anne. "'Gillette: The best a beta can get': Networking hegemonic masculinity in the digital sphere." New Media & Society 24, no. 6 (2022): 1417-1434; Okech, Awino. "Feminist digital counterpublics: Challenging femicide in Kenya and South Africa." Signs: Journal of Women in Culture and Society 46, no. 4 (2021): 1013-1033.*

109 *Cirhigiri, Christian. "Youth on the Frontlines: Preventing Human Rights Abuses in Violent Contexts, A Case Study of LUCHA in the DR of Congo." International Journal of Transitional Justice 16, no. 1 (2022): 133-150*

110 *Touré, Ibrahima. "Jeunesse, mobilisations sociales et citoyenneté en Afrique de l'Ouest: étude comparée des mouvements de contestation «Y'en a marre» au Sénégal et «Balai citoyen» au Burkina Faso." Africa Development 42, no. 2 (2017): 57-82*

111 *Dang, Sheila. 'Twitter Dissolves Trust and Safety Council'. Reuters, 13 December 2022, sec. Technology. https://www.reuters.com/technology/twitter-dissolves-trust-safety-council-2022-12-13/*

112 *Benton, Bond, Jin-A. Choi, Yi Luo, and Keith Green. "Hate speech spikes on twitter after elon musk acquires the platform." School of Communication and Media, Montclair State University (2022).*

113 *Madowo, Larry. 'Twitter Africa Employees Accuse Elon Musk of Discrimination over Severance Terms | CNN Business'. CNN, 21 November 2022. https://www.cnn.com/2022/11/21/tech/twitter-africa-elon-musk-intl-lgs/index.html*

114 *Dang, Sheila. 'Twitter Dissolves Trust and Safety Council'. Reuters, 13 December 2022, sec. Technology. https://www.reuters.com/technology/twitter-dissolves-trust-safety-council-2022-12-13/*

Today's social networking platforms are primarily data companies that provide social networking services as a side concern. Individuals and groups conducting their activism online may not immediately appreciate that their participation in these platforms contributes to their popularity and, therefore, financial viability. While in the past, this fuelled a more symbiotic relationship between the platforms and the users, 2022 heralded a transformation in which the profit motive became more explicit than ever before. At the beginning of 2023, all the major social networking sites announced major layoffs that severely affected the units charged with monitoring and responding to hate speech, a broader trend within the industry.[115] Musk has already announced that Twitter would be scraping user data to build his own AI platform to compete with Open AI and other platforms.[116] This means that when an online activist is sharing a photograph of a group of women at a protest or creating a tweet thread about an incident, they are not merely communicating that information to the public: they are also training an algorithm and increasingly proprietary Artificial Intelligence software. African activists enter into an extractive relationship with technology companies when they increase the popularity of privately owned platforms by contributing to their reputation as sites for civic space.

Indeed, depending on privately held sites to advance civic action is a precarious proposition. Whereas the early days of the internet were characterised by a multiplicity of spaces where people could build community, in 2022, the internet is dominated and shaped by the interests of a handful of private companies that operate platforms primarily for profit. The cost of keeping users safe on these sites has grown significantly because of the sheer number of users. In order to protect their bottom line, several of these companies conducted mass layoffs in the latter half of 2022 even while user numbers continue to grow. In addition to Twitter, Meta, Alphabet, and ByteDance – the parent companies of Facebook, Google, and TikTok, respectively – all announced significant staff cuts targeting critical teams such as their Trust and Safety and regional teams as part of broad-ranging redundancies in their respective companies.[117]

African regional offices were particularly hard-hit by these developments as they were already small offices catering to a variety of interests in the second-largest continent in the world. There were already significant complaints that the platforms were systematically under-investing in language and content moderation on the continent. This was brought to the fore during the outbreak of war in the Tigray region of Ethiopia amid criticisms of Facebook's response to hate speech on the platform.[118] For those using online platforms to conduct their activism, the shifts in the social media landscape mean extra concerns about whether or not the platforms can or will keep them and their data safe. Some of the threats are increasingly from the platforms themselves, including complying with data requests from governments in order to remain active in those countries. Outside the United States, analysts argue that they have witnessed an alarming increase in speech that amounts to hate speech on Twitter. [119]

Governments around the world have struggled to properly respond to online activism. The rapid transformation in the social media space in 2022 underscored how dangerous it is for regulators to lack dynamism in this space. Regulations on the digital civic space passed by several African governments historically focus on taxation and attempts to censor or altogether block social media instead of protecting the rights of people to use the internet during times of political transformation. One notable outlier was Zambia. In March 2022, the Zambian High Court adopted a consent judgement that compelled the Zambian Information and Communications Technology Authority (ZICTA) to avoid internet shutdowns over all platforms under their control and to inform the public within 36 hours of any disruptions of the reason for that interruption.[120] This judgement effectively prohibits ZICTA from conducting an internet shutdown except in cases where it can provide a written explanation within 36 hours of bringing the measures into effect.

115 *Google, Meta, Amazon and other tech companies have laid off more than 104,000 employees in the last year https://www.cnbc.com/2023/01/18/tech-layoffs-microsoft-amazon-meta-others-have-cut-more-than-60000.html*

116 *Dang, Sheila, Krystal Hu, and Krystal Hu. 'Elon Musk Says XAI Will Examine Universe, Work with Twitter and Tesla'. Reuters, 14 July 2023, sec. Technology. https://www.reuters.com/technology/elon-musk-says-xai-will-use-public-tweets-ai-model-training-2023-07-14/*

117 *Vanian, Hayden Field, Jonathan. 'Tech Layoffs Ravage the Teams That Fight Online Misinformation and Hate Speech'. CNBC, 26 May 2023. https://www.cnbc.com/2023/05/26/tech-companies-are-laying-off-their-ethics-and-safety-teams-.html*

118 *Wong, David, and Luciano Floridi. "Meta's Oversight Board: A Review and Critical Assessment." Minds and Machines (2022): 1-24.*

119 *Benton, Bond, Jin-A. Choi, Yi Luo, and Keith Green. "Hate speech spikes on twitter after Elon Musk acquires the platform." School of Communication and Media, Montclair State University (2022).*

120 *Chapter One Foundation v. Zambian Information and Communications Technology Authority https://globalfreedomofexpression.columbia.edu/cases/chapter-one-foundation-v-zambian-information-and-communications-technology-authority/*

Looking Ahead

What is the future of African online activism and civic space within this shifting landscape? The challenges to online activism and the civic space persist. As stated, some of these challenges arise from the digital authoritarianism practices including the level of government information controls, the state of democracy, the use of legislation to limit freedom of speech and expression online, and the implementation of internet shutdowns. Internet shutdowns in Africa peaked in 2019, but while in 2022 there were fewer internet shutdowns across the continent than in 2021, there were still nine overall, including the second year of the internet blackout in Ethiopia's Tigray region.[121]

Uganda's election-related disruption continued from 2021 into 2022, with a specific shutdown of Meta's platform Facebook continuing throughout the year. Similarly, the Zimbabwean government implemented an election-related shutdown to chill coverage of the opposition party's main rally in September 2022. These are also connected to the challenge of private capital because the acquiescence and collaboration of internet service providers and mobile telephony companies are often required in order to make shutdowns work.

Despite all these challenges, African online activism remained dynamic and powerful throughout 2022. Sudanese people defied an internet shutdown in 2020 to use the internet to maintain the visibility of the civic resistance to military rule in the nation, despite signs from the international diplomatic community that the military regime would be normalised.[122] In Libya and Tunisia, African refugees and migrants used social media and platforms like Telegram and Signal to raise awareness over missing boats in the Mediterranean Sea while appealing for assistance for those who were stranded in dangerous detention camps across North Africa. Nigerians, Tanzanians, and Ugandans continued to challenge the social media bans and throttling in their respective countries. Movements calling for social change and accountability in countries across the continent continued to use digital technologies to advance their campaigns.

African entrepreneurship also responded to the challenge of dependence on foreign-owned platforms that do not reflect the social and political interests of African users. Cameroonian-founded Dikalo is a social networking site built through a coalition of funders and developers from across the continent that faces the continent first.[123] Launched in 2016, the site saw a dramatic increase in users around the time of the Musk acquisition of Twitter and continues to grow as the latter sails deeper into choppy water. Dikalo promises that its site is community-facing first, openly embracing a values-led, incremental approach to growth in the business model that Western-owned social networking sites have lately eschewed. The site remains privately held, in part reflecting the limited size of venture capital funding on the continent and the lack of information within user communities of alternatives to the dominant platforms. More importantly, for activists looking to use platforms to defend the civic space, the underlying challenge remains the same: privately owned spaces will always be imperfect substitutes for a truly public civic space because, at its extremes, the profit motive is at odds with the desire for the public good.

In a rapidly transforming global context, not least the rapid privatisation and fragmentation of the internet, African communities remain dynamic and creative, inviting African governments to do the same. The dream of an internet for the people, by the people, can only survive if all interested parties work together to focus on supporting the needs of African people first, rather than the corporations that profit from them or the institutions that act against them.

Nanjala Nyabola is a writer, political analyst, and activist and has writen extensively about African society and politics, technology, and international law.

121 *Access Now. 'Internet Shutdowns in Africa: Fewer Offenders in 2022, Still Causing Harm'. Accessed 2 August 2023. https://www.accessnow.org/press-release/keepiton-internet-shutdowns-2022-africa/*

122 *Eltahir, Nafisa, and Nafisa Eltahir. 'Sudan's Resistance Committees Take Centre Stage in Fight against Military Rule'. Reuters, 3 February 2022, sec. Africa. https://www.reuters.com/world/africa/sudans-resistance-committees-take-centre-stage-fight-against-military-rule-2022-02-02/*

123 *About Dikalo. 'About Dikalo'. Accessed 2 August 2023. https://about.dklo.co/*

Internet usage in Africa - statistics & f

Internet Freedom and New Forms of Censorship in Africa

Introduction

With 570 million internet users in 2022, Africa has witnessed rapid growth in online communication channels including social media, blogging, messaging applications and more.[124] From the early 2010s, the growth in internet and social media adoption was mainly via mobile phones.[125] These developments have fueled greater freedom of expression across the continent. While progress has been made, serious threats to free speech persist. These include actions by some African governments to suppress dissent through sophisticated methods of censorship, harassment, internet shutdowns and targeted online disinformation campaigns. In addition, the criminalisation of journalism and the imposition of social media taxes further imperilled open discourse.

However, the trajectory is not all bleak. The strengthening of democratic institutions and accountability mechanisms in many nations provides hope that all Africans may one day exercise their voice safely and freely. Overall, the history of internet freedom in Africa over the past 10 years is one of both progress and pushback. Although several challenges remain, the increasing integration of human rights into legal frameworks and the growth of independent media signal a promising future for internet freedom on the continent. With vigilance and collective action from civil society, governments, tech companies and citizens alike, the internet can fulfil its potential to give voice to the diverse people of Africa.

Overview of the Trends in Africa

Technological innovations like the spread of mobile broadband and Facebook's Express Wi-Fi have connected more Africans.[126] With over half a billion internet users now on the continent, these developments have provided unprecedented opportunities for accessing information, digital empowerment and economic participation. According to the International Telecommunication Union (ITU), internet use in Africa surged 23% between 2019 and 2021.[127] Kenya exemplifies this rapid growth, with internet users increasing from 13 million to 17 million during the period, largely due to the introduction of affordable smartphones and mobile data plans. Nigeria witnessed similar growth rising from 100 million to 120 million users, propelled by cheaper devices and connectivity, social media uptake, and increased reliance on digital services during the COVID-19 pandemic. As more Africans gain the means to make their voices heard online, the scope for free expression and open discourse expands.

Despite these positive trends, there are still challenges to internet freedom in Africa. Internet and media freedom has been deteriorating across Africa over the past decade as governments make explicit attempts to give preferential treatment to media outlets that give them positive coverage while silencing critical voices and divergent views. A growing number of African governments have introduced repressive laws targeting the online sphere[128] and adopted invasive technologies to monitor digital communication.[129] They have also sought to control the internet, through shutting it down or slowing it down, or simply removing content inconvenient to the ruling government.

Richard Ngamita

124 *Internet usage in Africa - statistics & facts https://www.statista.com/topics/9813/internet-usage-in-africa/#topicOverview*
The state of mobile internet connectivity in Sub-Saharan Africa: why addressing the barriers to mobile internet use matters now more than ever
125 *https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-internet-connectivity-in-sub-saharan-africa/*
Express Wi-Fi Technology Partner program: Getting more people online with fast and affordable Wi-Fi
126 *https://engineering.fb.com/2018/08/28/connectivity/express-wi-fi-certified-enabling-connections-that-matter/*
127 *Measuring digital development Facts and figures 2021 https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf*
128 *Data security and privacy laws develop across Africa https://www.bakermckenzie.com/en/newsroom/2022/04/data-security-and-privacy-laws-across-africa*
129 *Chinese firms are driving the rise of AI surveillance across Africa https://qz.com/africa/1711109/chinas-huawei-is-driving-ai-surveillance-tools-in-africa*

Likewise, the media in many African countries is tightly controlled through repressive legislation applied with impunity, arbitrary arrests, intimidation and harassment targeting journalists, bloggers and activists which makes it difficult for them to speak or report on issues such as corruption. In June 2018, the Nigerian Senate announced the introduction of a new bill to regulate social media use.[130] Prior to this, the country had made a series of attempts to regulate social media, including the adoption of the Cybercrime law. In Kenya,[131] the government introduced restrictive laws that implicate those who spread "false information" with a hefty fine and jail time, while others such as Uganda,[132] Malawi,[133] Rwanda[134] and Tanzania,[135] are employing vague computer misuse laws to arrest and prosecute government critics, on charges of “offensive communication” and cyber harassment.

According to the Committee to Protect Journalists (CPJ), 24 journalists were murdered between 2014 and 2020, while 165 journalists were imprisoned during the same period.[136] CPJ data shows that Algeria, Egypt and Angola have had 60, 12 and 10 journalists killed since 1994.[137] Entire media houses have been targeted in Uganda, Liberia, Guinea-Bissau, Burundi and Tanzania. The 2023 World Press Freedom Index showed a significant decline in press freedom in Africa, with the situation in nearly 40% of the countries being classified as “bad”.[138] Countries such as Algeria, Senegal, Tunisia, Burkina Faso, Cameroon and Eritrea, were cited for press violations.

Further, since 2015, internet shutdowns and disruptions have become more common in Africa, affecting approximately 25 countries on the continent.[139] These shutdowns have targeted entire countries in some cases, while in others they have focused on regions experiencing civic unrest and protests. Social media platforms like YouTube, Facebook and Twitter have been among the services disrupted, along with messaging apps like WhatsApp. Short Messaging Service (SMS) has also faced interruptions. One major shutdown occurred in Ethiopia in 2016 during the country's civil war, imposed by the government to control the flow of information about the conflict. [140] In 2018, Cameroonian authorities blocked access to social media and messaging apps for nearly four months in the Anglophone regions in an attempt to silence criticism of the government.[141] Cameroon saw at least two internet blackouts that year, with the government justifying them as necessary to curb the spread of hate speech and fake news by separatist groups in the Northwest and Southwest. Similar measures to disrupt internet and social media access have been witnessed in Uganda, Tanzania and Zimbabwe.

African governments have also invested in advanced surveillance tools and systems to monitor citizens online, including blocking anonymising tools. Investigations have revealed large-scale sales of sophisticated surveillance technology to African countries by Huawei, under the company's 'Safe City' program.[142] There are currently 12 Huawei 'Safe City' programs in Africa, including in Uganda, Kenya and South Africa. In 2019, Huawei faced allegations following a Wall Street Journal investigation that the company had assisted the Ugandan and Zambian regimes in tracking opposition politicians.[143] The growing surveillance capabilities across Africa threaten citizens' privacy and ability to freely express views online, especially for political dissidents.

