State of Internet Freedom in Africa 2019

Mapping Trends in Government Internet Controls, 1999 - 2019

September 2019

CIPESA

Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support of various partners.

This research documents the trends in government internet controls, 1999-2019 in select African countries, tracking key trends in recent years, analysing the key risk factors, and mapping notable developments on data protection and privacy legislation and violations, and users' understanding of protecting their privacy online. The study covers Bostwana Burundi, Cameroon, the DRC, Ethiopia, Kenya, Malawi, Nigeria, Rwanda, Senegal, Tanzania, Uganda, and Zimbabwe. The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa.

Table of Contents

1 Introduction

Internet freedom in Africa has been on the decline over the past years with several countries continually adopting aggressive and sophisticated measures that curtail internet freedoms. Most of the governments of the affected countries have turned internet shutdowns into a tool of political hegemony and control for political stability.[1] In fact, governments are more than ever before, using digital technologies to surveil, censor and suppress fundamental and basic freedoms of their people through among others censorship, filtering, blocking, throttling and internet shutdowns.[2] The curtailment and regression has been primarily characterised by the proliferation of retrogressive and repressive policies and laws that criminalise online communication and dissent, such as in Tanzania,[3] Rwanda,[4] and Malawi.[5]

For instance, some governments such as Kenya have used the need to control "fake news" as an excuse to introduce restrictive laws, while others such as Tanzania and Uganda, are employing Computer Misuse laws to arrest and prosecute government critics, on charges of "offensive communication" and cyber harassment. On August 1, 2019, Ugandan Dr Stella Nyanzi, an academic and human rights activist, was convicted for cyber harassment (and acquitted of offensive communication) against president Yoweri Museveni under sections 24(1) and (2)(a) of the Computer Misuse Act 2011.[6] Likewise, a number of people have been charged in Tanzania for "insulting" President Magufuli on social media under section 16 of the Cybercrime Act, 2015, which essentially prohibits the publication of false information.[7] The continued surveillance of the public with limited oversight, in addition to the increased surveillance capacity of governments, and the interception of communication including critics and human rights activists threaten internet freedom. These measures have been coupled with regulatory control of the internet, including the now widespread and restrictive measures such as censorship, filtering, blocking, throttling and internet shutdowns evident in several countries.

It should be noted that governments have over time embraced the integration of Information Communication Technologies (ICT), including internet-powered applications and services, in government functions and operations. This has partly revolutionised service delivery by partly promoting government efficiency. Further, several governments are rapidly introducing digitalisation, e-government and digital identity programmes that require citizens to provide detailed personal information, including biometrics for voters' cards, identity cards, and driver's licences, among others. This has been in addition to the requirements for SIM card registration. While sections of society welcome some of these measures as necessary to enhance security and government service delivery, they enhance African states' surveillance capacity which in turn affects citizens' digital rights such as privacy, expression and access to information.

---

[1] Digital Authoritarianism: Human Rights, Geopolitics and Commerce
http://ecipe.org/wp-content/uploads/2014/12/digital-authoritarianism-human-rights-geopolitics-and-commerce.pdf
[2] The Long View of Digital Authoritarianism https://www.newamerica.org/weekly/edition-254/long-view-digital-authoritarianism/
[3] Tanzania Issues Regressive Online Regulations, available at https://cipesa.org/2018/04/tanzania-enacts-regressive-online-content-regulations/
[4] Law Governing ICT in Rwanda, available at https://minict.gov.rw/fileadmin/Documents/Mitec2018/Policies___Publication/ICT_Laws/ICT_LAW-2-222__1_.pdf
[5] Malawi Electronic Transactions and Cyber Security Act, available at http://www.macra.org.mw/wp-content/uploads/2014/07/E-Transactions-Act-2016.pdf
[6] Al Jazeera, "Ugandan academic Stella Nyanzi jailed for 'harassing' Museveni," August 3, 2019, available at
https://www.aljazeera.com/news/2019/08/ugandan-academic-stella-nyanzi-jailed-harassing-museveni-190803141817222.html
[7] Tanzania's Cybercrime Act Makes It Dangerous to "Insult" the President on Facebook
https://advox.globalvoices.org/2016/04/18/tanzanias-cybercrime-act-makes-it-dangerous-to-insult-the-president-on-facebook/; Tanzania is threatening more citizens with jail for insulting the president on social media
https://qz.com/africa/782239/five-tanzanians-were-charged-with-cybercrime-for-insulting-president-john-magufuli-on-social-media/

Further, several governments have continued to demand cooperation from actors in the private sector to facilitate the interception of communications and to hand over the call data of subscribers. Social media has also emerged as a battle-ground where governments have sought to control conversations through their elaborate propaganda machinery especially during election periods. The use of social media bots and paid influencers to spread fake news has become widespread too, as have concerted efforts to muzzle critics through arrests, threats, intimidation and targeted cyber-attacks.

Developments in the financial sector have seen the introduction of new technologies including in mobile money, e-commerce, fin-tech services and mobile loans. Governments e.g. in Kenya and Uganda have introduced new internet-related taxes on data bundles, internet access and Over-The-Top (OTT) services. Indeed, evidence from countries like Uganda[8] has shown that increased taxation undermines the ability of sections of the public to access internet services.

While digital authoritarianism has been in existence for decades,[9] it is clear that its use by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations is a tool of state control over their rights. If left unchecked, democracy and internet freedom will continue to regress. While ensuring security is critical to the enjoyment of human rights, the implementation of security measures in the absence of key safeguards is in itself, a threat to the very rights sought to be protected. It is therefore important to situate the on-going discussions around internet rights by providing an in-depth analysis of the trends of how government policies and practices have shaped and are restricting digital rights in Africa over the last 20 years.