23%

Surge in internet use in Africa between 2019 and 2021

130 *Nigerians raise alarm over controversial Social Media Bill https://www.aljazeera.com/news/2019/12/18/nigerians-raise-alarm-over-controversial-social-media-bill*
131 *Kenya's Crackdown On Fake News Raises Questions About Press Freedom https://www.npr.org/sections/thetwo-way/2018/05/19/612649393/kenyas-crackdown-on-fake-news-raises-questions-about-press-freedom*
132 *The Computer Misuse (Amendment) Act, 2022 https://chapterfouruganda.org/resources/acts-bills/computer-misuse-amendment-act-2022*
133 *Electronic Transactions and Cyber Security Act https://malawilii.org/akn/mw/act/2016/33/eng@2017-12-31*
134 *Rwanda: Vague laws used to criminalise criticism of government https://www.amnesty.org/en/latest/press-release/2010/08/18403/*
135 *The Cybercrimes Act, 2015 https://www.parliament.go.tz/polis/uploads/bills/acts/1452061463-ActNo-14-2015-Book-11-20.pdf*
136 *The Squeeze on African Media Freedom https://www.journalofdemocracy.org/articles/the-squeeze-on-african-media-freedom/*
137 *CPJ Data https://cpj.org/data/*
138 *2023 World Press Freedom Index – journalism threatened by fake content industry https://rsf.org/en/2023-world-press-freedom-index-journalism-threatened-fake-content-industry*
139 *These are the African countries that censor the internet the most https://qz.com/africa/2165371/these-are-the-african-countries-that-censor-internet-the-most*
140 *Ethiopia shuts down social media to keep from ‘distracting’ students*
141 *https://www.washingtonpost.com/news/worldviews/wp/2016/07/13/ethiopia-shuts-down-social-media-to-keep-from-distracting-students/*
142 *Cameroon goes offline after Anglophone revolt https://www.cnn.com/2017/02/03/africa/internet-shutdown-cameroon/index.html*
143 *Uganda's cash-strapped cops spend $126 million on CCTV from Huawei https://www.reuters.com/article/us-uganda-crime/ugandas-cash-strapped-cops-spend-126-million-on-cctv-from-huawei-idUSKCN1V50RF*
144 *Huawei Technicians Helped African Governments Spy on Political Opponents https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017*

For many users in Africa, online platforms have also turned into spaces for hate speech, brutal, prolific online harassment and abuse, including targeted attacks that make it difficult for citizens or journalists to report on important issues. Beatrice Mutetwa, a top human rights advocate in Zimbabwe who has represented many journalists and opposition figures, has been targeted and subjected to online intimidation and harassment[145] to the point where she has had to go off social media. She has been called names, labelled a terrorist, dark force, and regime change agent, and on several occasions threatened with death. This trend is a threat to democracy, as it undermines the ability of citizens to hold their governments accountable. Several internet users and journalists have received death threats online, especially in times of crisis or events like elections. These threats have at times translated into offline risks of physical violence,[146] thereby undermining their safety and independence, while also eroding their freedom of expression.

However, in recent years, there has been a growth of independent and pluralistic media outlets that push back against government repression and the culture of silence.[147] These outlets have played a key role in exposing corruption and holding the governments accountable. For example, in Ghana, there are at least 100 media outlets, [148] including radio stations, television channels, and websites. Many of these outlets are privately owned and reflect a high degree of pluralism and diversity. These outlets have a large following and have been praised for their investigative journalism and willingness to challenge the government.

Civil society organisations in Africa are also playing a more active role in promoting internet freedom. They are conducting research on the state of internet freedom in Africa,[149] training journalists to report on sensitive issues without fear of reprisal, and advocating for policy changes that would protect freedom of expression. For example, the Media Institute of Southern Africa (MISA)[150] conducts research on the state of media freedom in the region, provides training to journalists, and advocates for policy changes that would protect freedom of expression. There are now more active organisations focused on defending internet freedom and digital rights across Sub-Saharan Africa. Groups like Paradigm Initiative in Nigeria, CIPESA, and Digital Society of Zimbabwe are engaging in litigation, policy advocacy, and public awareness campaigns.

Meanwhile, the African Union (AU) has adopted key resolutions affirming freedom of expression as a fundamental human right across the continent. For example, the African Commission on Human and Peoples' Rights adopted a Resolution on the Safety of Journalists and the Issue of Impunity in 2008.[151] This landmark resolution condemned attacks on journalists and called on states to investigate and prosecute crimes against media workers. Through such measures, the AU has established important norms protecting free speech and press freedom.[152] However, implementation gaps remain a challenge. Continued advocacy is needed to ensure AU member states uphold these standards in practice, as seen in 2020 when the AU called on Zimbabwe to investigate abuses against journalists and hold perpetrators accountable. By turning resolutions into reality, the African Union can solidify internet and media freedom as a cornerstone of democracy.

145 *Judicial Harrassment of Human Rughts Lawyer Beatrice Mtetwa https://www.frontlinedefenders.org/en/case/judicial-harassment-human-rights-lawyer-beatrice-mtetwa*

146 *Lucy Kassa on the dangers journalists face for uncovering truths in war https://www.economist.com/by-invitation/2022/05/03/lucy-kassa-on-the-dangers-journalists-face-for-uncovering-truths-in-war*

147 *African media breaks 'culture of silence' https://www.un.org/africarenewal/magazine/august-2010/african-media-breaks-%E2%80%98culture-silence%E2%80%99-0*

148 *Ghana https://rsf.org/en/country/ghana*

149 *SIFA 2020: Resetting Digital Rights Amidst the COVID-19 Fallout https://cipesa.org/2020/09/report-the-state-of-internet-freedom-in-africa-2020/*

150 *MISA https://misa.org*

151 *Resolution on the Safety of Journalists and Media Practitioners in Africa - ACHPR/Res.185(XLIX)11 https://achpr.au.int/en/adopted-resolutions/185-resolution-safety-journalists-and-media-practitioners-africa-achp*

152 *Resolution on the Human Rights Situation in the Republic of Zimbabwe - ACHPR/Res. 443 (LXVI) 2020 https://achpr.au.int/en/adopted-resolutions/443-resolution-human-rights-situation-republic-zimbabwe-achprres*

Impact on Internet Freedom in Africa

There are new and emerging issues that threaten internet freedom in Africa. The rise of misinformation and computational propaganda, including the use of bots, algorithms and fake accounts to spread mis/disinformation, has undermined the quality of online information and has been used to manipulate public opinion. During the Nigerian election in 2023,[153] there was widespread sharing of political disinformation across social media platforms like Facebook, Twitter, and WhatsApp. Much of this disinformation was spread through coordinated inauthentic accounts and "political bots" designed to automatically disseminate content. The spread of fake news and disinformation is a major challenge to internet freedom in Africa. This is because many people in Africa still lack access to reliable sources of information, making them vulnerable to manipulation. Fake news and disinformation have been used to sow discord, undermine trust in institutions, and even incite violence.

There is also a rise of "digital authoritarianism" across the continent as some governments are embracing technologies like AI-enabled surveillance, facial recognition and big data analytics to monitor and control citizens. In Uganda, President Yoweri Museveni has consolidated his authoritarian rule in part through increased control and surveillance of digital technologies.[154] Ahead of the 2021 elections, the government deployed Chinese-made CCTV cameras with facial recognition technology across Kampala, imposed an internet blackout and shut down social media access to suppress political organising and dissent. The rise in "digital authoritarianism" is a threat to human rights in many African countries. In addition, African governments are increasingly monitoring and censoring online activity, in some cases using sophisticated surveillance technologies such as Pegasus and Circles.[155] This has had a chilling effect on freedom of expression and has made it difficult for citizens to access information and communicate with each other freely.

Case studies: Online Harassment as the "New Censorship"

Online harassment often includes attacks on an internet user or journalist's credibility, smear campaigns, identity-based attacks, and even threats of violence against them and their family and friends. The common tactics in this harassment include coordinated disinformation, cyberbullying, trolling, cyberstalking, defamation, doxxing, public shaming, impersonation, identity theft and hacking. Online harassment and targeting of marginalised groups have become a new mechanism to censor news content and for authoritarian governments to silence dissent. Online harassment poses a significant risk to the free flow of information, press freedom, and the democratic exchange of ideas. In Ghana, anti-LGBTQ disinformation[156] and hate speech spiked with proposed bills seeking to criminalise LGBTQ identities. LGBTQ Ghanaians face outings, threats, and abuse off and online.

The use of coordinated disinformation campaigns including the use of troll accounts to harass those critical of governments has been a major tactic employed by actors seeking to harass, intimidate and censor critical voices online in Africa. The non-consensual sharing of private information, known as doxxing, is another insidious harassment tactic. In June 2021, several suspicious hashtags like #KatibaMbichi emerged on Kenyan social media, spreading narratives aimed at discrediting anti-corruption activists associated with the Linda Katiba movement. An Investigation[157] revealed that these campaigns were driven by networks of fake accounts that manipulated algorithms to ensure certain hashtags trend.

153 *Nigeria election triggers deluge of 'fake news' on social media https://www.aljazeera.com/features/2023/2/15/nigeria-election-triggers-deluge-of-fake-news-on-social-media*
154 *Huawei Technicians Helped African Governments Spy on Political Opponents https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017*
155 *The Spread of Surveillance Technology in Africa Stirs Security Concerns https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/*
156 *Ghana: Discrimination, Violence against LGBT People https://www.hrw.org/news/2018/01/08/ghana-discrimination-violence-against-lgbt-people*
157 *Inside the Shadowy World of Disinformation for Hire in Kenya https://assets.mofoprod.net/network/documents/Report_Inside_the_shadowy_world_of_disinformation_for_hire_in_Kenya_5._hcc.pdf*

In May 2021, Ethiopian journalist Lucy Kassa faced a wave of online harassment after reporting on a 13-year-old victim of an incendiary weapon attack.[158] A pro-government Facebook account with 200,000 followers openly called for her arrest in a country where dozens of reporters have been detained.[159] For weeks, Kassa endured death threats, sexual harassment, and viral smear campaigns like #ShameOnLucy. These cases demonstrate how coordinated attacks disproportionately target those seeking accountability, utilising sock puppet accounts, doctored images, gaslighting, and dangerous incitement in attempts to silence dissent.

In March 2023, Al Jazeera released a documentary exposing corruption in Zimbabwe's mining industry titled "Gold Mafia - The Laundry Service."[160] Several journalists who reported on or commented on the film subsequently faced a wave of online harassment from suspected state-sponsored bots.[161] For example, the Twitter account "Tinoedza Zvimwe" (@Tinoedzazvimwe1),[162] believed to be run by Zimbabwean president's spokesperson George Charamba, tweeted threats and intimidation at reporters,[163] warning them not to discuss the "defamatory" documentary. This exemplifies how officials often hide behind anonymous accounts to coordinate sophisticated harassment campaigns in an effort to chill critical journalism and dissent.[164] However, despite these tactics that aim to silence them through digital means, journalists across Africa continue uncovering malfeasance in the public's interest.

In September 2021, 25-year-old Mirabelle Lingom was falsely accused by members of Cameroon's opposition PCRN party of appearing in a sex tape with journalist Paul Chouta.[165] Chouta had previously reported on government abuses and been jailed for "defamation." An anonymous Facebook user claimed to identify Lingom in the explicit video, doxxing her contact details. She endured waves of graphic online harassment, with trolls fabricating demeaning lies about her and Chouta. The bullying spread across Cameroonian social media for days. Shortly after, Lingom fell ill and passed away.

Reflections on Internet Freedom Over the Next 10 Years

The next decade shows promise for advancing internet freedom in Africa. In recent years, many countries enacted laws protecting free speech and media rights online, a trend that is expected to continue. Citizens will continue to recognise the importance of internet freedom for enabling open dialogue, access to information, and economic development, hence pushing back on any restrictions. Some governments will still impose internet shutdowns and social media blocks while citing security concerns, especially during elections and crises. Expanding surveillance technologies like facial recognition could also grow across the continent, enabling state monitoring and control if left unregulated. Still, as internet access rises, citizens will likely demand greater freedom of expression, pressuring governments to respect digital rights.

Also, Internet and mobile technology access will continue growing across Africa, providing economic and educational opportunities. However, struggles around censorship, surveillance and corporate or government control of the internet will persist. Governments may attempt to restrict online freedoms through controversial cybercrime and hate speech laws. Civil society advocates will need to keep pushing back against limitations and promote balanced regulatory approaches. More citizens may turn to encrypted apps and VPNs to evade state surveillance.

158 *Exclusive: Ethiopians suffer horrific burns in suspected white phosphorus attacks https://www.telegraph.co.uk/news/2021/05/23/exclusive-ethiopians-suffer-horrific-burns-suspected-white-phosphorus/*

159 *@timnitGebru@dair-community.social on Mastodon on X https://twitter.com/timnitGebru/status/1458200751327494146*

160 *Who are the Gold Mafia? Godmen, conmen and a president's niece https://www.aljazeera.com/news/2023/3/23/gold-mafia-godmen-conmen-president-niece*

161 *@Mduduzi Mathuthu on X https://twitter.com/Mathuthu/status/1640803149962268680?s=20*

162 *@Tinoedzazvimwe1 on X https://twitter.com/Tinoedzazvimwe1*

163 *@TrevorNcube on X https://twitter.com/TrevorNcube/status/1641335319998889985*

164 *Zanu-PF unleashes trolls on social media https://www.thezimbabwemail.com/technology-science/zanu-pf-unleashes-trolls-on-social-media/*

165 *Death of Mirabelle Lingom: The Moving Testimony of Paul Chouta https://www.camerounactuonline.com/death-of-mirabelle-lingom-the-moving-testimony-of-paul-chouta/; Paul Chouta https://cpj.org/data/people/paul-chouta/*

Further, social media and AI will play a significant role in Africa's digital sphere. The benefits of technologies like generative AI for creative empowerment and organising must be weighed against the risks of disinformation and polarisation if misused. For example, while generative AI could help activists and marginalised communities create content to educate or persuade, it also risks being weaponised to spread false information or incite division if proper oversight is lacking. Realising the positive potential of emerging technologies requires anticipating and mitigating potential harms through ethical frameworks, literacy efforts, and accountable governance. Ensuring internet spaces are safe and inclusive for women, LGBTQ groups and other marginalised communities will be crucial. As the internet grows in impact, policy debates around regulation, censorship, privacy and taxation will likely intensify. Overall, maximising opportunities while mitigating the harms of technology will require multi-stakeholder dialogue and rights-focused imperatives.

In general, the expansion of the internet in Africa will empower citizens but also introduce new policy challenges around rights and governance. Ongoing advocacy and policy innovation will be needed to try to maximise the benefits of the internet for human development and minimise potential harm. It is expected that African leaders will rise to the challenge and ensure that freedom of expression is protected for all citizens.

Therefore, the future of internet freedom in Africa will depend on the ability of civil society, tech policy groups, and human rights advocates to push back against restrictions while also promoting balanced regulatory approaches. With vigilance and continuing advocacy, the internet can be harnessed to expand human rights and democratic participation across the African continent in the coming decade. But this will require embracing both the opportunities and responsibilities that come with digital transformation.

Combating Online Harassment

The cases highlighted in this essay show the real-world consequences of digital harassment campaigns, particularly the weaponisation of private information and sexual shaming against women. Ultimately, the goal should be to create an online landscape where harassment is not tolerated and victims feel empowered to speak up and report abuse through proper channels. With regular diligence, education, and policy changes, the internet can become a safer place for discussion and civic participation without fear of reprisal.

There are several strategies individuals can use to protect themselves, such as ignoring or blocking harassers, increasing personal cybersecurity practices, documenting abuse, and utilising support organisations. It is also critical that tech companies, governments, civil society groups, and media organisations work together to research tactics used by harassers and advocate for better protections. They also need to take care of their mental health and talking to trustworthy friends can help cope with the effects of online harassment.

Civil society organisations should develop programs that work to protect internet users and journalists from online harassment. These organisations can provide support to journalists who are being targeted, and they can also advocate for change. They can also provide Internet users and journalists with legal support if bringing legal action against an online aggressor would deter future behaviour. Other support mechanisms may include psychological support, digital security support, and peer support.

Richard Ngamita is a digital researcher and computer scientist and has recently conducted digital investigations on disinformation on social media platforms.

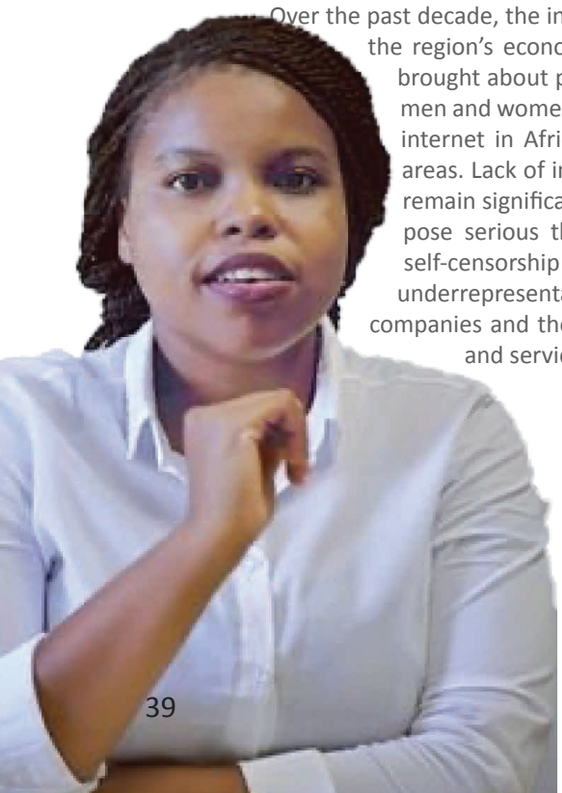
Beyond the Screen: A Look at Gender and the Internet in Africa Over the Last Decade

Introduction

Gender refers to the socially constructed characteristics of women and men.[166] Africa's history of gender reflects a complex interplay between traditional values, external influences, and evolving attitudes toward gender roles and rights. In many African societies, traditional gender roles were deeply ingrained – men were often responsible for the financial upkeep of the family and political leadership, while women were primarily engaged in tasks related to domestic work and childcare – which generally influenced social structures and power distribution. Women did, nonetheless, play crucial roles in African economies, contributing significantly to food production and small-scale business activities, which were fundamental to the local economy. Further, women in Africa have historically been active participants in resistance movements against colonial rule, apartheid, and other forms of oppression. They played key roles in political activism, organising protests, and advocating for change. Even though their contributions have been essential, many post-colonial societies maintained patriarchal systems, limiting women's access to education, healthcare, and political power.

Efforts to address these issues and ensure women's rights do not continue to be marginalised have been ongoing, with varying levels of success across different countries. Various women's empowerment movements have emerged across Africa over the last few decades, contributing towards changing attitudes and policies related to gender. These include laws against gender-based violence, quotas for women's political representation, and initiatives to promote women's economic empowerment.

Notably, the African Union adopted the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (Maputo Protocol), guaranteeing comprehensive rights to women, including the right to take part in the political process, to social and political equality with men, and improved autonomy. While the Protocol has had a positive impact on women's rights in Africa, challenges remain in terms of implementation and enforcement. The effectiveness of the Protocol depends on the commitment of governments, civil society organisations, and various stakeholders to work together to create meaningful change for women across the continent which is diverse in terms of cultures, languages, and traditions. While some societies have been more progressive in terms of gender equality, others have been slower to change and this has been reflected and amplified on the internet.



Over the past decade, the internet has significantly transformed people's lives across Africa, shaping the region's economic, social, and cultural landscape. Technological advancements have brought about positive changes but the impact has not been equally distributed among men and women. Today, numerous challenges continue to hinder gender equality on the internet in Africa. The digital gender divide persists, particularly in rural and remote areas. Lack of infrastructure, high data costs, and limited digital literacy among women remain significant barriers. Furthermore, gender-based violence and online harassment pose serious threats to women's safety and well-being on the internet, leading to self-censorship and withdrawal from online participation. Moreover, the underrepresentation of African women in decision-making positions within tech companies and the broader technology sector limits the extent to which digital products and services are designed with women's needs and preferences in mind.

Amanda Manyame

166 *Sex and gender, Council of Europe, https://www.coe.int/en/web/gender-matters/sex-and-gender#:~:text=Sex%20refers%20to%20"the%20different,groups%20of%20women%20and%20men.*

This essay explores the evolution of gender and the internet in Africa over the last 10 years, highlighting the key trends, progress and challenges in achieving gender equality in digital access, opportunities, and representation for women who make up 50% of Africa's population. It also considers the impact that these challenges have had on internet freedom in Africa over the last decade and looks toward the future of internet freedom for women across the continent.

Overview of the Trends in Africa

Digital Literacy and Empowerment of Women

The internet has become a powerful tool for empowering women across Africa. In Nigeria and Kenya, women have been increasingly using online marketplaces and platforms to start and grow their businesses. Platforms like Jumia, Konga, and Kilimall have provided women entrepreneurs with a digital space to sell products ranging from fashion to household items, contributing to their economic empowerment. Organisations like She Code Africa and Andela are providing coding and technology education specifically targeted at women. These initiatives offer coding boot camps, workshops, and mentorship programs to help women develop skills in technology and programming. More and more women are now working in the technology sector and organisations such as Women in Tech Africa (WiTA) focus on entrepreneurship expansion and multiplying the numbers of women in technology and have chapters in Ghana, Malawi, Zimbabwe, Kenya, Tanzania and Mauritius. Online banking and financial services have become more accessible, enabling women to manage their finances, access credit, and engage in economic activities more conveniently.

Increased Civic Participation

African women have also been actively using social media platforms to raise awareness and advocate for various social and political issues. The #BringBackOurGirls campaign in Nigeria and the WomensMarchKE movement in Kenya are examples of women-led online campaigns that gained significant attention and generated great impact. Women are using social media and online platforms to engage in political discourse, advocate for gender equality, and connect with other women in leadership positions. Moreover, gender disparities in online content creation and representation can affect the diversity of voices present online. While representation is increasing, the gender digital divide limits the range of perspectives available, impacting women's internet freedom to access diverse viewpoints. Women's participation in online political discourse and activism might also be influenced by cultural and gender norms that limit their engagement in public affairs.

Addressing Access and Connectivity

Various organisations and governments have launched initiatives to promote digital inclusion, aiming to provide women and girls with the skills and resources needed to effectively use the internet. These initiatives often include training programs, workshops, and educational campaigns. In Rwanda, MTN, a telecoms company, partnered with the Bank of Kigali to provide a Device Financing Program enabling customers to buy smartphones and tablets by paying instalments of Rwf200 (17 US cents) per day.[167] Likewise, Zenzeleni Community Networks, South Africa's first cooperative-owned Internet Service Provider (ISP), provides affordable internet to a remote rural community using a solar-powered, community-owned Wi-Fi telecommunications network solution. [168]

Across the continent, governments, civil society organisations, and private sector actors have joined forces to establish several community-based digital centres, enhancing digital skills and empowering women to navigate the online world effectively. For instance, Apps and Girls, an NGO based in Tanzania is dedicated to bridging the technology gender gap in Tanzania and across sub-Sahara Africa.

167 *AllAfrica. 2022. Rwanda: MTN, Bk Launch Device Financing Drive for Smartphone Affordability. https://allafrica.com/stories/202211250099.html*
168 *https://www.apc.org/en/member/zenzeleni-networks-npc*

Legal and Policy Initiatives

There have also been multiple policy initiatives established on the continent to adapt to the digital economy, and an African Digital Transformation Strategy[169] was adopted in order to fully incorporate digital transformation technologies and advanced technological systems into the continent's economy. The adoption and implementation of the African Continental Free Trade Area (AfCFTA) furthers the development of a digital single market for Africa. In 2022, the Resolution on the Protection of Women Against Digital Violence in Africa passed by the African Commission on Human and People's Rights, called on States to, amongst other things, review and adopt laws that are aimed at combating all forms of digital violence, including expanding the definition of gender-based violence to include digital violence against women.[170]

Many countries have been strengthening and enforcing laws to hold perpetrators accountable for cybercrimes. Examples include South Africa's Cybercrimes Act, Egypt's Anti-Cyber and Information Technology Crimes, Ghana's Cybersecurity Act, and Lesotho's Cybercrime Bill. As civil society has continued to advocate for better laws to protect women from online gender-based violence (OGBV), some countries have passed laws to protect from some aspects of OGBV. For instance, in Kenya, the National Cohesion and Integration Act and in Ethiopia, the Hate Speech and Disinformation Prevention and Suppression Proclamation were enacted to address, amongst other things, hate speech targeted at a particular person or group of people. South Africa passed and amended national legislation and policies, including the Protection from Harassment Act, the Domestic Violence Act and the National Strategic Plan on Gender-based Violence and Femicide to address the violence against women in the physical world and online. Similarly, Angola's Data Protection Act criminalises doxxing and non-consensual sharing of intimate images.

E-Health Solutions

The internet has become a valuable source of health information for women, offering access to resources related to reproductive health, maternal care, family planning, and general well-being. Denko Kunafoni, in Mali, specialises in the health of women, pregnant women, mothers, and children and provides information on maternity, advice, and access to specialist doctors. GiftedMom is a digital platform helping to fight against child mortality by amongst other things, reminding mothers and pregnant mothers of the dates of vaccinations or consultations.[171]

Challenges:

Access and Connectivity

Access to the internet is a global concern, and Africa has not been immune to this challenge. The ITU[172] reported that in 2022 internet use in Africa stood at 28% of the population, while in the same year, the GSMA reported [173] that 46% of men used the internet compared to 34% of women that used it. Clearly, access to the internet is a major challenge in Africa, but more concerning is that there are still many women who are not aware of the internet and its benefits and others who do not have the know-how or technical skills. A larger number are not able to access the internet because of the unaffordability of technological devices that enable access to the internet, unaffordability of data, and concerns about safety while on the internet.

USD **100 billion**
investment required to provide universal internet access across Africa

169 *African Digital Transformation Strategy https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf*
170 *Resolution on the Protection of Women Against Digital Violence in Africa - ACHPR/Res. 522 (LXXII) 2022 https://achpr.au.int/en/adopted-resolutions/522-resolution-protection-women-against-digital-violence-africa-achpr#:~:text=THE%20AFRICAN%20COMMISSION,-Calls%20on%20States&text=Review%2Fadopt%20legislation%20that%20aims,2.*
171 *https://www.do4africa.org/en/e-health-status-in-africa/*
172 *ITU. 2023. Measuring digital development – Facts and Figures: Focus on Least Developed Countries https://www.itu.int/hub/publication/d-ind-ict_mdd-2023/*
173 *GSMA. 2022. The Mobile Economy Sub-Saharan Africa. https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/10/The-Mobile-Economy-Sub-Saharan-Africa-2022*

The gender digital divide is a multilayered challenge for the continent. It is not just about access to the internet but meaningful access, which encapsulates a number of factors, starting with having the necessary infrastructure in place to provide internet services. According to the World Bank, achieving universal, good-quality internet access across Africa will require an investment of USD 100 billion, with nearly 80% of that investment being used for the core infrastructure to establish and maintain broadband networks.[174]

men who used the internet in 2022

Second, across Africa, the main device historically used to access the internet is the mobile phone.[175] Yet in Sub-Saharan Africa, households spend almost 45% of their average monthly income to purchase the cheapest available smartphone on the market.[176] The third factor is the cost of the data to access the internet. Data costs a lot in Africa; for instance, in Equatorial Guinea, one gigabyte of mobile data costs USD 49.67; in Sao Tome and Principe, it costs USD 30.97, Malawi it costs USD 25.46, Chad it costs USD 23.33 and Namibia it costs USD $22.37.[177] Another factor to consider is digital literacy, that is, having the know-how to use the Internet.

Online Safety

Another growing concern has been that of OGBV. Online platforms have become breeding grounds for harassment, discrimination, and abuse – disproportionately affecting women in all their intersections. OGBV refers to any act of violence, harassment, or discrimination that targets individuals based on their gender through the use of digital technologies. This form of violence manifests in various ways, including cyberbullying, non-consensual sharing of intimate images, sexual coercion and extortion, misogynistic comments, stalking, and threats of violence.[178] Also, gendered data privacy concerns can arise particularly when women's personal data is collected, shared, or used without their informed consent.[179]

Women, across their different intersections, often experience more severe and persistent forms of OGBV due to deeply entrenched patriarchal norms and gender inequalities in many African societies. Those most affected include women who are activists, human rights defenders, politicians, entertainers, influencers, celebrities, journalists, business women, young girls and refugees, etc.[180] A recent global study showed that harassment was most prevalent on Facebook with 39%, followed by Instagram (23%), WhatsApp (14%), Snapchat (10%), Twitter (9%) and TikTok (6%).[181] Perpetrators of OGBV often hide under the cloak of anonymity and as a result of their actions, kick many women and girls out of the platforms.

The consequences of OGBV are profound and far-reaching, including psychological trauma, wherein survivors often experience anxiety, depression, and post-traumatic stress disorder, affecting their mental health and overall well-being.[182] Another impact is that of women opting to stay offline for fear of online abuse, which in turn deters women from engaging in public discussions, limiting their participation in social, political, and economic spheres.[183] Further, the digital divide is also exacerbated by the fear of OGBV, which prevents women from accessing online resources and opportunities. OGBV also perpetuates harmful gender stereotypes by reinforcing the idea that women should remain passive and voiceless. Online violence can also foster an atmosphere of distrust and hostility, hindering meaningful dialogue and understanding between genders.

174 *WorldBank. 2019. Achieving Broadband Access for All in Africa Comes With a $100 Billion Price Tag. https://www.worldbank.org/en/news/press-release/2019/10/17/achieving-broadband-access-for-all-in-africa-comes-with-a-100-billion-price-tag*

175 *The Conversation. 2015. Mobile phones the pathway to internet in Africa. https://theconversation.com/mobile-phones-the-pathway-to-internet-in-africa-42363*

176 *How expensive is a smartphone in different countries? https://a4ai.org/news/how-expensive-is-a-smartphone-in-different-countries*

177 *Business Insider Africa. 2023. The high cost of mobile data in Africa: Top 20 most expensive countries. https://africa.businessinsider.com/local/lifestyle/20-african-countries-with-the-most-expensive-mobile-data-prices-is-your-country-on/sjxr35p*

178 *Understanding Online Gender-based Violence in Southern Africa https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/FINAL_v_Understanding_oGBV_in_Southern_Africa.pdf*

179 *MyDataMyRights. 2020. A feminist approach to assessing AI, privacy and data protection in South Africa. https://mydatarights.africa/a-feminist-approach-to-assessing-ai-privacy-and-data-protection-in-south-africa/*

180 *OGBV in the Global South https://webfoundation.org/2022/09/ogbv-in-the-global-south/#:~:text=Among%20the%20dominant%20forms%20of,%2C%20sexualised%2C%20and%20gendered%20abuse.*

181 *Ibid*

182 *The impact of online gender-based violence on women in public life https://webfoundation.org/2020/11/the-impact-of-online-gender-based-violence-on-women-in-public-life/*

183 *Understanding Online Gender-based Violence in Southern Africa https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/FINAL_v_Understanding_oGBV_in_Southern_Africa.pdf*

Gaps in Legal Protection

Although there has been a strengthening of legal and policy protection across the continent, there are gaps in protection. Cybercrime laws that are being passed include offences for financial crimes committed online, data privacy violations, criminalisation of online speech, child sexual abuse material (CSAM), and cyberstalking and harassment. These do not adequately address the full spectrum of the manifestations of OGBV. Considering cybercrime from a gendered perspective is largely lacking, yet it is important in order to develop gender-sensitive crime prevention strategies and to ensure a more comprehensive approach to countering cybercrime and cyber violence. There is a need for a greater gender balance in institutions dealing with cybercrime and the development of gender-sensitive victim-oriented approaches and programs with survivor-centred outcomes.

Further, the legal protections are siloed and do not always address OGBV in its entirety, but address certain forms. This leaves victims or survivors with either no legal recourse or having to apply laws such as data protection or copyright laws, whose provisions are not fit for purpose, are outdated, have the onerous burden of proof requirements, and ultimately leave women without any reasonable recourse.

Factors for the Trends in Africa

Online Safety

OGBV is part of a continuum of gender-based violence that is rooted in structural and gender inequalities inherent in patriarchal societies. This continuum highlights the interconnectedness of various forms of violence, harassment, and discrimination that target individuals based on their gender. [184] It has taken time for OGBV to be recognised as a concern in Africa. Women's rights organisations and other organisations advocating for safety online have helped increase awareness. The worldwide 16 Days of Activism against Gender-Based Violence campaign has also been used by many to highlight the increase in OGBV.

Digital Inclusion

Women and men do not have equal access to the internet. This divide is a result of historical, social and economic inequalities suffered by women. These include responsibilities for unpaid care and household work, social norms and gender roles. It is also a result of the differences in women's access to and control over assets and finance and unequal investments in the capabilities of girls and boys – which limits women's choices relative to men's with regard to employment, ability to earn an income and overall access to digital technologies. Digital inclusion is crucial for women to access emerging technologies that offer platforms to voice their concerns, identify their specific needs, and promote access to basic services. However, with nearly three billion people not being connected to the internet as of 2022, access remains a global concern, more so for women.