Aims of the Study

This research sought to document the extent to which government controls of the digital space affect/limit Internet Freedom in Africa since the year 1999 in 13 countries. Specifically, it traced the trends and developments in the digital space during the periods: 1999-2005; 2006-2010; 2011-2015; and 2016-2019. The study focussed on the proliferation of retrogressive or repressive policies and laws; surveillance and surveillance capacity of governments; digitization programmes; censorship; demands on private sector actors; and the new frontiers like the introduction of Internet related taxes.

The study also sought to identify measures that can secure internet freedom in Africa and inform policy makers, the media, academia, technologists, civil society and other researchers on the policy, legal, institutional and practice landscape with a view of identifying opportunities for improvement of the digital space.

---

8 Social Media Tax cuts Uganda Internet Users by 5millions, available at;
https://cipesa.org/2019/01/%EF%BB%BFsocial-media-tax-cuts-ugandan-internet-users-by-five-million-penetration-down-from-47-to-35/
9 Exporting digital authoritarianism https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf

2 Methodology

The study employed a qualitative approach including literature review, policy and legal analysis, and key informant interviews with purposively selected respondents. Reports of previous studies, media reports, academic works, government documents, and other literature, were reviewed. The literature review generated an understanding of the developments in the focus countries.

The legal and policy analysis included a review of relevant laws, policies and practices in the various countries. Such laws and policies include those that govern the telecoms sector, the media, social media use, access to information, interception of communications, security and intelligence agencies, and security enforcement in general.

The Key Informant Interviews (KIIs) were conducted with purposively selected respondents from each of the countries studied. These included staff of private companies (such as banks, telecoms firms, Internet Service Providers), government ministries (such as those responsible for ICT, security), semi-autonomous bodies such as electoral commissions, telecoms regulators, media houses, social media users, human rights defenders and activists, consumers' associations, academics and lawyers.

Country Context 3

This section provides a general overview of the state of ICTs on the African continent. Thus it highlights the political environment and the factors affecting democratisation processes in the reviewed countries. In addition, it describes the economic status of the countries under study, presenting indicators on GDP per capita, income levels and the Human Development Index. The section also provides an overview of the status of relevant policies and laws that have shaped the ICT sector over the years.

3.1 ICT Status

In the year 2000, most of the countries under review had very limited connectivity to the internet, with most reporting a penetration rate of less than 1%, and only reaching 2% around 2005. In order to develop the ICT sector, restructuring policies were implemented in many countries, often with the assistance of international partners such as the International Telecommunications Union (ITU) and the World Bank.[10] Prior to the telecommunications sector reforms, telecommunications services were largely provided under monopoly conditions, primarily by state entities and to a lesser extent, by private companies.[11]

The enactment of national ICT laws to govern the liberalisation of the telecommunication sectors saw the end of state monopoly providers and the establishment of national telecommunication services regulators such as the Communications Commission of Kenya, Botswana Telecommunications Authority, the Regulatory Authority for Post and Telecommunications of the DRC, Malawi Communication and Regulatory Authority (MACRA), Rwanda Utilities Regulatory Authority (RURA), the Tanzania Communications Regulatory Authority (TCRA),[12] the Uganda Communications Commission, the Zimbabwe Media and Information Commission, and the Ethiopian Information and Communication Technology Development Authority.[13] However, the regulators do not have complete independence from the executive.

These reforms in the ICT sector have had a strong impact on the economies of most African countries along many dimensions, with the most remarkable being the exponential growth in mobile technology use.[14] By the end of 2018, an estimated 51.2% of the global population, or 3.9 billion people, were using the internet, according to figures from the ITU, the United Nations specialised agency for information and communication technologies (ICT).[15] In Africa, the percentage of people using the internet stood at 24.4%, having jumped from a mere 2.1% in 2005. Even then, the Africa is still lagging on the road to achieve universal access to the internet since, according to the 2019 GSMA report on Mobile Internet Connectivity,[16] the Sub-Saharan region accounts for 40% of the global population not covered by a mobile broadband network.

---

10 AU (2008) Study on the harmonisation of the Telecommunication, ICTs Policies and Regulation in Africa
https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/2_Draft_Report_Study_on_Telecom_ICT_Policy_31_March_08.pdf

11 The Evolution of Regulatory Reforms http://www.ictregulationtoolkit.org/toolkit/6.2

12 TCRA Profile https://www.tcra.go.tz/index.php/about-tcra/tcra-profile

13 360/2003 A Proclamation To Provide The Establishment Of Ethiopian Information And Communication Technology Development Authority

14 UNECA (2017) Review of the legal and regulatory frameworks in the information and communications technology sector in a subset of African countries
https://www.uneca.org/sites/default/files/PublicationFiles/review_of_the_legal_and_regulatory_framework.pdf

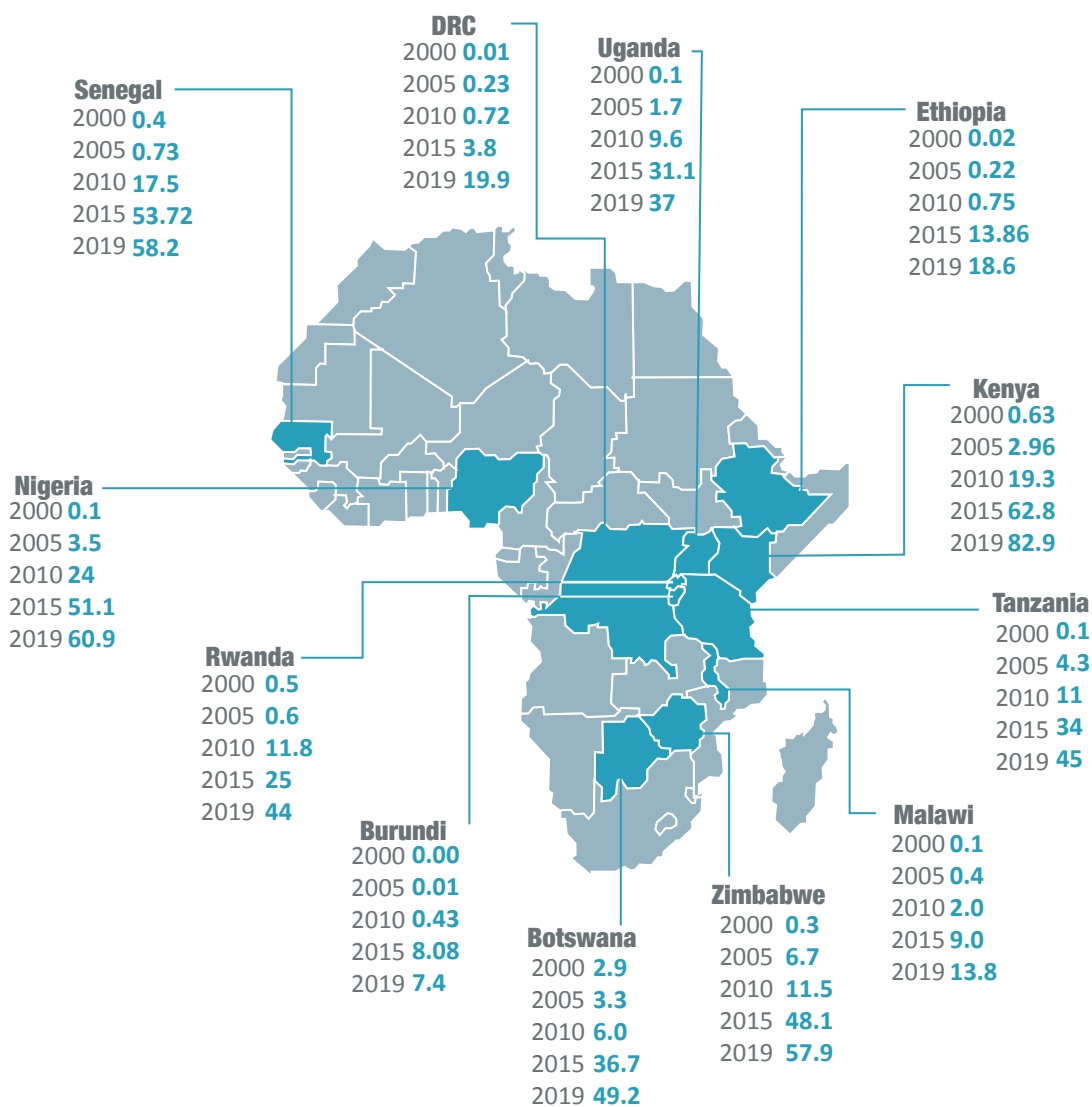**15** ITU 2018 https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

16 Mobile Internet Connectivity 2019 Sub-Saharan Africa Factsheet
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/Mobile-Internet-Connectivity-SSA-Factsheet.pdf

Internet usage also differs markedly by country within Africa. Whereas more than half the population uses the internet in South Africa, rates are closer to 30% in West Africa, and only around 10% in Central Africa. Internet usage is particularly low in landlocked countries, where the physical infrastructure necessary to provide infrastructure is costlier, and access is more dependent on neighbouring countries.[17]

The figure below provides the status of internet penetration in the countries under study during the periods 2000-2019. In the year 2000, most of the countries under review had very limited connectivity to the internet, with most reporting a penetration rate of less than 1%. Penetration rates have since grown significantly in some countries, with Kenya recording the highest penetration rate of 82.9% in 2019, followed by Senegal at 58.2% and Zimbabwe at 57.9%. In contrast, there was no significant growth in some countries such as Burundi, Malawi and the DRC, where the penetration rates remained low at 7.4%, 13.8% and 19.9% respectively. The slow growth in some countries indicates that there could be several challenges that need to be overcome to ensure access to the internet for more people.

Figure 1: Internet Penetration rates in Select Countries[18]

DRC
2000 **0.01**
2005 **0.23**
2010 **0.72**
2015 **3.8**
2019 **19.9**

Uganda
2000 **0.1**
2005 **1.7**
2010 **9.6**
2015 **31.1**
2019 **37**

Senegal
2000 **0.4**
2005 **0.73**
2010 **17.5**
2015 **53.72**
2019 **58.2**

Ethiopia
2000 **0.02**
2005 **0.22**
2010 **0.75**
2015 **13.86**
2019 **18.6**

Kenya
2000 **0.63**
2005 **2.96**
2010 **19.3**
2015 **62.8**
2019 **82.9**

Nigeria
2000 **0.1**
2005 **3.5**
2010 **24**
2015 **51.1**
2019 **60.9**

Tanzania
2000 **0.1**
2005 **4.3**
2010 **11**
2015 **34**
2019 **45**

Rwanda
2000 **0.5**
2005 **0.6**
2010 **11.8**
2015 **25**
2019 **44**

Burundi
2000 **0.00**
2005 **0.01**
2010 **0.43**
2015 **8.08**
2019 **7.4**

Botswana
2000 **2.9**
2005 **3.3**
2010 **6.0**
2015 **36.7**
2019 **49.2**

Zimbabwe
2000 **0.3**
2005 **6.7**
2010 **11.5**
2015 **48.1**
2019 **57.9**

Malawi
2000 **0.1**
2005 **0.4**
2010 **2.0**
2015 **9.0**
2019 **13.8**

17 World Bank: Internet Access in Sub-Saharan Africa - http://documents.worldbank.org/curated/en/518261552658319590/pdf/135332-POV-Practice-Note-13.pdf
18 Africa Internet Stats https://www.internetworldstats.com/stats1.htm