Political Participation and Online Spaces

Women's participation in online political discourse and activism has been influenced by cultural and gender norms that limit their engagement in public affairs. Furthermore, when a woman is criticised, the criticism often targets her physical appearance or is sexually violent.[185] This has had an impact on women's freedom and ability to participate in shaping online political discussions as it forces them to self-censor and refrain from online political or other engagement.

184 *Hicks.2021. Global evidence on the prevalence and impact of online gender-based violence. K4D Helpdesk Report. Institute of Development Studies. DOI:10.19088/K4D.2021.140*

185 *Diego B. P. Gomes and Carine Meyimdjui. 2023. Digitalization and Gender Equality in Political Leadership in Sub-Saharan Africa. IMF Working Paper 23/122. https://www.imf.org/en/Videos/view?category=9*

Advocacy by Civil Society

Several organisations in Africa have actively campaigned for policy changes to support women's rights and empowerment online. For instance, the Feminist Internet, the Web Foundation, the Association for Progressive Communication (APC), the African Women's Development and Communication Network (FEMNET), Equality Now, and the Women of Uganda Network (WOUGNET), work in various countries to promote digital rights and gender equality online. They continue to advocate for policies that enhance women's participation on the internet and the digital economy.

Increased Internet Penetration

The increased internet penetration across the continent has had a positive impact on more Africans, especially women, gaining access to the internet. This is primarily due to the increased availability of smartphones, improved connectivity, and efforts to bridge the digital divide. This has provided women with greater opportunities to engage in online activities and access information.

New and Emerging Technologies

The landscape of technology is constantly evolving. However, mobile phones have become a powerful tool for reaching women in rural and remote areas with essential information and services. Mobile-based apps and services can provide education, healthcare information, financial services, and more, thereby empowering women and girls. It is likely that the way in which mobile phones are used will continue to evolve to provide more and better access to financial services and improve agricultural activities, education, healthcare and business.

The emerging trend of making use of data-driven technologies and artificial intelligence (AI) will help to evolve the gathering and analysis of gender-disaggregated data, allowing policymakers and organisations to make informed decisions and develop targeted interventions that bring value to women in Africa. This will enable the continent to be better equipped to harness the opportunities provided by emerging technologies such as general-purpose artificial intelligence (GPAI), and mixed reality technologies such as the metaverse and address challenges that these emerging technologies present.

Impact on Internet Freedom in Africa

Gender has a significant impact on internet freedom in Africa, influencing how individuals, especially women, access, use, and navigate online spaces. Gender disparities in access to technology and internet infrastructure have limited women's ability to fully utilise online platforms. Digital literacy and technical skills have impacted women's confidence and competence in using the internet. Women continue to face barriers to learning how to navigate online spaces, use digital tools effectively, and protect their online privacy. This has led to women avoiding certain online activities.

Women in Africa are often targets of OGBV which has deterred them from expressing themselves freely online and participating in public discourse. This adds to the societal norms and cultural expectations, which influence how women are perceived and treated online. Some women may be discouraged from participating in online discussions or sharing their opinions due to fears of social backlash or negative repercussions within their communities. Moreover, women's voices and perspectives are sometimes marginalised or underrepresented in online discussions and platforms. This lack of representation leads to a narrower range of topics being discussed and limits the diversity of viewpoints available to internet users.

Reflections on the Future

Gender and internet freedom are intricately linked in Africa, with significant disparities in access, representation, and digital rights. Empowering women with digital literacy and promoting gender equality in online spaces are essential steps toward creating a more inclusive and diverse digital landscape on the continent. As the continent is moving towards digital transformation with basic services such as government services, digital ID systems, and other e-commerce solutions being implemented across the continent, it is important for the historic challenges highlighted above to be addressed as a matter of urgency.

African governments should therefore accelerate the implementation and adoption of existing policies, frameworks, and strategies to eliminate the gender digital divide, including by ensuring the leadership of women in digital transformation initiatives. Women need to be met in the spaces they occupy, in different formal and informal industries. Moreover, the inclusion of women in the growing digital economy will further enhance women's contribution, participation and leadership. This includes consciously increasing resources available to women-led businesses and establishing programs to effectively support the education of women and young girls in developing information and communication technologies in order to harness the power of the digital economy.

Enacting laws and policies to address OGBV, implementing educational programs that raise awareness about OGBV, promoting digital literacy, and teaching empathy and respectful communication are all important for internet freedom to thrive. In addition, empowering women to take on more active roles in shaping the digital landscape, and ensuring their voices are heard and respected, is pivotal to ensuring safer online spaces and the realisation of internet freedom in Africa.

Lastly, governments and policymakers in Africa must take proactive steps to address gender-specific challenges to internet freedom. By fostering a more inclusive and supportive digital environment, Africa can unleash the full potential of women on the continent, and consequently drive sustainable development and advance gender equality and women empowerment across the continent.

Amanda Manyame is digital law and rights expert and a proponent of public interest technology. She is also a Digital Rights Advisor at Equality Now.

Reflection on State Accountability for Digital Rights in the Past Decade: The Ups and Downs

Introduction

Under international human rights law, states are expected to take measures of a political, legal, administrative, social and economic nature to ensure that all persons enjoy their rights and freedoms under no or minimal interruptions. States have tri-pronged obligations and duties with respect to human rights which are essentially all measures and mechanisms undertaken by states as duty bearers to respect, protect and fulfil rights.[186] State accountability requires that those with authority have the responsibility to account for and provide answers for their actions.[187] It also includes measures by states' peers and civil society actors to hold them accountable, whether at the national, regional or international level.

This paper explores state accountability with respect to digital rights in Africa. It underscores the fact that States are mandated to ensure universal access to and the enjoyment of digital rights and freedoms.

State Accountability

Human rights accountability dates back to the Magna Carta in the thirteenth century when limits to the powers of the Royal government in England were set.[188] Similarly, the roles of the American Declaration of Independence in 1776 and the Declaration des droits de l'Homme et de du citoyen of 1789 (Declaration of the Rights of Man and Citizen) in setting the foundation for countering human rights abuse cannot be understated.[189] Later, the effect of the first and second world wars created a need for human rights protection following the perpetration of various atrocities against humans. Hence the UN Charter which forms the core of human rights came into being in 1945. The charter-based system was established to ringfence individuals against human rights violations.[190] Consequently, the Universal Declaration of Human Rights was adopted in 1948, followed by the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR) in 1966.

To date, a number of international treaties have been adopted and continue to be adopted to protect human rights, including at the regional level. Within the treaties, accountability mechanisms are provided such as treaty monitoring bodies. In this regard the Office of the United Nations High Commissioner for Human Rights and a number of human rights monitoring committees have been established.

At the African regional level, efforts have been undertaken to protect human rights including the creation of regional human rights institutions such as the African Commission on Human and Peoples Rights (ACHPR), the African Court on Human and Peoples Rights as well as other sub-regional initiatives in the various Regional Economic Communities (RECs) especially since the 1970s.[191] These institutions form a critical pillar for accountability of human rights violations including in the digital sphere. Accountability is enabled through engagements with the ACHPR, special mechanisms and litigation at the regional courts such as the East African Court of Justice (EACJ) and the Community Court of Justice of the Economic Community of West African States (ECOWAS Court).

Edrine Wanyama

186 *Office of the UN High Commissioner for Human Rights, "International Human Rights Law," https://www.ohchr.org/en/instruments-and-mechanisms/international-human-rights-law#:~:text=By%20becoming%20parties%20to%20international,and%20to%20fulfil%20human%20rights.&text=The%20obligation%20to%20fulfil%20means,enjoyment%20of%20basic%20human%20rights.*

187 *OHCHR, "WHO WILL BE ACCOUNTABLE? Human Rights and the Post-2015 Development Agenda Summary", https://www.ohchr.org/sites/default/files/Documents/Publications/WhoWillBeAccountable_summary_en.pdf*

188 *Viljoen, Frans. "International human rights law: A short history." Un Chronicle 1, no. 2 (2009): 8-13.*

189 *Ibid.*

190 *Ibid.*

191 *Ibid.*

Mechanisms within the RECs including the Economic Community of West African States (ECOWAS), the Common Market for Eastern and Southern Africa (COMESA), the Southern African Development Community (SADC) and the East African Community (EAC) have over the years contributed fundamentally to the enjoyment of human rights including digital rights. More importantly, these mechanisms are open to individuals and civil society organisations who have over time contributed to the development of jurisprudence of digital rights. It should be noted that the RECs in Africa such as the EAC have suffered integration challenges including at political, social and economic levels that led to its collapse and was later rebuilt. Some of the reasons for the failure include the lack of political will as well as accusations and suspicions among member states.

Overview of the Trends in Africa

As earlier observed, participation in the human rights monitoring mechanisms has been central in the realisation of digital rights.[192] Since 2006, the Universal Periodic Review (UPR)[193] which is a 193 membership mechanism, the human rights record of African countries has been reviewed severally. Recommendations have been made on freedom of expression, access to information, assembly and association online, access to the internet and the space for the exercise of civic rights and freedoms. Over the years, there has been a steady increase in the number of recommendations on freedom of expression including digital freedoms, on which Tunisia received 15 and Morocco 17 recommendations in 2022.[194]

As a result of these engagements, there have been some levels of improvement in the space within which digital rights are enjoyed. Cases of total internet shutdowns during elections on the continent did not happen in Kenya, Nigeria and Zimbabwe which just concluded their general elections, although Zimbabwe slowed down the internet.[195] Courts such as the East African Court of Justice (EACJ) have made progressive decisions on digital rights as was the Tanzanian case of Mseto v. Attorney General[196] where the EACJ declared[197] that a Ministerial order banning a Tanzanian newspaper for three years violated the rights to freedom of expression and press freedom. Similarly, in Good v Botswana,[198] the African Commission decided that the deportation of an Australian national for expression of unpopular political views violated freedom of expression and information.

The African Commission has also presented opportunities, especially during the 76 ordinary sessions it has held so far[199] and entertainment of communications in which it has been emphatic on the protection of individual and group rights on the continent. The four ordinary sessions which are held every year have improved the human rights record of states over the decades since they are a platform for reflection and making proposals for reform.[200] The Commission has 12 special mechanisms including the special rapporteurs, committees, and working groups.

192 *Basic facts about the UPR, https://www.ohchr.org/en/hr-bodies/upr/basic-facts*

193 *UN Human Rights Council, "Universal Periodic Review," https://www.ohchr.org/en/hr-bodies/upr/upr-home*

194 *See for example, Dodo Wang, "summary of our accomplishments from the last half of 2022." Uproar, February 16, 2023, https://www.uproar.fyi/blog/article/uproar-updates, see also A summary of recommendations made to Benin, Gabon and Ghana during the 42nd session of the Universal Periodic Review, https://www.uproar.fyi/blog/article/the-42nd-session-of-the-universal-periodic-review-digital-rights-in-benin-gabon-and-ghana*

195 *The East African, "Zimbabwe 'slows down' internet as voting begins," August 23, 2023, https://www.theeastafrican.co.ke/tea/rest-of-africa/zimbabwe-slows-down-internet-as-voting-begins-4344448*

196 *Managing Editor Mseto and Hali Halisi Publishers Ltd Applications Nos. 3 and 4 of 2019, https://www.eacj.org/wp-content/uploads/2020/06/Mseto-V-AG-Final.pdf Mseto v. Attorney General https://globalfreedomofexpression.columbia.edu/cases/mseto-v-attorney-general/*

197 *313/05: Kenneth Good / Republic of Botswana, https://achpr.au.int/sites/default/files/files/2022-11/achpr4731305eng.pdf*

198 *The 77th Ordinary Session is coming up in October 2023, "Upcoming Session 77th Ordinary Session of the African Commission on Human & Peoples' Rights (ACHPR),"*

199 *https://achpr.au.int/en/news/press-releases/2023-09-05/upcoming-session-77th-ordinary-session-african-commission*

200 *ACHPR, "Sessions," https://achpr.au.int/en/sessions/overview*

Specifically, the Special Rapporteur on Freedom of Expression and Access to Information mechanism was created in 2004.[201] Since then, the rapporteur who operates through a working group, has adopted 31 resolutions and issued four mechanism reports which highlight the plight of expression and access to information and the need for reform. Governance and accountability have improved as a result.[202] The communications procedure similarly presents opportunities to hold states accountable for human rights violations in their countries.[203] With efforts of individuals and Civil Society Organisations (CSOs) through established procedures,[204] the human rights record of some states including digital rights has improved.

Additionally, by creating binding and non-legal force or persuasion respectively, hard and soft laws have been instrumental in promoting state accountability in the digital civic space.[205] For instance, the UDHR, ICCPR, ICESCR, other conventions and covenants, declarations, resolutions, general comments and special rapporteur reports at the UN level and African region have influenced and shaped the digital civic space on the continent, including the promotion and enhancement of human rights in businesses that directly affect human rights. In Africa, the Declaration of Principles of Freedom of Expression and Access to Information in Africa, 2019 forms part of the soft laws made under article 9 of the ACHPR, including the Model Law on Access to Information for Africa of 2013 and the Guidelines on Access to Information and Elections in Africa, 2017.

State responses to the human rights monitoring mechanisms have seen an increment in laws enacted domestically to provide and regulate the digital civic space including promoting spaces for enjoyment and checking harms that are often perpetrated by business. For instance, 36 out of 54 countries on the continent have enacted data protection and privacy laws.[206] The African Union Convention on Cyber Security and Personal Data Protection[207] has today garnered 18 signatures and 14 ratifications.[208] Similarly, out of the 54 countries on the African continent, at least 23 have enacted access to Information laws with 11 having pending bills.[209] Furthermore, at least 33 countries have laws that regulate electronic transactions,[210] 39 countries have cybercrime laws,[211] and, 28 enacted Online Consumer Protection Legislation.[212]

201 *ACHPR, "Special Rapporteur on Freedom of Expression and Access to Information," https://achpr.au.int/en/mechanisms/special-rapporteur-freedom-expression-and-access-information*

202 *Ibid.*

203 *ACHPR, "Communications Procedure," https://achpr.au.int/en/communications-procedure*

204 *The African Commission on Human and Peoples' Rights, "Information Sheet No.3 Communication Procedure Organisation of African Unity," https://achpr.au.int/sites/default/files/files/2021-04/achprcommunicationprocedureeng.pdf*

205 *Charlotte Piveteau, "Between law and values: why soft law reinforces the hybrid nature of international human rights law," https://www.implications-philosophiques.org/between-law-and-values-why-soft-law-reinforces-the-hybrid-nature-of-international-human-rights-law/*

206 *Hogan Lovells, "Recent developments in African data protection laws - Outlook for 2023," https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45#:~:text=Here%2C%20the%20authority%20in%20charge,and%2C%20until%202022%2C%20Nigeria.*

207 *African Union Convention on Cyber Security and Personal Data Protection https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf*

208 *African Union Convention on Cyber Security and Personal Data Protection, "List of Countries which have Signed, Ratified/Acceded," https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf*

209 *Article 19, "The right to information around the world," https://www.article19.org/right-to-information-around-the-world/*

210 *UNCTAD, "E-transactions Legislation Worldwide," https://unctad.org/page/e-transactions-legislation-worldwide*

211 *UNCTAD, "Cybercrime Legislation Worldwide," https://unctad.org/page/cybercrime-legislation-worldwide*

212 *UNCTAD, "Online Consumer Protection Legislation Worldwide," https://unctad.org/page/online-consumer-protection-legislation-worldwide*

From a business perspective, states are taking legal and policy measures that aim to ensure compliance with the UN Guiding Principles on Business and Human Rights (UNGPs).[213] It is also a means to ensure that business is not conducted to the detriment of human rights including digital freedoms. Through the responses, states' human rights record is improved. Responsible business practices checks are often a measure in human rights monitoring mechanisms.[214] The African Union is indeed taking steps to ensure that Member States operate in full compliance with the current Draft AU Policy Framework on Human Rights and Business.

A fundamental milestone is evident in the integration of provisions which are specific to human rights including the establishment of human rights monitoring and adjudicating bodies in national constitutions. In most African countries including Algeria, Benin, Cameroon, Chad, Ghana, Kenya, Liberia, Malawi, Mauritania, Morocco, Nigeria, Rwanda, Senegal, Sierra Leone, South Africa, Tanzania, Togo, Tunisia, Uganda and Zambia where the constitution is the supreme law, there are specific provisions establishing national human rights commissions.The commissions are considered independent with a goal to protect human rights. There has been positive progress by human rights commissions with annual reports highlighting the state of human rights and recommendations requiring states to take specific actions for human rights accountability.