3.2 Political Environment

Africa continues to be dominated by 23 authoritarian regimes, with 7 countries including Botswana, Senegal, South Africa and Ghana classified as flawed democracies, and 13 "hybrid regimes", Mauritius standing out as the only fully fledged democracy.[19] In 2011, there were several pro-democracy movements, that were later termed as the Arab Spring that swept North Africa, ridding the region of the despots in Tunisia, Egypt, and Libya. The wave of change through movements and protests have continued to have an impact, spreading to other parts of the continent with similar impact in Angola, Burkina-Faso, the Gambia,[20] Zimbabwe, Algeria, and most recently in Sudan. As is shown in this study, efforts by governments to stem the wave has had significant impact on internet freedom.

Burundi's political environment has suffered a major setback despite the political stability ushered in by the 2002[21] Peace Accord signed after a decade of civil war. Having manipulated the 2005 and 2010 presidential elections,[22] President Nkurunziza once again announced his bid for a third team in April 2015, a move which was widely opposed and declared unconstitutional by Burundian opposition and civil society organizations. Following the announcement, there were demonstrations and unrest in the capital Bujumbura lasting a week. Also, a coup attempt on 13 May 2015 worsened the crisis. The government response led to the commission of serious human rights abuses as reported by different Human Rights organizations such as Human Rights Watch[23] and United Nations.[24] In May 2018, Burundi adopted a new constitution following a referendum which allowed Nkurunziza to run for at least two more terms.[25] While elections are scheduled for 2020, there are doubts by the UN Commission on Burundi, on whether they will be free and fair, in a country where the past elections have been marred by irregularities, violence and serious human rights violations.[26]

Cameroon's ruling party, the Cameroon People's Democratic Movement (CPDM),[27] has long dominated the country's political landscape since independence in 1960. Under the leadership of President Paul Biya since 1982, the party occupies 148/180 seats in the National Assembly and 81/100 in the Senate. Biya, 86, won the disputed election in November 2018, and is serving his seventh term as president.[28] However, since October 2016, the country has been engulfed in a deadly conflict that arose following concerns from Northwest and Southwest regions around deeper, long-held grievances around use of the French language given its rich and complicated colonial history, marginalisation by the central government, poor governance, inequitable political and social representation, the deterioration in the rule of law, corruption and the suppression of free speech and human rights.[29] The presidential elections in October 2018 coupled with hate speech and fake news, especially on social media accelerated the crisis.[30] In September 2019, the president announced his intention to hold a major "national dialogue" to put an end to the conflict between security forces and armed separatists from the anglophone minority in the west.[31]

19 Democracy Index 2018 https://www.eiu.com/topic/democracy-index; Africa is home to only one fully fledged democracy
https://qz.com/africa/894326/nigeria-south-africa-kenya-and-tanzania-fail-to-improve-on-global-corruption-index/
20 Africa's Top 5 most politically-stable countries https://www.inonafrica.com/2018/02/08/africas-top-5-politically-stable-countries/
21 Complete Peace In Burundi Requires Full Support Of International Community, Deputy President Of South Africa Tells Security Council
https://www.un.org/press/en/2002/sc7586.doc.htm
22 Burundi: Missteps at a crucial moment https://www.hrw.org/legacy/backgrounder/africa/burundi1105/2.htm
23 World Report 2018: Burundi https://www.hrw.org/fr/world-report/2018/country-chapters/312965
24 Burundi: Human rights violations continue, says UN Commission of Inquiry https://news.un.org/fr/story/2018/09/1022742
25 Burundi referendum: First a third term https://www.bbc.com/news/world-africa-44110338
26 UN Commission Warns of New Burundi Political Crisis in 2020 https://www.voanews.com/africa/un-commission-warns-new-burundi-political-crisis-2020
27 CPDM http://www.rdpcpdm.cm
28 Biya wins again in Cameroon as crackdown disrupts anglophone vote
https://www.theguardian.com/world/2018/oct/22/paul-biya-cameroon-85-year-old-president-wins-re-election-landslide
29 Crisis worsens in Cameroon https://www.un.org/africarenewal/magazine/december-2018-march-2019/crisis-worsens-cameroon; Cameroon's conflict keeps schools shut
https://www.bbc.com/news/world-africa-49529774
30 Anglophone crisis: Dog, Rat, Ambazozo example for hate speech weh deh di cause palava for Cameroon – LYC https://www.bbc.com/pidgin/tori-46873718; Media professionals
to counter hate speech in Cameroon crisis
https://unchrd.org/index.php?option=com_content&view=article&id=531:media-professionals-to-counter-hate-speech-in-cameroon-crisis&catid=41:top-headlines
31 Cameroon's president vows 'national dialogue' to ease tensions with anglophone separatists
https://www.france24.com/en/20190911-cameroonian-president-biya-national-dialogue-anglophone-separatists

Similarly, the DRC faced political rebellion from May 1997 following the toppling of President Mobutu's government by Laurent Kabila, who later became president after a ceasefire in 1999, but later assassinated in January 2001. His son, Joseph, who took over as head of state, oversaw the promulgation of a new constitution in 2005, and was elected president in 2006. Rebellions were later to be witnessed in the country and heightened in November 2016, at the end of his second term, when he attempted to amend the constitution and seek a third term in office.