Common Challenges to State Accountability

While state accountability has over time shown to be effective in enhancing the protection and promotion of digital rights and freedoms, there are a number of challenges and shortcomings that undermine accountability.

The lack of political will remains a significant challenge as states' failure to investigate and prosecute human rights violations has created unsafe spaces for the enjoyment of digital rights.[215] While pointers of commitment exist, the lack of independent judicial systems in some countries often results in injustice against victims. Similarly, corruption has had an adverse impact on the realisation of digital rights. The 2022 Transparency International report shows that at least 90% of the countries in Sub-Saharan Africa scored below 50 in the fight against corruption.[216] In most cases, rights are violated with impunity with no clear accountability and effective oversight mechanisms on the continent.

Even the institutions charged with protecting rights such as the Police do not always operate independently. They are often susceptible to bias, political interference and direction. Coupled with weak legal systems characterised by regressive and retrogressive laws, rights are often left at the mercy of regimes in power with curtailment being at the core. As a result, the civic space for actors and activists such as CSOs and media is limited and continues to shrink.

Authoritarian governments in Cameroon, Djibouti, Eritrea, Equatorial Guinea, Morocco, Republic of the Congo, Rwanda, South Sudan, Swaziland and Uganda have overstayed their time in power and are intolerant of criticism from activists including CSOs, media, the private sector and human rights defenders (HRDs). Moreover, these governments often have predetermined and weak judicial systems that lack judicial independence and do not have the moral authority to entertain matters which warrant judicial attention and adjudication.

213 *UN Guiding Principles on Business and Human Rights (UNGPs) https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf*

214 *UNDP, "Business and Human Rights," https://www.undp.org/rolhr/business-and-human-rights*

215 *Navanethem Pillay, "Establishing Effective Accountability Mechanisms for Human Rights Violations," https://www.un.org/en/chronicle/article/establishing-effective-accountability-mechanisms-human-rights-violations*

216 *Transparency International, "Corruption Perceptions Index, 2022" https://www.transparency.org/en/cpi/2022*

The securitisation of the government sectors and issues relating to human rights enforcement have curtailed rights and freedoms. Digital rights alongside other rights are now a "security" issue and some governments have tended to brand the enjoyment of rights such as association and assembly as a threat to national peace and security. In some cases, civic space actors have been branded as terrorists and protests viewed as terrorism threats, which are essentially scapegoats to curtail the enjoyment of rights.

In addition, the weak nature of the existing regional and international human rights protection and monitoring mechanisms has hindered state accountability. Firstly, the investigatory processes and special rapporteur reports take long periods before conclusion. Similarly, decisions of specialised courts and commissions take a long time to yield the desired results or to be concluded against states. Secondly, in most cases their decisions in most cases are not binding or enforceable. They are mere observations, recommendations and conclusions to which states against whom the decisions are made are never compelled to comply with and therefore unenforceable in most cases. States often raise the non-interference justification with respect to domestic matters relying on the sovereignty doctrine under international law. Resultantly, state accountability continues to has been severely and continues to be undermined to the detriment of rights and freedoms.

Factors for the Trends of State Accountability

The progress toward State accountability is mixed, with increases in some areas and declines in other areas. Improved state accountability can be attributed to a number of factors including the integration of human rights-based approaches[217] in most state initiatives and the growth of activism among citizens. Additionally, the increased knowledge and awareness of rights and ways to demand for them has enhanced accountability by States. Also, the vibrant Citizens, CSOs, media and other players have developed strategies to document, monitor and report human rights violations while keeping track of the various developments. Similarly, pressure from other state parties aimed at promoting development, compliance with established human rights standards and countering discrimination have enhanced state accountability.[218]

Inversely, the states' human rights records have been on the decline due to irresponsible use of digital platforms by actors including activists, political dissidents, HRDs, media and CSOs. The slow response by states to addressing human rights concerns as well as the generally increased abuse of rights with impunity has bled activism for accountability and regional and international levels. Furthermore, the weaponization of laws has embedded authoritarianism by governments as a control tool, thereby undermining accountability for human rights violations. For instance, in Cameroon, Ethiopia, Kenya, Nigeria and Uganda combating hate speech, terrorism, disinformation, misinformation and false news has become a common justification by States to curtail freedoms through the enactment of regressive laws.[219]

In addition, failed security sectors with no major progressive reforms, loss of confidence in the justice, law and order sectors, lawlessness, general disrespect for human rights, a weakened and helpless citizenry and endemic corruption on the continent have made achieving state accountability for human rights violations difficult.[220]

217 *See for instance, WHO, "Accountability as a driver of health equity," https://apps.who.int/iris/bitstream/handle/10665/312282/9789289054096-eng.pdf?sequence=1&isAllowed=y*

218 *OHCHR, "Who Will Be Accountable? Human Rights and the Post-2015 Development Agenda," https://www.ohchr.org/sites/default/files/Documents/Publications/WhoWillBeAccountable_summary_en.pdf*

219 *See for instance, CIPESA, "Disinformation Pathways and Effects: Case Studies from Five African Countries," https://cipesa.org/wp-content/files/briefs/Disinformation_Pathways_and_Effects_Case_Studies_from_Five_African_Countries_Report.pdf*

220 *USAID, "Promoting Accountability & Transparency," https://2017-2020.usaid.gov/what-we-do/democracy-human-rights-and-governance/promoting-accountability-transparency*

Impact on Internet Freedom in Africa

State accountability for digital rights violations has had a mixed impact on internet freedom in Africa. Importantly, there is now increased recognition of digital rights and freedoms by states. Indeed, it is now recognised that rights enjoyed online must be afforded similar protection as those enjoyed offline.[221] Today, the Special Rapporteurs on freedom of expression and access to information have fundamentally contributed to the realisation of digital rights by following up on states and holding them accountable. Perhaps, it is not an overstatement to note that states have become more compliant with international reporting obligations in fear of embarrassment before their peers. They now report more frequently to the African Commission than they used to do in the past. Overall, the accountability mechanisms have helped protect digital rights by deterring governments from violating them and have provided avenues for redress for victims of violations.

Of concern is that as a result of increased recognition of digital rights, some countries are not convinced by both local and international duties and obligations. They find internet freedoms to be overly empowering to their citizens who are increasingly demanding accountability. As a result, there are increased deliberate efforts by States to justify repressive laws and practices to silence dissent including the control and limitation of access to the internet under the guise of safeguarding human rights. This has been witnessed by the common trends of internet shutdowns, internet throttling and social media restrictions such as in Ethiopia, the Democratic Republic of Congo, Sudan, Tanzania, Uganda, Zambia and Zimbabwe.

New and Emerging Issues for Consideration

As digital rights continue to gain relevance, the multifaceted range of issues that affect them also have an impact on state accountability. Technological advancement such as the use of artificial intelligence is shaping the digital civic space. Innovators are quick to develop new technologies which could endanger rights and freedoms. States are also up in arms with countermeasures to contain what are considered threats posed by new technologies. While technology is critical for the progressive development and realisation of digital rights, it is imperative that the proposed policy and regulatory measures are checked to ensure that they do not curtail digital rights. These developments also require appropriate response mechanisms from activists, human rights defenders, CSOs, the private sector and other players to ensure that potential harms to digital rights are avoided or minimised.

Reflections on the future

The future for digital rights in Africa appears bright. State accountability can improve the respect, protection and promotion of digital rights in the continent. While there are possibilities of regression, it is important to concentrate on potential progressive efforts and developments that will enhance state accountability and the space for digital rights. Positive progress will require the combined efforts of the Academia, Civil Society, Government and the Business and Tech community as highlighted below.

221 Resolution HRC res 20/8, June 2012, https://ap.ohchr.org/documents/dpage_e.aspx?si=a/hrc/res/20/8 Reaffirmed in Resolution HRC res 26/13, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/082/83/PDF/G1408283.pdf?OpenElement

- Governments should have the political will to promote, protect and fulfil digital rights and freedoms in accordance with international human rights law. Where the will has been lost, States should make efforts to renew the political will and commitment to ensure robust protection of digital rights. Renewed political will and commitment is critical to fight corruption, empower citizens and promote human rights.
- Governments should build, strengthen and guarantee independence to its oversight and enforcement agencies including the human rights monitoring bodies, the police and judicial systems.
- Governments should increase the funding to human rights bodies such as the African Commission and the regional courts within RECs so as to enhance their operations, hear more cases, and be more efficient and accessible.
- Governments should provide a favourable environment for the operations of academia, civil society, business and the tech communities such as through the enacting of enabling and progressive legislation. This will facilitate efforts such as lobbying and advocacy engagements that seek to promote the realisation of digital rights.
- The academia, civil society, business and the tech community need to work jointly to promote accountability of governments for digital rights by among others conducting evidence-based research and objectively reporting on state parties' progress to the established human rights monitoring mechanisms. In turn, governments should heed to recommendations and observations to ensure the protection and promotion of digital rights.
- The academia, civil society, business and the tech community should collectively and collaboratively make efforts to promote and enhance the protection of digital rights including through collaborative public interest litigation as a means to achieving progressive reforms.
- The civil society, academia, and the tech community should advance and enhance advocacy in the new and emerging areas of human rights and technology and accelerate state reporting at regional and global levels. Documentation of the impact of new and emerging technologies, the benefits and costs of violations will improve the human rights record.
- International and regional accountability bodies including courts, commissions, committees and sub-committees should adopt measures to enhance their efficiency such as through the use of video conferencing to engage individuals, CSOs, media and academia as well as other stakeholders.
- The government, jointly with the academia, civil society, business and the tech community should collectively build the capacity and awareness of citizens and other players to demand for their rights and accountability for rights violations
- The business and tech community should progressively and proactively integrate and observe human rights in their businesses so as to check human rights harms emerging from themGovernments should take all measures to ensure that the policy and legal frameworks address potential harms of doing business to digital rights.

Edrine Wanyama is a human rights lawyer and the Legal Officer at CIPESA. He is a digital rights expert, lecturer, advocate and researcher in human rights, rule of law and democracy.

Africa's Digital Revolution: A Paradigm Shift in Economy, Society and Internet Freedom

Introduction

Africa is currently undergoing a transformative digital revolution which promises to have far-reaching effects on the continent's economy, society, and the concept of internet freedom. With the fastest-growing telecommunications markets in various aspects, this revolution has been particularly influential in the financial services sector[222] and has played a significant role in promoting internet freedom.

Nevertheless, a notable digital divide persists across the continent. In this comprehensive exploration, we delve into the intricate dimensions of Africa's digital revolution, from its historical context to its current impacts and what it means for internet freedom. We also discuss the challenges and potential solutions for Africa as it navigates the complexities of this digital transformation.

Historical Context

The digital revolution in Africa has a unique historical context characterised by a relatively late adoption of the internet compared to other regions of the world. While the internet had already made significant inroads in North America and Europe by the late 1980s, it was only in this period that Africa began to witness the initial presence of the internet. Primarily, the internet arrived in Africa through international research and educational networks, highlighting its initially academic and research-oriented nature on the continent.[223]

In the mid-1990s, African countries started taking steps to establish their first internet service providers (ISPs) and develop national internet infrastructure. However, progress was slow and was hindered by a range of factors, including limited telecommunications infrastructure, high costs associated with setting up and maintaining internet connectivity, and regulatory barriers that impeded the growth of the internet ecosystem.

Moreover, the digital divide between urban and rural areas was a significant hurdle to internet access and adoption. Urban centres, with their better infrastructure and resources, had more access to the internet compared to rural areas, where connectivity remained limited.[224] This urban-rural divide exacerbated disparities in access to information, education, and economic opportunities.

Overview of the Trends in Africa

Positive Trends

Infrastructure and the Growth of Internet Connectivity

The early 2000s marked a turning point in Africa's digital journey. Governments and private sector entities began recognising the immense potential of the internet for economic growth and development. This recognition spurred a series of initiatives aimed at expanding telecommunications infrastructure, including the introduction of policy reforms, and encouragement of competition in the telecommunications sector.[225]

Amb. Prof. Bitange Ndemo

222 *European Investment Bank (2021) The rise of Africa's digital https://www.eib.org/attachments/thematic/study_the_rise_of_africa_s_digital_economy_en.pdf*

223 *ISOC. History of the Internet in Africa https://www.internetsociety.org/internet/history-of-the-internet-in-africa/*

224 *Fuchs, C, Horak, E., (2008). Africa and the digital divide. http://fuchs.uti.at/wp-content/uploads/divide.pdf*

225 *Ndemo, E.B., 2015. Political Entrepreneurialism: Reflections of a Civil Servant on the Role of Political Institutions in Technology Innovation and Diffusion in Kenya. Stability: International Journal of Security and Development, 4(1), p. Art. 15.DOI: https://doi.org/10.5334/sta.fd*

One of the key outcomes of these efforts was the substantial increase in investments in submarine fibre-optic cables, terrestrial networks, and mobile internet services. These investments significantly improved internet connectivity across the continent. As a result, Africa's internet landscape underwent a profound transformation.[226]

Initially, internet connectivity had been limited to a few academic and research institutions, and access was expensive and restricted. However, with the expansion of telecommunications infrastructure and policy reforms, the internet became more accessible to a broader segment of the population. This democratisation of internet access paved the way for Africa's digital revolution.

The Ubiquity of Mobile Phones:

Mobile phones have had the most influence on Africa's digital transformation. The rise, particularly with the introduction of mobile money services, has been phenomenal. Mobile phones have become ubiquitous in Africa, even in regions with limited access to traditional infrastructure like roads and electricity. This widespread adoption of mobile technology has played a crucial role in expanding internet access and by extension, internet freedom, to a larger portion of the population. Also, initiatives such as the East African Community One Network Area Roaming Initiative have enabled cheaper communication within the region.[227]

Mobile money services, such as M-Pesa in Kenya, have been particularly transformative. These services have revolutionised access to financial services for previously unbanked populations. Users can conduct financial transactions, pay bills, and even access credit through their mobile phones. This trend has increased economic opportunities and reduced poverty by providing access to essential financial services. Mobile money has also enabled users to easily purchase internet data bundles to use the internet. As of 2021, 40% of the adult population and 22% of the total population in sub-Saharan Africa were connected to mobile internet services[228].

Since M-Pesa's inception in 2007, other African countries have witnessed a surge in fintech startups. These startups offer a wide range of financial services, from lending and insurance to savings and investment platforms. In 2022, there were 1.6 billion registered mobile accounts in Sub-Saharan Africa, transacting USD 3.5 billion daily.[229] Indeed, the proliferation of fintech in Africa demonstrates the continent's adaptability and innovation in the digital financial space.

Moreover, the growth of digital financial products has facilitated the expansion of e-commerce platforms. Consumers now have more options for online shopping, contributing to economic growth and the creation of jobs. In parallel, the African Continental Free Trade Area (AfCFTA) secretariat has developed the Pan-African Payments and Settlement System (PAPSS).[230] This system aims to simplify and reduce the cost of cross-border monetary transactions for African merchants and businesses. By enabling trading in local currencies, PAPSS has the potential to significantly lower transaction costs.

The Cost of Cross-Border Payments

It is essential to highlight the significance of PAPSS and initiatives addressing the issue of costly cross-border payments in Africa. According to Dianna Games and Afreximbank, money transfer systems cost Africans about USD five billion in charges every year.[231] This makes cross-border payments in Africa the most expensive in the world when compared to the global average. By enabling transactions in local currencies, PAPSS seeks to mitigate this burden and promote regional trade and economic integration.

226 *RTI Working Paper (2020) Economic Impacts of Submarine Fiber Optic Cables and Broadband Connectivity in South Africa. https://www.rti.org/publication/economic-impacts-submarine-fiber-optic-cables-and-broadband-connectivity-south-africa/fulltext.pdf*

227 *East Africa One Network Area roaming initiative https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.ONA-2016-PDF-E.pdf*

228 *New insights on mobile internet connectivity in Sub-Saharan Africa https://www.gsma.com/mobilefordevelopment/blog/new-insights-on-mobile-internet-connectivity-in-sub-saharan-africa/*

229 *State of the Mobile Money Industry in Sub-Saharan Africa 2023 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2023/08/GSMA-SOTIR-2023_Sub-Saharan.pdf*

230 *Pan-African Payments and Settlement System (PAPSS) https://papss.com/*

231 *Dianna Games https://african.business/2023/06/dossier/revolutionary-african-cross-border-payment-solution*

Other Positive Trends

With the expansion of telecommunications infrastructure and policy reforms, the internet has become more accessible to a broader segment of the population. This democratisation of internet access has paved the way for increased access to online education and resources, bridging gaps in learning opportunities and knowledge dissemination.

In addition, the advent of a data-driven economy has given rise to big tech and social media applications. These platforms have provided spaces for individuals and groups to express their opinions, organise social and political movements, and participate in public discourse. This increased civic engagement has been instrumental in pushing for accountability and transparency in governance, as well as facilitating participation in elections and decision-making processes.

Challenges

It is important to note that while these innovations have improved financial inclusion and economic opportunities, they have also raised concerns about data privacy and security. As digital financial services collect and analyse vast amounts of customer data, there is a heightened need to safeguard personal information. Additionally, the increasing reliance on digital platforms makes them attractive targets for cyberattacks. Consequently, many African governments are actively working on regulatory frameworks to govern digital financial services and protect consumers.

The increased reliance on digital platforms and the collection of vast amounts of personal data raise concerns about data privacy and security. Further, as a result of the widespread use of digital services, digital platforms often use personal data for targeted advertising and other purposes, raising questions about the extent to which individuals are unwittingly participating in an economic system driven by their data. The advent of Digital IDs which can streamline access to various services, also raises concerns about surveillance and data security. Therefore, striking the right balance between convenience and privacy will be a critical issue in the coming years.

One other challenge especially in the realm of digital financial services is striking the right balance between fostering innovation and ensuring consumer protection. While stricter regulations may stifle innovation and hinder the growth of the digital economy, lax regulations may expose consumers to risks. Therefore, ensuring robust cybersecurity measures and data governance mechanisms is crucial to protect consumers' financial data and maintain trust in online services.

Impact on Internet Freedom in Africa

Analysis of the Impacts

Internet freedom is of paramount importance for Africa and its population. It serves as a foundational pillar that enables individuals to express their thoughts, ideas, and opinions without fear of censorship or repression. By providing unrestricted access to information, a free and open internet empowers people to stay informed, engage in critical thinking, and actively participate in democratic processes.

In Africa, where diverse cultures and traditions coexist, the internet acts as a platform for cultural exchange and the dissemination of knowledge. It allows for the sharing of ideas, stories and perspectives, fostering a rich tapestry of experiences that contributes to societal growth and understanding. This digital connectivity promotes inclusivity, tolerance, and respect for diversity, breaking down barriers and promoting global citizenship.

Moreover, an open internet fuels innovation and creativity. By providing a level playing field for entrepreneurs, artists, and creators, it facilitates the development and dissemination of new ideas, products, and services. Startups and small businesses can leverage the internet to reach broader markets, establish international partnerships, and drive economic growth. The digital economy, encompassing e-commerce, digital services, and online marketplaces, thrives in an environment of internet freedom, enabling job creation, income generation and poverty reduction.

Beyond economic benefits, the internet plays a crucial role in advancing human rights and promoting social change. Online platforms serve as spaces for individuals to voice their concerns, challenge injustice and hold governments accountable for their actions. Activists, civil society organisations and ordinary citizens can rally support, mobilise movements and raise awareness about pressing social and political issues. Also, the internet amplifies marginalised voices, giving them a platform to be heard and fostering empowerment.

Furthermore, freedom of expression online means individuals can freely communicate, share ideas, and engage in public discourse. Privacy rights safeguard personal information and protect individuals from unwarranted surveillance and data breaches. Access to information ensures that people can seek knowledge, make informed decisions and participate fully in their societies.

On a broader scale, an open internet facilitates global connectivity and fosters cross-cultural understanding. It enables people from different countries and backgrounds to connect, collaborate, and exchange ideas, breaking down geographical boundaries. Social interactions, friendships, and communities formed online transcend physical limitations and create a sense of global solidarity.

Implications of the Digital Divide

Despite the significant strides made in Africa's digital transformation, a substantial digital divide still exists, particularly affecting those in rural and underserved areas who lack access to the internet and digital financial services. This persistent divide carries serious implications for the continent's future. Firstly, it widens economic disparities as urban areas reap the benefits of digital opportunities, leaving rural counterparts behind in terms of economic prospects, education, and access to vital information.

Second, it fosters inequality in education, as access to digital resources becomes indispensable for effective learning and skill development. Students without internet access face significant disadvantages in accessing educational opportunities and online learning resources. Third, the digital divide limits civic participation, preventing those without internet access from engaging in online civic spaces, thereby reducing their involvement in political and social discussions.

Fourth, small businesses in underserved regions encounter difficulties competing in the digital economy, constraining their growth potential. Lastly, the digital divide has profound implications for healthcare, as access to telemedicine and digital health services is critical, particularly in remote areas. This divide exacerbates healthcare disparities by restricting access to essential medical services. Addressing these challenges is imperative to ensure a more equitable and prosperous future for Africa.

New and Emerging Issues for Consideration - Artificial Intelligence

As I write this article, I single out Artificial Intelligence (AI) among emerging technologies that have the potential to impact internet freedom both positively and negatively. On one hand, AI can enhance internet freedom by improving access to information, enabling personalised content recommendations and enhancing cybersecurity measures. On the other hand, concerns exist regarding AI's potential for surveillance, censorship and the manipulation of online content, which could threaten internet freedom.

To limit interference and protect internet freedom in the context of AI, several measures can be taken. First, developers and organisations should prioritise the development and deployment of AI systems that adhere to ethical guidelines. This includes transparency, accountability and avoiding biases that may discriminate or restrict freedom of expression. Establishing ethical frameworks and guidelines for AI development can help ensure that AI technologies respect human rights and uphold internet freedom principles.

Second, governments should collaborate to establish regulatory frameworks to govern the use of AI in relation to internet freedom. These regulations should address issues such as data privacy, algorithmic transparency and accountability of AI systems. Striking a balance between innovation and protecting fundamental rights is crucial, and regulations should be regularly updated to keep pace with evolving AI technologies.

Third, promoting public awareness and education about AI and its impact on internet freedom is essential. This includes educating individuals about AI algorithms, data collection practices and potential biases. By empowering users with knowledge and promoting digital literacy, people can make informed decisions and better understand the implications of AI on internet freedom.

Fourth, collaboration among governments, civil society organisations, technologists, and industry stakeholders is vital in addressing the challenges posed by AI to internet freedom. Multistakeholder dialogue and partnerships can facilitate the sharing of expertise, development of best practices and collective efforts to ensure that AI technologies are deployed responsibly and do not infringe upon internet freedom.

Lastly, establishing independent oversight bodies or regulatory authorities to monitor AI systems' impact on internet freedom can help identify and address any potential abuses or biases. Regular audits of AI systems can ensure transparency, accountability, and adherence to ethical standards, thereby mitigating risks to internet freedom.

By implementing these measures, it is possible to harness the benefits of AI while safeguarding internet freedom and minimising its potential negative impacts. It requires a combination of technological advancements, legal and regulatory frameworks, public awareness, and collaborative efforts to ensure that AI is developed and used responsibly in the context of internet freedom.

Reflections on the Next 10 Years

Predicting the future of internet freedom in Africa over the next decade is speculative, but several trends and potential strategies can be considered. Stakeholders, including academia, government, business, civil society, and the tech community, must remain proactive and adaptive as emerging technologies reshape the digital landscape.

One significant strategy involves establishing robust legal frameworks. Governments can play a pivotal role in this regard by creating and periodically updating legal frameworks that protect internet freedom while keeping up with technological advancements. These frameworks should align with international human rights standards and offer clear guidance on issues such as data protection, surveillance, and censorship.

Promoting digital literacy is another essential strategy that requires collaboration among various stakeholders. Academia, civil society organisations and businesses should work together to develop and implement digital literacy programs. These programs educate individuals about their rights, online safety and responsible digital citizenship. By doing so, people can make informed decisions, navigate the internet effectively, protect themselves from online threats and ultimately foster a culture of respect for internet freedom.

Technological innovation is crucial for enhancing internet freedom. This includes developing and promoting technologies like secure communication tools, privacy-enhancing technologies, and tools to circumvent censorship and surveillance. Encouraging open-source initiatives, fostering collaboration between academia and industry, and supporting startups focused on digital rights can drive technological innovation in favour of internet freedom.

Multi-stakeholder collaboration is yet another critical aspect of safeguarding internet freedom. Governments, civil society organisations, businesses, academia and the tech community should engage in regular dialogue and partnerships. Such collaborations enable the development of comprehensive solutions to internet freedom challenges. They can also help shape policies, and facilitate the sharing of best practices and the implementation of effective strategies while considering diverse perspectives and expertise.

Global cooperation and advocacy are also indispensable. Addressing internet freedom will require efforts at the international level. Governments and civil society organisations can collaborate to advocate for internet freedom in international forums, promote international standards and support initiatives that protect digital rights on a global scale. These collaborative efforts can help establish norms and principles that ensure internet freedom remains a global priority.

Conclusion

Africa's digital revolution is reshaping the continent's economy, society and concepts of internet freedom. The journey from late internet adoption to becoming a hub of digital innovation and connectivity has been remarkable. The growth of digital financial services, expansion of e-commerce and increased civic engagement online are all indicative of the transformative power of digitalization.

However, challenges persist, including the digital divide, data privacy concerns and the delicate balance between innovation and regulation. As Africa continues on its path of digital transformation, stakeholders must remain vigilant and proactive in safeguarding internet freedom and ensuring that the benefits of the digital economy are accessible to all.

The future of internet freedom in Africa will depend on the collective efforts of governments, civil society, businesses, academia and the tech community. By establishing robust legal frameworks, promoting digital literacy, fostering technological innovation, engaging in multi-stakeholder collaboration and advocating for global cooperation, Africa can navigate the complexities of the digital age while upholding the principles of freedom, privacy, and inclusion.

The writer is Kenya's Ambassador to Belgium, the European Union Mission, the Organization of African Caribbean and Pacific States and the World Customs Organization.

Disinformation in Africa: A threat to Internet Freedom and Democracy

« Ignorance leads to fear, fear leads to hate and hate leads to violence »
Averroes, Muslim philosopher (1126-1198)

Introduction

Over the last decade, the world has witnessed an exponential increase in the amount of disinformation[232] and hate speech, aided partly by recent developments in mobile technological advances and people's abilities to manipulate information. Anyone with an internet-enabled phone can collect and disseminate news and information. According to the World Bank, the percentage of individuals using the Internet in Sub-Saharan Africa has risen from 1% in 2000 to 36% in 2021.[233] By 2022, the number had risen to 40% (566 million) across Africa.[234] In 2022, there were at least 384 million social media users in Africa,[235] with Facebook leading in market share with 271 million users, followed by WhatsApp (200 million).[236]

Although disinformation is not a new phenomenon, several factors, including the rapid growth of social media usage, emerging media viability challenges, politicians' increasing influence on the media, the outbreak of the Covid-19 pandemic, and the involvement of mainstream media in spreading disinformation, have certainly influenced its growth.[237] Unfortunately, several countries have responded by enacting repressive laws and policies criminalising the spread of fake or false news and or misinformation and providing for excessing and harsh punishment,[238] thereby curbing people's right to freedom of expression and access to information.

Drivers of Disinformation in Africa

Across the continent, elections and armed conflicts have become key drivers of disinformation as governments have used both disinformation and the response to it to entrench themselves in power, shrinking civic space, and targeting opponents and critics. In West and Central Africa, targeted manipulation of information and heightened propaganda aimed at discrediting the activities of the powers in question not only damaged diplomatic ties but also encouraged the advance of rebel forces in these countries. Russia's mercenary military group, the Wagner Group has particularly been accused of using fake news outlets and influencers to influence public opinion in favour of their military in the region.[239]

In countries such as Cameroon, and the Democratic Republic of Congo politicians, armed groups, and their allies create tension by spreading disinformation to both manipulate public opinion and generate support for their extremist political views or groups and channelling the public anger to promote hate speech and disinformation.[240]

Blaise Pascal Andzongo Menyeng

232 *Defined by the African Centre for Strategic Studies as is the intentional dissemination of false information with the intent of advancing a political objective https://africacenter.org/spotlight/mapping-disinformation-in-africa/*

233 *Individuals using the Internet (% of population) - Sub-Saharan Africa https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZG*

234 *Internet use https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-internet-use/*

235 *Social media in Africa - statistics & facts https://www.statista.com/topics/9922/social-media-in-africa/?#topicOverview*

236 *Africa's WhatsApp economy is on the rise https://it-online.co.za/2023/03/02/africas-whatsapp-economy-is-on-the-rise/#:~:text=We%20live%20in%20a%20WhatsApp,plug%20into%20the%20global%20economy.*

237 *Combating Disinformation in Africa: Challenges and Prospects https://cipesa.org/2021/10/combating-disinformation-in-africa-challenges-and-prospects/*

238 *Disinformation Pathways and Effects on Democracy and Human Rights in Africa https://cipesa.org/2022/06/new-report-disinformation-pathways-and-effects-on-democracy-and-human-rights-in-africa/*

239 *How the Russian propaganda machine works in Africa https://www.lemonde.fr/en/international/article/2023/07/31/how-the-russian-propaganda-machine-works-in-africa_6074552_4.html*

240 *Disinformation and Hate Speech Continue to Fuel the Conflict in Eastern DR Congo https://cipesa.org/2023/05/disinformation-and-hate-speech-continue-to-fuel-the-conflict-in-eastern-dr-congo/*

In others such as Ethiopia, Ghana, Kenya, and Uganda, government functionaries have been reported to have resorted to using social media to spread disinformation as a way of influencing public opinion and voting decisions.[241] While disinformation campaigns and attempts at destabilising governments are often conceived and disseminated from outside African operations to local "franchised" influencers who are supplied content from a central source,[242] many African actors have also used disinformation strategies mainly for political purposes. According to a 2021 study by CIPIT, during the 2020 presidential elections in Ghana, the results revealed that the two main candidates used strategic campaigns on social networks. While Mahama's campaigns seemed to aggressively use robots (bots) and spread propaganda content, Akufo-Addo's campaign relied on authentic accounts (i.e. man-controlled).

Indeed, fake news has become such a dangerous media weaponization tool, by ignorance and many times as a pillar of geopolitics."[243] The growing trend of national political actors deploying targeted misinformation programs requires improved fact-checking capabilities in Africa as well as collaboration with social media organizations."[244]

Criminalisation of Free Speech

In many countries, governments have responded to the growing disinformation trends by weaponised disinformation laws to stifle legitimate expression while hampering access to critical and pluralistic information. In Cameroon for example, the country's Law on Cybersecurity and Cybercrime and the law governing electronic communications criminalises "false news", while Section 24 of Nigeria's Criminal Code Act and the Cybercrimes Act 2015 penalises "cyberstalking" and online publication of messages "he knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another." In Senegal, section 255 of the Penal Code[245] prohibits the publication, dissemination, disclosure, or reproduction, by any means whatsoever, of false news prescribing a penalty of imprisonment for a term between one and three years upon conviction. In Zambia, section 67 of the Penal Code[246] prohibits the publication either orally or in writing, of any false news, providing for a three-year term of imprisonment upon conviction.