The move resulted in political demonstrations initiated by civil society and the opposition which were met with force. In response, the government implemented an internet shutdown and the filtering of social networks and websites were implemented terming them necessary to protect public order. However, in a surprise turn of events, President Kabila announced in August 2018 that he would not seek a third term, despite delaying the 2016 presidential election and stay in power for two years.[32] In January 2019, his ally, Félix Tshisekedi was sworn in as president despite Martin Fayulu, a fellow candidate, claiming victory in the election. Fayulu believes Tshisekedi was "appointed" and is Kabila's puppet.[33] Consequently, what was supposed to be the first democratic transfer of power since independence appears tainted by political manipulation.[34]

Compared to her neighbours, Kenya has remained relatively stable save for a post-election violence period in 2007 – 2008 that left more than 1,100 dead and 600,000 people displaced.[35] President Mwai Kibaki who took over in 2002 after President Daniel Arap Moi's 24-year authoritarian rule, initiated a series of governance reforms including overseeing the promulgation of a new constitution in August 2010. Despite facing charges against crimes against humanity at the International Criminal Court (ICC), the Jubilee administration led by President Uhuru Kenyatta[36] came to power in 2013. As was in 2007 and 2013, Kenya's August 2017 general election was contested. The ensuing political stalemate was characterised by the spread of hate speech and fake news online. The government reacted by enacting the controversial Computer Misuse and Cybercrimes Act, 2018, deemed as a weapon for targeting its critics including journalists and bloggers. In May 2018, the Bloggers Association of Kenya (BAKE) successfully obtained orders suspending 26 sections of the law.[37] Also, the controversial government's digital ID programme dubbed 'Huduma Namba' was in 2019 allowed by the courts to proceed despite raising concerns over privacy violations.[38]

Uganda has enjoyed some political stability, but has seen a deterioration of her human rights record over time, partly due to measures taken to ensure President Yoweri Museveni's long stay in power since 1986 is preserved.

In Malawi, the country's founding president, Hastings Kamuzu Banda held absolute power for 31 years before being forced out in 1994 following internal and external pressure to end his authoritarian regime and adopt democratic system of government.[39] The country has conducted elections every five years since 1994, when it became a multiparty democracy and is currently ranked as a hybrid democracy by Economist Intelligence Unit's Democracy Index.[40] The May 2019 presidential elections were perhaps the most contested in the history of the country,[41] pitting the then incumbent, President Mutharika against opposition leaders Lazarus Chakweya and Saulos Chilima. Following the election, there were nation-wide protests over several days and a court case challenging the controversial electoral results. The protestors and the opposition argued that the poll had been rigged as there were serious irregularities requiring a rerun.[42] Mutharika who narrowly won the election, was sworn in after an injunction ordered by the country's High Court was lifted.[43]

32   DR Congo President Joseph Kabila not seeking third term https://www.bbc.com/news/world-africa-45112960
33   Martin Fayulu : "Félix Tshisekedi est la marionnette de Joseph Kabila", available on
https://www.france24.com/fr/20190321-rd-congo-rdc-martin-fayulu-invite-plateau-france24-felix-tshisekedi-joseph-kabila
34   Historic day as Tshisekedi is sworn in as DR Congo president https://www.bbc.com/news/world-africa-46987439
35   Kenya since 2007-2008 post-election violence https://www.nation.co.ke/news/politics/Kenya-since-post-election-violence-/1064-4046876-12j38pyz/index.html
36   Kenya leader Uhuru Kenyatta's ICC trial shelved https://www.bbc.com/news/world-africa-29083115
37   BAKE is successful after court suspends 26 sections of the Computer Misuse and Cybercrimes Act
https://www.ifree.co.ke/2018/05/bake-is-successful-after-court-suspends-26-sections-of-the-computer-misuse-and-cybercrimes-act/
38   High Court allows Huduma Namba listing but with conditions
https://www.nation.co.ke/news/Huduma-Namba-Govt-barred-from-forced-listing/1056-5051788-t78f1xz/index.html
39   Malawi: Between the Referendum and the Elections: May 1st 1994 https://bit.ly/2xXaNCm
40   The Economist Intelligent Unit's Democracy Index, 2018, https://bit.ly/2ASGPl8
41   Malawi elections: a three-horse race too close to call, May 2019, http://bit.ly/2KYHTJw
42   Malawi's maturing democracy to be tested further by more protests, August 2019, http://bit.ly/2zq0kQY
43   Malawi election: President Mutharika re-elected after court battle https://www.bbc.com/news/world-africa-48426781

Nigeria, Africa's most populous country has a hybrid regime of democracy, putting it in the same category of countries like Kenya, Sierra Leone, Gambia and Cote D'Ivoire. While elections have been held consistently every four years since 1999, they have had substantial irregularities preventing them from being free and fair. The government commonly puts pressure on opposition parties and candidates and also suppresses political opponents. Moreover, there are serious weaknesses in political culture, including in the functioning of government and political participation. Corruption tends to be widespread, while the rule of law is weak and the Judiciary is not independent. Civil society remains weak and journalists continue to be harassed, a trend which has been on the rise since 2015.

Rwanda has been recognized globally as having a Parliament with the highest number of women in the world. Gender equity is one of the pillars of the country's governance. Moreover, it has been relatively politically stable and maintained continuous economic growth since the 1994 genocide. During the period under review, the country held two referendums, to adopt a new constitution in 2003[44] and to amend the constitution in 2015.[45] The 2015 amendments allowed president Paul Kagame to vie for re-election in 2017, a move that could extend his stay in power to 2034, despite having won all three presidential elections held since 2000. The government has however been criticized for its poor human rights record including silencing critics and the media, and limiting freedom of expression. The 2018 European Union report on the country's Human rights and democracy raised concern over the serious violations of civil and political rights despite progress on economic and social rights.[46]

Senegal on the other hand, has been a politically stable democracy during the period under review and gained a reputation of being a West African country that has not having experienced a coup d'état. Long serving opposition leader for 25 years Abdoulaye Wade came to power in 2000, ending the domination of the then dominant Socialist Party. Despite initiating positive constitutional reforms, including multiparty democracy and an independent media, his legacy was tarnished towards the end of his second term, when despite his age, he made a controversial bid for a third term in 2012, which he lost. The current President, Macky Sall is serving his second term having won the last election in February 2019. ICTs continue to play an important role in elections and the results are available as soon as the polls closed. However, challenges still exist. Political opposition demonstrations are often banned and freedom of expression and opinion remains under threat. The latest incident was in July 2019, where an activist, Guy Marius Sagna, who is the leader of a movement called "France Releases", was placed under arrest and detained for raising a false alert to terrorism on Facebook.[47]

In East Africa, Tanzania's ruling party Chama Cha Mapinduzi (CCM), continues to dominate the political scene, having won all presidential elections since 2000. Its transition to a true multiparty democracy has been frustrated by institutional weaknesses, weak party structures and processes, a lack of ideology and weak internal party democracy.[48] In October 2015, President John Pombe Magufuli came to power in what was considered "the most fierce" election the government party had faced after 54 years in power.[49]

In order to stem the declining public support and trust ahead of the 2020 elections, President Magufuli has embarked on a campaign that has resulted in a crackdown on human rights, and any form of opposition, including legitimate criticism. The result has been suspicious defections of local leaders to CCM,[50] including President Magufuli's challenger in the 2015 election, Edward Lowassa.[51]

44   EU election observation mission to Rwanda in 2003
https://eeas.europa.eu/headquarters/headquarters-homepage/26331/eu-election-observation-mission-rwanda-2003_mn
45 Rwanda: Referendum Approves Extended Presidential Terms https://www.loc.gov/law/foreign-news/article/rwanda-referendum-approves-extended-presidential-terms/
46 EU Annual Report on Human Rights and Democracy in the World 2018 - Rwanda
https://eeas.europa.eu/delegations/rwanda/62839/eu-annual-report-human-rights-and-democracy-world-2018-rwanda_en
47 Senegal: Activist Guy Marius Sagna placed under arrest warrant for "false alert to terrorism"
https://www.jeuneafrique.com/806191/politique/senegal-lactiviste-guy-marius-sagna-place-sous-mandat-de-depot-pour-fausse-alerte-au-terrorisme/.
48 State of Politics in Tanzania https://www.kas.de/c/document_library/get_file?uuid=5255a2d1-92dd-75e9-92ce-0bc85a47f08c&groupId=252038
49 Tanzania poll: John Magufuli of CCM defeats Edward Lowassa https://www.bbc.com/news/world-africa-34669468
50 Chadema leaders defect to CCM https://www.thecitizen.co.tz/news/Chadema-leaders-defect-to-CCM/1840340-5078702-p7aj44/index.html
51 Veteran Tanzanian politician Edward Lowassa returns to CCM
https://www.theeastafrican.co.ke/news/ea/Veteran-Tanzanian-politician-Edward-Lowassa-returns-to-CCM/4552908-5005600-10br1dqz/index.html

3.3 Economic Status

At the turn of the century, African countries remained by and large dependent on the export of a few commodities, and terms of trade have aggravated their capacity to invest in human and physical infrastructure. The levels of national savings and investment have been insufficient to ensure a process of accumulation necessary to place Africa on a sustainable growth path.[52] However, by 2015, Africa was considered the world's second fastest growing economy after East Asia. Growth in real GDP was estimated at 3.6%, higher than the 3.1% for the global economy and 1.5% for the euro area.[53]

By 2018, almost 20 years later, African economies had become resilient and were gaining momentum. Real output growth was estimated to have stabilised at 3.6% between 2015 and 2017 and projected to accelerate to 4.1% in 2018 and 2019, according to the 2018 African Economic Outlook Report by the African Development Bank[54] In Nigeria, growth reached 1.9% in 2018, up from 0.8% in 2017, reflecting a modest pick-up in the non-oil economy. South Africa came out of recession in the third quarter of 2018, but growth was subdued at 0.8% over the year, as policy uncertainty held back investment.[55] Economies such as Kenya, Rwanda, Uganda, and several in the West African Economic and Monetary Union, including Benin and Côte d'Ivoire are reported to have recorded solid economic growth in 2018.[56]

Regrettably, many African governments are reported to have failed to translate this economic wealth into Sustainable Economic Opportunity for their citizens. Almost half (43.2%) of Africa's citizens live in one of the 25 countries where Sustainable Economic Opportunity has declined in the last ten years.[57]

Figure 2: Country GDP per capita (PPP)[58] and HDI Ranking[59]

Botswana	2000	2005	2010	2015	2019
GDP per capita (PPP)	$8,008.24	$10,012.87	$12,534.25	$15,569.94	$18,636
HDI ranking[60]	187	196	186	174	146
Burundi					
GDP per capita (PPP)	$517.37	$572.4	$659.2	$700.54	$657.0
HDI ranking	237	253	253	251	185
Cameroon					
GDP per capita (PPP)	$1,905.4	$2,256.2	$2,522.9	$3,115.4	$3,624.6
HDI ranking	216	223	223	220	151

52   Economic Developments in Africa 2001 available at https://unctad.org/en/Docs/pogdsafricad1.en.pdf

53   African Economic Outlook 2016

54   https://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/African_Economic_Outlook_2018_-_EN.pdf