During the COVID-19 pandemic, several countries passed policies and regulations that criminalised the publication of COVID-19-related information. For example, in April 2020, Algeria passed a bill amending its Penal Code that criminalises the broadcast of "fake news" that is deemed to be harmful to "public order and state security."[247] On the other hand, Regulations 11(5) of South Africa's Department of Cooperative Governance and Traditional Affairs (COGTA) March 2020 Regulations Issued In Terms of Section 27(2) of the Disaster Management Act, 2002, states that any person who "publishes any statement, through any medium, including social media, with the intention to deceive any other person about COVID-19; COVID-19 infection status of any person; or any measure taken by the Government to address COVID-19, commits an offence and is liable on conviction to a fine or imprisonment for a period not exceeding six months, or both such fine and imprisonment."[248]

241 *Disinformation Pathways and Effects on Democracy and Human Rights in Africa https://cipesa.org/2022/06/new-report-disinformation-pathways-and-effects-on-democracy-and-human-rights-in-africa/*

242 *Mapping Disinformation in Africa https://africacenter.org/spotlight/mapping-disinformation-in-africa/*

243 *The only weapon against fake news: knowing how to seek, question, reconnect with the human process, doubting and checking, https://fr.sputniknews.africa/20210701/la-seule-arme-contre-les-fake-news-savoir-chercher-questionner-renouer-avec-le-processus-humain-1045819514.html*

244 *Increase in internal disinformation in Africa, https://africacenter.org/fr/spotlight/hausse-de-la-desinformation-interieure-en-afrique/*

245 *Senegal / Coronavirus: Abdoulaye Mbaye Pékh lectured for spreading fake news https://cio-mag.com/ssenegal-coronavirus-abdoulaye-mbaye-pekh-sermonne-pour-diffusion-de-fake-news/&prev=search&pto=aue*

246 *Penal Code http://www.parliament.gov.zm/sites/default/files/documents/acts/Penal%20Code%20Act.pdf*

247 *Algeria criminalises 'fake news' to protect 'state security' https://www.aljazeera.com/news/2020/04/algeria-criminalises-fake-news-protect-state-security-200422201042011.html*

248 *The Regulations https://altadvisory.africa/wp-content/uploads/2020/03/COVID-19-Regulations-issued-in-terms-of-the-Disaster-Management-Act-2002-18-March-2020.pdf*

In March 2020, Zimbabwe also introduced the Statutory Instrument 83 of the Public Health (Covid-19 Prevention, Containment and Treatment) (National Lockdown) Order, 2020 which criminalised the publication or communication of false or fake news about "any public officer, official or enforcement officer involved with enforcing or implementing the national lockdown in his or her capacity as such, or about any private individual that has the effect of prejudicing the State's enforcement of the national lockdown" under section 14.[249]

Impact of Disinformation on Democracy and Internet Freedom in Africa

Progressive democracy thrives when people have access to accurate and credible information that enables them to make informed decisions. However, disinformation however hampers citizens' ability to make informed decisions, and affects the right of citizens to hold individual opinions without interference.[250] It also has a corrosive effect on social trust, critical thinking, and citizens' ability to engage in politics fairly—the lifeblood of a functioning democracy, [251] particularly as it has the potential to hijack the political discourse and undermine elections by limiting access to credible, factual, and pluralistic information about candidates, parties, and issues.[252] In addition, many social media users find themselves used as unwitting foot soldiers to amplify disinformation or conspiracy theories online due to their limited capacity to correctly verify and contextualise the information.[253]

The situation is made worse by the different countermeasures, such as criminalises of publication of fake/false news and internet shutdowns, that have been adopted by governments under the pretext of combating disinformation. Many citizens end up disengaging from online public discourses for fear of reprisals due to the excessive punishments they would be subjected to if found guilty and the denial of access to critical information during internet shutdowns.

Reflections on the Future of Disinformation in Africa

Cases of disinformation are projected to increase in Africa as different players seek to influence the continent's narrative. Reports show that in recent years, dozens of carefully designed campaigns have pumped millions of intentionally false and misleading posts into Africa's online social spaces,[254] and this is not about to change.

And while combating disinformation remains a complex and ongoing challenge, it requires a comprehensive and coordinated approach. African countries must increase their collaboration by promoting innovative and effective approaches, improving legislation, guaranteeing freedom of expression, and strengthening media and information literacy.

249 *Statutory Instrument 83 of 2020 https://www.veritaszim.net/sites/veritas_d/files/Pub%20Health%20Lockdown%20Order%20%28SI%2083%2C2020%29%20Latest%20Consolidation.pdf*

250 *Disinformation Pathways and Effects on Democracy and Human Rights in Africa https://cipesa.org/2022/06/new-report-disinformation-pathways-and-effects-on-democracy-and-human-rights-in-africa/*

251 *Mapping Disinformation in Africa https://africacenter.org/spotlight/mapping-disinformation-in-africa/*

252 *Disinformation Pathways and Effects on Democracy and Human Rights in Africa https://cipesa.org/2022/06/new-report-disinformation-pathways-and-effects-on-democracy-and-human-rights-in-africa/*

253 *Disinformation In A Digital Age – What Impact On African Democracies? https://democracyinafrica.org/disinformation-in-a-digital-age-what-impact-on-african-democracies/*

254 *Mapping Disinformation in Africa https://africacenter.org/spotlight/mapping-disinformation-in-africa/*

More specifically, both governments and civil society need to invest in media and information literacy (MIL) for the public as it can enhance critical functions, critical thinking, and proper decision-making and can ensure what Len Masterman calls 'critical autonomy. It also allows the public to be aware of digital issues by knowing how to use the Internet, and how to assess the content before liking and sharing. A 2023 study conducted in four African countries, showed that media literacy training had the capacity to transform informational practices by enabling people to understand the principles and techniques guiding the production of reliable information and distinguish between real and false facts.[255]

In addition, fact-checking remains a necessity for Internet users and journalists, to enable them to verify the reliability of the information. Today, many organisations including Africa Check, BBC Media Action, Arij, Ijinet and others, are working on promoting verification for collective interest. Governments will remain an important and even a key factor in ensuring an effective fight against fake news. In Libya, some journalists are training on fact-checking through a platform called "Maa" created In October 2019. Also, the Deutsche Welle Academy in their "Media in Libya - Stability through Reconciliation" project is building the capacity of Libyan journalists to identify false news, verify allegations and assess the credibility of sources and the media.[256]

Governments should also work towards appealing repressive laws that criminalise the publication of false news and information.

The third strategy is to strengthen journalists' skills in fact-checking. To date, apart from continental fact-checking bodies such as Africacheck, many fact-checking bodies are developing in many African countries such as Congocheck, Guinea Check, Data Cameroon, Ghanafact, etc. Therefore, it will be necessary to strengthen existing programmes in more countries. For example, Facebook's fact-checking programme is present in Burkina Faso, Cameroon, Côte d'Ivoire, Democratic Republic of Congo, Ethiopia, Ghana, Guinea Conakry, Kenya, Nigeria, Somalia, South Africa, Tanzania, Uganda, Zambia, etc. Talk Peace has projects in Cameroon, while Désinfox Afrique by CFI is present in Benin, Burkina Faso, Cameroon, Chad, Côte d'Ivoire, Niger, and Senegal.

The fifth strategy is the facilitation of public engagement. For example, in South Africa, the development of an online disinformation reporting platform enabled citizens to alert authorities to possible opinion manipulation on elections on social media. Also in Tunisia, the Independent High Authority of Audio-visual Communication (HAICA) contributed to the establishment of a platform that facilitated the detection, from collaborative work with many journalists, of false information during the 2019 elections. These examples could be replicated in other African countries to maximize the chances of disinformation being reduced to its simplest expression. They also highlight the need for African governments to express a real willingness to promote the right to information and set a clear strategy to combat fake news.

Blaise Pascal ANDZONGO MENYENG, MIL specialist, founder of Cameroonian Association for Media Education, Africa representative of UNESCO MIL Alliance

Rima ROUIBI, Lecturer at Higher National School of Journalism and Information Sciences (ENSJSI), Algiers (Algeria), Head of Media Literacy Unit.

255 *Andzongo (2023)*
256 *TSC https://tsc.org.ly/?page_id=21*

Case Studies

Algeria

On 22nd February 2019, an appeal from an anonymous source spread online, calling for a demonstration against President Abdelaziz Bouteflika's fifth term in Office. This changed Algerian history as Algerians became aware of their collective strength.[257] The political context in Algeria since the popular mobilisation (Hirak),[258] on 22nd February 2019, not only led to a change in governance following the resignation of President Bouteflika on 2nd April 2019 but also to developments in the use of social networks.

The lack of trust between citizens and media currently labelled as the media of shame, has strengthened the power of social networks. In April 2019, 800-1,000 fake news articles were resurrected by the co-admins of the Fake news page DZ, Nassim and Lokman, who were two students residing in France. Their aim was "enlightening the Algerian public, in a sensitive context". During the Hirak and COVID-19 pandemic, there was widespread disbelief about the reality of the pandemic.

Since its independence, Algeria has been confronted with many difficult situations. Some of these explain the evolution of fake news within the society. Events at Ghardaia showed a dangerous spread of fake news, as riots between Ibadits and Chaamba had set the city on fire for months[259] Five years later, wildfires in Tizi Ouzou[260] and the exploitation of hate speech between Arabs and Kabyles, caused the death of a younger man "Djamel Ben Smail". Also, the political conflict with Morocco has introduced hatred between Algerians and Moroccans. Nuances around culture, policy, and religion are used as excuses "to justify" the rise of rising hate.

According to Facebook's Inauthentic Behaviour Report, Algeria was a target of fake news and the investigations revealed suspected coordinated inauthentic behaviour in the region. Accordingly, 130 Facebook accounts, 221 Pages, 35 groups, and 29 Instagram accounts in Algeria that targeted primarily domestic audiences and were linked to individuals in Algeria, including some who worked for the 2019 campaign of the current President were removed.[261]

Morocco:

The advent of fake news and hate speech in Morocco is not recent. An example is the case of "Abu Naim", a Salafist known for his extremist positions. He was arrested for publishing a video that was cited as incitement to hatred and violence", with a fatwa against the Moroccan Kingdom and its Institutions after announcing the closing of mosques for worshipers.

It's important to underscore that since the beginning of the political conflict between Algeria and Morocco, hate speech has been common across both countries. Morocco was the target following a broadcast of a documentary on prostitution in the Kingdom by the national Algerian television channel. Also, some Moroccan journalists openly showed their happiness after a wildfire that hit the northern region of Algeria. Internet users in Morocco recently posted fake footage on social media showing the damage caused by the earthquake. It is possible some are simply looking for the buzz or trying to reach a maximum number of followers.

Therefore they are exploiting the sadness and human tragedy, a phenomenon Lippmann called "whistle the emotion". "Times of crisis are always a heyday for disinformation, misinformation and conspiracy myths," according to Lena Frischlich, a media psychologist and an expert on conspiracy theories.[262] The tragic earthquake in Morocco on 09th September 2023, which left at least 2,900 victims, is a perfect example that characterises the spread of fake news. In the aftermath of the natural disasters, there were videos showing that a "laser weapon" was used to trigger the earthquake. Joscha Weber notes that the relationship between fiction and fake news on social media is strong and difficult to expose and contain.[263]

257 *Filiu 2019*

258 *Hirak, Arabic word for mobilization. This qualifier has been used to designate, including in the French and English languages, socio-political mobilization in Algeria. During the first weeks of the political protest, this term was transcribed in the form of Harak. The first journalistic, academic and militant writings transcribe the word with the letter "a" rather than the letter "i".*

259 *Rouibi, 2016*

260 *Is an Algerian area located 30 km south of the Mediterranean coast, and 100 km east of the capital Algiers.*

261 *June 2021 Coordinated Inauthentic Behavior Report https://about.fb.com/news/2021/07/june-2021-coordinated-inauthentic-behavior-report/*

262 *Fact check: Morocco earthquake not caused by 'laser weapon' https://www.dw.com/en/fact-check-morocco-earthquake-not-caused-by-laser-weapon/a-66799897*

263 *Fact check: Morocco earthquake not caused by 'laser weapon' https://www.dw.com/en/fact-check-morocco-earthquake-not-caused-by-laser-weapon/a-66799897*

Communication Interception and Surveillance in Africa: Trends

Introduction

Communication interception and surveillance have surfaced at the top of the policy and academic agenda in the past two decades in Africa. A sizeable number of research reports have shined the spotlight on the deleterious impact of communication interception and surveillance on the enjoyment of inalienable human rights and freedoms both online and offline including the right to privacy, freedom of expression, the right of access to information and freedom of assembly and association.

In this essay, focus is placed on the various manifestations of communication interception and surveillance in Sub-Saharan Africa. Communication interception, refers to ways of listening to the calls made on a telephone, or opening and reading the contents of a target's emails, mobile phone messages, social media, bank accounts, et cetera. In most countries, surveillance and interception is enabled by laws which are often applied abusively. Communication surveillance denotes the monitoring, interception, collection, preservation, and retention of information that has been communicated, relayed, or generated over communications networks to a group of recipients by a third party.[264]

As the triple societal processes of digitisation,[265] platformisation,[266] and datafication[267] have gathered pace, African governments have been quick to acquire and deploy smart surveillance technologies. The mass permeation of digital technologies in everyday life has created a conducive environment for the algorithmic automation of surveillance. Furthermore, the digitisation of telephony and correspondence that accompanied mobile phones and internet email and messaging, has made it possible to automate the search for keywords in real-time communications.

Compared to the analogue communication era, it is now easier for state agencies to conduct mass surveillance and interception of all citizens' communications and to micro-target individuals for in-depth surveillance that draws data from mobile calls, SMS, internet messaging, GPS location and financial transactions in real-time. The advent of digital surveillance has also seen the entry of new surveillance actors. These include social media companies, telecommunication operators, and a whole host of internet intermediaries.

Most of the smart surveillance technologies supplied by companies predominantly from the USA, China, Europe, and Israel have been used to monitor opposition politicians, human rights defenders, journalists, trade unionists, and civic activists. This is despite the fact that Africa, compared to other continents, faces relatively insignificant threats of organised terrorism, a common justification for intense surveillance. This has significantly contributed to a "chilling effect" and the closure of civic space.

Dr Admire Mare

264 Communication Surveillance, https://privacyinternational.org/explainer/1309/communications-surveillance

265 This is the process of converting information into a digital format.

266 It refers to the penetration of infrastructures, economic processes and governmental frameworks of digital platforms in different economic sectors and spheres of life, as well as the reorganisation of cultural practices and imaginations around these platforms.

267 This denotes a technological trend turning many aspects of our life into data which is subsequently transferred into information realised as a new form of value.

Countries such as Angola, Botswana, Cameroon, Ethiopia, Lesotho, Kenya, Nigeria, Malawi, Zambia, and Zimbabwe have resorted to conducting surveillance, intercepting private communications, and restricting access to the internet.[268] Some of these countries have justified their actions on the basis of attempting to combat organised crimes and terrorism and addressing threats against public order. Even more startling is that surveillance in Africa is taking place in both democratic and authoritarian contexts. Countries such as Namibia and South Africa, which are often touted as the "paragons of liberal democracy and constitutionalism"[269] have been found on the wrong side of the law. This has raised concerns about the gradual retreat in what think tanks and foundations have called "digital authoritarianism".

The abuse of surveillance is more prevalent in authoritarian regimes compared to democratic settings where levels of accountability and transparency are relatively higher.[270] In authoritarian contexts, state institutions are generally weak and are often captured by seating governments the political elite.[271]

The Historical Context of Communication Interception and Surveillance in Africa

Surveillance predates the digital age. It has always been part and parcel of human relations since time immemorial.[272] In the African context, surveillance was introduced by colonial administrations and was retained by post-colonial administrations. The process of watching over "the other" has been implicated in the categorisation and discrimination of black bodies during the colonial era.

It has been refined and repurposed by current African governments to pursue narrow political, economic, military, gender, and ethnic power interests. In most cases, communication interception and surveillance in Africa are often justified under the pretext of protecting citizens from terrorism, organised crime, and pandemic threats such as ebola, COVID-19 and meningitis. Surveillance has also been deployed by African governments to track the movements of opposition politicians, investigative journalists, human rights defenders and lawyers.[273]

Under regional and international human rights instruments, governments have an obligation to respect, protect and fulfil human rights and freedoms.[274] Notwithstanding the fact that most of the African countries are signatories of regional and international treaties, the majority continue to engage in illegal communication surveillance, interception of private communications, and restrictions in flagrant violation of human rights law.

African governments may impose restrictions on fundamental human rights In line with international human rights law standards. To this end, the UN Special Rapporteur on the Right to Privacy's Draft Legal Instrument on Government-led Surveillance and Privacy[275] provides a clear guide for drafting and assessing the compliance of surveillance legislation with international human rights law. Likewise, Principle 41 of the Declaration of Principles on Freedom of Expression and Access to Information (2019) is explicit in its articulation of circumstances under which surveillance is permissible. It provides that:

"States shall only engage in targeted communication surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim."