55   The World Bank in Africa https://www.worldbank.org/en/region/afr/overview#1

56   Ibid

57   2018 Ibrahim Index of African Governance http://s.mo.ibrahim.foundation/u/2018/11/27173840/2018-Index-Report.pdf

59   AFDB Socio Economic Database, 1960-2019 http://comstat.comesa.int/wiqcbkg/afdb-socio-economic-database-1960-2019?tsId=1244030

59   The Human Development Index (HDI) is a summary measure of average achievement in key dimensions of human development: a long and healthy life, being knowledgeable and having a decent standard of living.- Human Development Index - HDI https://countryeconomy.com/hdi

60   Human Development Index (HDI) http://hdr.undp.org/en/content/human-development-index-hdi

DRC	2000	2005	2010	2015	2019
GDP per capita (PPP)	$423.4	$491.1	$602	$811.4	$860.7
HDI ranking	152	167	168	176	176

Ethiopia					
GDP per capita (PPP)	$494.3	$647.7	$1,052	$1,632.6	$2,183.8
HDI ranking	171	170	157	174	173

Kenya					
GDP per capita (PPP)	$1,730	$2,031.2	$2,487.2	$3,097.3	$3,733.8
HDI ranking	206	213	213	214	142

Malawi					
GDP per capita (PPP)	$690.7	$765.2	$1,039.3	$1,185.2	$1,333.3
HDI ranking	221	224	242	241	171

Nigeria					
GDP per capita (PPP)	$2,249.8	$3,518.9	$5,019.2	$6,004.7	$5,978.2
HDI ranking	-	225	231	226	157

Rwanda					
GDP per capita (PPP)	$622.9	$919.3	$1,319.2	$1,829.5	$2,308.3
HDI ranking	160	168	152	159	158

Senegal					
GDP per capita (PPP)	$1,515.4	$1,870.4	$2,131.3	$2,424.5	$3,022.9
HDI ranking	229	236	238	238	164

Tanzania					
GDP per capita (PPP)	$1,181.2	$1,588	$2,008.7	$2,594.8	$3,200.1
HDI ranking	224	230	226	225	154

Uganda					
GDP per capita (PPP)	$933	$1,277.5	$1,767.6	$2,061.6	$2,311
HDI ranking	222	232	229	232	162

Zimbabwe					
GDP per capita (PPP)	$2,020.4	$1,459.4	$1,442.4	$2,035.9	$2,087.1
HDI ranking)	214	235	236	224	156

Among the countries reviewed, Nigeria has the highest population in 2019 with 201.8 million people, followed by Ethiopia with 112.5 million.[61] The smallest countries by population are Burundi and Rwanda with populations of 11.5 million and 12.6 million respectively. With regards to economic status, International Monetary Fund[62] figures show that as of 2019, Botswana had the highest GDP per capita (PPP) at USD 8,263.2 followed by Nigeria (USD 6,027), Kenya (USD 3,690), Senegal (USD 3,651) and Tanzania (USD 3,443). DR Congo and Burundi recorded the lowest GDP per capita at USD 767.3 and USD 732.5 respectively.

According to HDI statistics, Kenya ranked highest among the countries in the present research at 142 with Botswana following closely at 146. Burundi was ranked lowest at 185, followed by the DRC at 176.

[61] 2019 World Population by Country http://worldpopulationreview.com/
[62] World Economic Outlook Database, April 2019 http://tiny.cc/3308bz

Results 4

4.1　Key Trends of the Internet Control Over the Last Two Decades

This section traces the history, evolution and shifts and milestones of internet control measures in Africa, since 1999. The reason is to provide a deeper appreciation of the intervening political and socio-economic considerations behind the different control measures as introduced and applied by different governments.

4.1.1 Weaponising the Law to Legitimise Actions

As early as 2005, some countries had already introduced digital rights infringing provisions in their ICT-related laws and policies. As ICT usage grew, the provisions became more restrictive – providing for state surveillance, interception of private communication, and online censorship, among others. Most of the legislation were introduced under the pretext of ensuring national security and fighting terrorism and cybercrime. By the end of 2018, all the countries under review either had a law or bill related to Computer Misuse and/or Cybercrime.

Legalising Surveillance and Interception of Communication

A number of countries adopted legislation to legitimise surveillance practices through legalised interception by State agencies supported by communication intermediaries.

In 1998, Kenya adopted the National Security Intelligence Service (NSIS) Act which was later amended in 2012. The Act among others establishes the NSIS which is inter alia, is charged with gathering intelligence and regulating security intelligence in the country. Further, section 42 permits the interference of persons' communications through legalised investigation. Likewise, the DRC in 2003, established the National Intelligence Agency (ANR) through Law N° 003-2003 whose article 3(3) grants the ANR authority to conduct surveillance of national or foreign persons or groups of persons suspected of carrying on an activity likely to endanger the security of the state.[63]

Similarly, the Ethiopian Aviation Security Proclamation adopted in 2004 empowers the Security, Immigration and Refugee Affairs Authority and the Federal Police Commission to intercept and surveil without a court warrant, so as to prevent unlawful acts against aviation institutions and flight safety equipment. Before its adoption, the Ethiopian government had in 2002 amended Proclamation No. 49/1996 providing for the regulation of telecommunications, and prohibiting non-state actors from providing telecommunication services, leaving monopoly of the sector to the state-owned Ethio Telecom.[64]

---

[63] January 11, 2003. Decree-law n ° 003-2003 establishing and organizing the National Intelligence Agency, available at https://www.leganet.cd/Legislation/Droit%20Public/Ordre/DL.11.01.2003.htm on august 15, 2019.