268 *Munoriyarwa, A. and Mare, A. (2023). Digital Surveillance in Southern Africa: Policies, Politics and Practices', Cham: Springer; Roberts, T.; Mohamed Ali, A.; Farahat, M.; Oloyede, R. and Mutung'u, G. (2021) Surveillance Law in Africa: a review of six countries, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.059*

269 *Wasserman, H. (2010). Freedom's just another word? Perspectives on media freedom and responsibility in South Africa and Namibia. International Communication Gazette, 72(7), 567–588.*

270 *Wang, J., Hu, Z.J., & Galligan, D. (2022). The era of digital surveillance: Authoritarianism vs. democracy? Oxford Global Society Report. See: https://oxgs.org/wp-content/uploads/2022/10/digital-surveillance-authoritarianism-vs-democracy.pdf*

271 *Munoriyarwa, A. and Mare, A. (2023). Digital Surveillance in Southern Africa: Policies, Politics and Practices', Cham: Springer.*

272 *Ibid.*

273 *Mare, A. (2016). 'A qualitative analysis of how investigative journalists, civic activists, lawyers and academics are adapting to and resisting communications surveillance in South Africa'. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/duncan_2_comm_surveillance.pdf*

274 *Hunter, M. and Mare, A. (2020). Patchwork For Privacy: Communication Surveillance In Southern Africa. MPDP: Johannesburg; Roberts, T.; Mohamed Ali, A.; Farahat, M.; Oloyede, R. and Mutung'u, G. (2021) Surveillance Law in Africa: a review of six countries, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.059*

275 *United Nations. (2018). Draft Legal Instrument on Government-Led Surveillance and Privacy (accessed 7 August 2023).*

All these international and regional instruments concur that communication surveillance is only justifiable when it is lawful, necessary for the protection of legitimate purposes, based on proportionate aim, and complies with the principle of non-discrimination both in their design and application.

Nevertheless, most surveillance laws in Africa are outdated and not aligned with the necessary and proportionate principles. Many African countries have enacted laws that permit surveillance, mandate telecommunication intermediaries to facilitate the interception of communication, impose mandatory SIM card registration requirements, 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.[276]

A combination of surveillance-enabling legislation and opaque procurement processes[277] involved in the acquisition and deployment of surveillance technology has created fertile ground for the creation of surveillance states in Africa.[278] This is further compounded by the lack of effective oversight over surveillance activity. In most cases, the activities of security agents, their budget lines, and contractual obligations are shrouded in secrecy which has undermined accountability and transparency.

Besides state actors, non-state actors, including telecommunication operators, have also joined the bandwagon of communication surveillance and interception in Africa. Recently, MTC Namibia, a private telecommunication company in Namibia, refused to acquiesce to a directive from the Communication Regulatory Authority of Namibia (CRAN) to discontinue capturing clients' biometric data in the absence of a data-protection legislative framework.[279] The telecommunication operator has continued to collect fingerprints and take face photos of subscribers for SIM registration in clear violation of the Communication Act of 2009.

Overview of the Communication Interception and Surveillance Trends in Africa

Over the last decade, Africa has witnessed concerning trends as far as the normalisation and rationalisation of communications interception and surveillance are concerned. our trends have emerged, that is the digital turn in surveillance, legalisation of surveillance, roll out of data collection programmes, and the acquisition of surveillance technologies. Before unpacking these trends, it is noteworthy to highlight that African post-colonial administrations are spending billions of dollars annually to conduct surveillance on their own citizens.[280] Most of the surveillance technologies are supplied by companies based in Europe, North America, the Middle East, and Asia.

276 *CIPESA, "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa," https://cipesa.org/wp-content/files/reports/Privacy-Imperilled-Analysis-of-Surveillance-Encryption-and-Data-Localisation-Laws-in-Africa-Report.pdf; CIPESA, "Digital*

277 *Authoritarianism and Democratic Participation in Africa," https://cipesa.org/wp-content/files/briefs/Digital-Authoritarianism-and-Democratic-Participation-in-Africa-Brief-.pdf Munoriyarwa and Mare (2023)*

278 *These are countries where the government engages in pervasive surveillance of large numbers of its citizens and visitors.*

279 *Namibia's Biometric Verification Travesty https://www.namibian.com.na/namibias-biometric-verification-travesty/*

280 *Jili, B. (2020) 'Surveillance Tech in Africa Stirs Security Concerns' Africa Center for Strategic Studies (accessed 1 July 2021); Roberts, T.; Mohamed Ali, A.; Farahat, M.; Oloyede, R. and Mutung'u, G. (2021) Surveillance Law in Africa: a review of six countries, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.059*

The Digital Turn in Surveillance

Like elsewhere, the African continent has witnessed a shift from traditional to digital forms of surveillance.[281] This digitisation of surveillance has been accompanied by the heavy use of digital technologies to monitor and track the movements of citizens. This does not mean that traditional forms of surveillance are no longer being deployed. In some cases, the confluence of traditional and digital surveillance has brought into existence hybrid surveillance infrastructures.[282] This has enabled surveillance actors to monitor offline and online forms of communication.

Given the rapid advances in digital technologies, as evidenced by the use of mobile phones, social media, artificial intelligence, algorithms and smart devices, digital surveillance in Africa has expanded in terms of breadth and scope. Research has shown that most African countries are deploying spyware, drones, and video surveillance (CCTV), as well as social media monitoring, mobile phone location tracking, and the hacking of mobile phones, messaging, and email applications.[283]

In light of the above, five communication interception and surveillance categories in Africa can be identified. These include internet interception, mobile phone interception, social media monitoring, public space surveillance, and biometric digital IDs. Internet interception often relates to legal and illegal access to the signal, collecting the signal, and exfiltrating the signal. Most of the time, national governments work in partnership with internet access and service providers to intercept communication data and metadata. Social media monitoring consists of using invasive technologies to track and categorise communication between users on platforms such as WhatsApp, Meta (Facebook), X (Twitter), Instagram and YouTube.

Public space surveillance relates to the use of closed-circuit television (CCTV) surveillance cameras to track the movements of people in public spaces such as streets, shopping malls and public offices. The roll-out of biometric digital IDs has been accompanied by unprecedented mass data collection of personal information. Large amounts of personal data such as name, birth date, place of birth, gender, eye colour, height, current address, photograph, and other information are linked to the ID numbers and stored in a centralised databases. Geolocation tracking, video surveillance and facial recognition software built on top of large biometrics collections can further enable pervasive surveillance systems.[284]

Currently several African countries have deployed communication interception technologies. In 2021, Morocco, Rwanda and Togo were reported as users Pegasus software,[285] while Nigeria, Kenya, Botswana, Equitorial Guinea, Morocco, Zimbabwe and Zambia were reported to be using Circles.[286] These invasive technologies are being used for covert spying on citizens' emails, instant messaging, browsing and search histories. Many African governments require internet service providers to save all citizens' internet communications and metadata so that government agents can access it upon production of a judicial warrant. Research in Namibia and South Africa has shown that communication surveillance often takes place outside of the legal framework.[287]

Mobile phone interception technologies are also popular among African governments. These technologies are generally used for covert spying on citizens' phone calls, text messages, instant messaging or internet communications using a mobile phone. Because more than 90% of all internet access is through mobile internet access, several African governments have acquired mobile malware or IMSI Catchers[288] for surveillance purposes.

281 *Munoriyarwa and Mare (2023)*

282 *ibid*

283 *ibid*

284 *Electronic Frontier Foundation. Mandatory National IDs and Biometric Databases. Retrieved from https://www.eff.org/issues/national-ids*

285 *Pegasus Lands in Africa https://www.theafricareport.com/110214/morocco-rwanda-togo-how-involved-is-africa-in-pegasus-gate/*

286 *The seven African governments using Israeli cyberespionage tools https://africanarguments.org/2021/02/the-seven-african-governments-using-israeli-cyberespionage-tools/*

287 *Hunter, M. and Mare, A. (2020). Patchwork For Privacy: Communication Surveillance In Southern Africa. MPDP: Johannesburg; Mare, A. (2019). Communication Surveillance in Namibia: An Exploratory Study. Media Policy and Democracy Project. See: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/namibia_report_3rd_pages.pdf*

288 *According to Privacy International, 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 number that is connected to a SIM card. See https://privacyinternational.org/explainer/4492/how-imsi-catchers-can-be-used-protest*

In a continent where social media penetration rates continue to surge, it is unsurprising that there is a huge market for social media surveillance technologies in Africa. Security agents are profiling, categorising and monitoring social media accounts of their targets on platforms such as Twitter, Facebook, YouTube, Instagram, and TikTok. Social media data has been used to surveil citizens for political marketing and disinformation purposes in Nigeria and Kenya.[289] The Cambridge Analytica scandal is a case in point. In South Africa, Bell Pottinger, a UK company, was found to have used social media to manipulate political opinions at the height of the state capture scandal.[290]

Legalisation of Mass Surveillance

Some African countries have enacted mandatory SIM card registration laws which in essence create a surveillance target database. For instance, the Namibian Communications Act of 2009 requires telecommunications operators to collect basic information such as names, dates of birth, addresses, and copies of identification documents to register a SIM card. Countries such as Botswana, the Democratic Republic of Congo, Eswaini, Kenya, Tanzania, Uganda, Zambia and Zimbabwe have also enacted SIM card registration laws.

In a study published in 2020, it was revealed that at least 25 African countries have enacted a law to authorise and regulate the interception of communications.[291] Some of these laws place powers under the authority of a judge, others with the executive, and some take a "hybrid" approach where the authority is shared between the judiciary and the executive.

Besides laws focusing on interception of communications, electronic transactions, protection of personal information and cyber-security-related laws, the absence of data protection laws has also facilitated increased state surveillance across the continent. So far, 36 African countries have adopted specific personal data protection laws.[292] Research shows that "violations of privacy rights by state and non-state actors are on the rise".[293]

Rollout of Data Collection Programmes

The African continent has also been reduced to a 'safe cities' experiment hub. The 'safe cities' initiative is dominated by Chinese and American companies. For instance, China has offered several African governments loans to buy surveillance technology packages from Chinese companies such as Huawei and ZTE.[294] These packages often include the installation of CCTV cameras that have facial recognition and car licence plate recognition capabilities. It also includes a command-and-control rooms and data centres from which police and security forces can surveil citizens moving around public space in real-time.

Zambia and Mauritius are classic examples of the 'safe cities' experiment in Africa.[295] The Mauritius Safe City Project (MSCP), financed by a loan from China, has from the outset been shrouded in opacity.[296] Besides Zambia and Mauritius, countries such as Ghana, Mauritius and Morocco have spent millions of dollars on mass surveillance "safe cities" infrastructure from China. This is despite the fact that "safe" and "smart" city systems carry a plethora of potential security and human rights risks. These projects are often marketed as "hubs of safety and security" yet involve the subtle monitoring of people through data mining, facial recognition, and other kinds of large language models (LLMs).

289 *Ekdale, B. and Tully, M. (2020, January 9). How the Nigerian and Kenyan media handled Cambridge Analytica. The Conversation. See: https://theconversation.com/how-the-nigerian-and-kenyan-media-handled-cambridge-analytica-128473*

290 *How Bell Pottinger, P.R. Firm for Despots and Rogues, Met Its End in South Africa https://www.nytimes.com/2018/02/04/business/bell-pottinger-guptas-zuma-south-africa.html*

291 *Mavedzenge, J. (2020).*

292 *Hogan Lovells, "Recent developments in African data protection laws - Outlook for 2023," https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45#:~:text=Here%2C%20the%20authority%20in%20charge,and%2C%20until%202022%2C%20Nigeria*

293 *CIPESA. (2021). Mapping and Analysis of Privacy Laws in Africa. See: https://cipesa.org/wp-content/files/briefs/Mapping-and-Analysis-of-Privacy-Laws-in-Africa-2021.pdf*

294 *Dahir, A.L. (2019, September 18). Chinese firms are driving the rise of AI surveillance across Africa. Quartz. https://qz.com/africa/1711109/chinas-huawei-is-driving-ai-surveillance-tools-in-africa; Gagliardone, I. (2020). The impact of Chinese tech provision on civil liberties in Africa. SAIIA Policy Insights No 99, December 2020. See: https://saiia.org.za/research/the-impact-of-chinese-tech-provision-on-civil-liberties-in-africa/*

295 *Munoriyarwa and Mare (2023).*

296 *Kasenally, R. (2022). The Trappings of the Mauritius Safe City Project. Hoover Institution Press. https://www.hoover.org/research/trappings-mauritius-safe-city-project*

Another arena where communication interception and surveillance have started to thrive in Africa relates to the roll-out of biometric ID technologies. These technologies have encroached into the realm of communication surveillance in ways that were unimaginable in the last few years. Many African governments are implementing compulsory digital ID systems using biometric fingerprints, iris scans, or facial recognition technologies. From immigration officials to telecommunication operators, biometric ID technologies have become the latest fashionable trend in the surveillance ecosystem. This "biometrification of everyday life"[297] has a significant impact on the protection and enjoyment of civil liberties.

Most of these digital ID systems are often linked to citizens' mobile phones and to their banking or mobile money accounts. In some African countries, a biometric ID has become an important requirement to obtain a passport, driving licence, healthcare services, social protection payments, and other government services or entitlements.

The Acquisition of Surveillance Technologies

Although African governments have the power to resist the acquisition and deployment of surveillance technologies marketed by companies from North America, Europe and Asia, it can be argued that most of them are willing clients in these opaque transactions. An exception is Malawi, which rejected the "safe city" surveillance package offered by China.

The continent has become a huge market for surveillance companies from the Global North. For instance, the United States of America and the United Kingdom are the main suppliers of social media surveillance technologies and "political marketing" consultancy services in Africa. Germany, Italy and Israel are the major exporters of mobile phone hacking malware. Britain exports fake cell towers (IMSI Catchers) to spy on mobile calls and messaging.

Impact on Internet Freedom in Africa

The increasing cases of interception of communication and surveillance in Africa have led to wanton violations of citizens' right to privacy. It has also affected the enjoyment of several human rights and freedoms as enshrined in national, regional, and international instruments. Cases of digital surveillance have adversely affected African countries with fragile democracies, constrained civil society, weak legal protections, and existing restrictions on political freedoms and civic space.[298]

In its various manifestations, communication interception and surveillance pose enormous threats to the realisation and enjoyment of digital rights. It affects the ability of individuals and organisations to organise, mobilise, and engage in democratic processes. It contributes to the curtailment of rights to freedom of expression, access to information, association and assembly.

The fear of repercussions associated with surveillance curtails the rights of individuals who have been victims of surveillance to freely express themselves. It nurtures an uncomfortable climate of chilling effects, which leads to self-censorship, political resignation, and apathy.

297 *Munoriyarwa and Mare (2023).*
298 *CIPESA (2021). 2021 State of Internet Freedom in Africa*

Reflections on Communication Interception and Surveillance futures in Africa

What will our African surveillant futures look like? There is no doubt that as digital technologies continue to evolve, there is a high probability that communication interception and surveillance in hyper-datafied societies will also become more pronounced. This is already evident in the ways in which large language models, artificial intelligence (AI), facial recognition, and machine learning technologies are implicated in digital surveillance practices in Africa. Governments and corporates are increasingly sorting and sifting huge datasets in order to identify, monitor, track, regulate, predict and prescribe.

Surveillance in Africa could be punctuated by the transnational tracking and monitoring of communication data and metadata across space and time. These practices could see more African countries investing in mobile phone tracking, surveillance cameras, online monitoring, Global Positioning System and RFID tracking and intelligent video analytics. Investments in face, object and event recognition capabilities accompanying the roll-out of AI technologies could result in proactive, real-time surveillance of citizens in Africa. As already mentioned, the gateway to these transnational surveillance imaginaries will be an overreliance on biometrics, installation of CCTV cameras in public spaces, popularisation of 'safe cities' projects and strategic deployment of facial recognition technologies. Therefore, ensuring respect for human rights as these developments unfold will be critical to prevent the erosion of human rights in the continent.

The essay makes the following key recommendations:

- Governments should repeal, amend, or review existing laws, policies, and practices on interception of communication and surveillanceto ensure compliance with regional and international human rights standards.
- Judiciaries, Parliaments and Data Protection Authorities should provide comprehensive and independent oversight overthe state and its agencies in their surveillance operations.
- The media should investigate, document and publish stories highlighting the risks presented by communication interception and surveillance to human rights.
- The media should spotlight suppliers, customers, and the users of surveillance technologies.
- Academia should conduct evidence-based research on communication interception and surveillance and its human rights impact.
- Academics should partner with civil society organisations in collecting evidence-based information and advocacy on interception of communication and surveillance in Africa.
- Civil society organisations (CSOs) should investigate, document, and expose human rights violations arising from communication interception and surveillance.
- CSOs should engage in strategic public interest litigation to challenge surveillance laws, measures and practices.
- CSOs should enhance their cybersecurity and data protection measures.
- Intermediaries should regularly publish, update, and widely disseminate privacy policies and transparency reports regarding surveillance.
- Intermediaries should put in place privacy and data protection policies and inform users about the measures taken to protect their right to privacy.
- Vendors of surveillance technologies should conduct human-rights assessments and inculcate due diligence measures in compliance with the UN Guiding Principles on business and Human Rights.

Admire Mare is an Associate Professor in the Department of Communication and Media at the University of Johannesburg, South Africa.

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