[64] Text of the proclmation https://chilot.me/2011/08/proclamation-no-491996telecommunications/

Zimbabwe's Interception of Communications Act (ICA)[65] adopted in 2007 requires telecommunications service providers to have at their own cost, "the capability of interception" and ensure that their services are "capable of rendering real time and full-time monitoring facilities for the interception of communications and storage of call-related information.[66] The law does not provide for independent judicial oversight. Moreover, its supervisory powers are placed in the Office of the President and Cabinet and warrants are issued by the Prosecutor-General. In September 2011, POTRAZ, the Zimbabwean regulator, stopped Econet Wireless from introducing Blackberry Messenger, which provided encrypted messaging services, without a specific license from the regulator.[67] Similarly, Rwanda's interception of communication law passed in 2008; Uganda's Computer Misuse Act, 2011 under section 28 and Section 11 of Uganda's Regulation of Interception of Communications Act 2010; Nigeria Communications Commission (NCC) Guidelines for the Provision of Internet Service 2013 and the Mutual Assistance in Criminal Matters Law Nigerian Government;[68] and Kenya's Computer Misuse and Cybercrimes Act, 2018 provide for the requirement of communication service providers including internet intermediaries to ensure that their systems are technically capable of supporting lawful interceptions at all times as provided by the regulatory laws in force.

Rise of National Security as Justification for Repressive Laws

The protection of national security, preservation of public order and the fight against terrorism have been widely used on the continent to enact repressive legislation. Moreover, the termsThese terms have not been clearly defined and therefore largely ambiguous and abused to extend to all aspects of society with a common trait of promoting impunity by state agencies in their operations.

In Rwanda, Article 52(1) of the Law No. 44/2001 of 30/11/2001 Governing Telecommunications empowers the minister in charge of telecommunications policy and law, to "interrupt or cause to be interrupted, any private communication which appears dangerous to the national integrity, contrary to law, public order or public morals".[69] The law further further provided for legalised interception of communication in the interest of national security and the prevention, investigation, detection, and prosecution of criminal offences. Similarly, the DRC Framework Law No. 013-2002 of October 16, 2002 in article 46 and Ethiopia's Anti-Terrorism Proclamation of 2009 similarly proviside for interception of communications. .

In both Uganda and Zimbabwe, lawful interception of communication is allowed following the issuance of a warrant by a judge if there is "reasonable grounds" for interception to take place. This includes "an actual threat to national security or any compelling national economic interest" or "concerning a potential threat to public safety or national security." Uganda's Regulations of Interception of Communication Act 2010 extends its grounds for interception to include - "... any national economic interest, or if there is a threat to the national interest involving the State's international relations or obligations." The law gives the Minister of ICT powers to set up a monitoring centre connected to telecom service providers' systems.

In May 2012, Burundi amended the Law Number 1/025 of November 2003, through Press Law No 1/11 of 4 June 2013 which introduced provisions (Articles 26-35 and 44-45) that unduly regulate publications whether in print or on the internet. It also imposes restrictions on media reporting on matters that would undermine public order and national security, national unity, national sovereignty, morality good morals.[70] In the same year, Ethiopia, introduced the Telecom Fraud Offense Proclamation, which criminalised call back services, Voice Over Internet Protocol (VoIP) services like WhatsApp, Viber, Skype, and others. The government justified the need for the law, stating in its preamble that "telecom fraud is a serious threat to national security".[71]

65 Interception of Communications Act, long title. Accessed here: http://archive.kubatana.net/html/archive/legisl/070803ica.asp?sector=legisl
66 Challenges in promoting privacy and freedom of expression in Zimbabwe,
http://nehandaradio.com/2013/06/11/challenges-in-promoting-privacy-and-freedom-of-expression-in-zimbabwe/
67 Econet BlackBerry service 'banned' https://www.telegeography.com/products/commsupdate/articles/2011/06/20/econet-blackberry-service-banned/
69 Paradigm Initiative sends FoI Request to NCC on Nigeria's New Surveillance Provisions
https://paradigmhq.org/paradigm-initiative-sends-foi-request-to-ncc-on-nigerias-new-surveillance-provisions
70 Law No. 44/2001 of 30/11/2001 Governing Telecommunications http://www.rura.rw/fileadmin/laws/TelecomLaw.pdf
Text of the law https://www.assemblee.bi/IMG/pdf/N%C2%B01_11_4%20juin_2013.pdf
71 Telecom Fraud Offences Proclamation No - 761/2012 https://chilot.me/2012/12/proclamation-no-7612012-telecom-fraud-offence-proclamation/

In Malawi, section 24 of the Electronic Transaction and Cyber Security Act, 2016[72] provides that public communications could be restricted in order to, among others, protect public order and national security and facilitate technical restriction to conditional access to online communication. However, no definition of national security is provided. In Senegal, section 192 of Press Code, Law 2017-27 of July 13, 2017 allows a "competent authority", without authorisation of a judge, in exceptional circumstances to seize publications, stop broadcasts or temporariluy shut down a media outlet, so as to prevent or stop a breach of national security or territorial integrity, or to stop incitement of hatred or a call for murder".[73] Additionally, Article 90-10 of Law No. 2016-30 of 08 November 2016 of Senegal grants an investigating judge power to use software to search a computer system remotely and to collect relevant evidence relevant to the trial or investigation.[74]

Terrorism as a Justification

The fight against terrorism has also been used as a basis for introducing repressive laws. In 2014, following a terrorist attack at the Westgate Shopping Mall in Nairobi in September 2013, the government introduced an amendment to the Prevention of Terrorism Act under the Security Laws (Amendment) Act (2014). The amendment limited the right to privacy under the constitution and authorised National Security Organs to intercept communication for the purposes of detecting, deterring, and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary. The procedures are yet to be made public.

Under Uganda's Anti-Terrorism Act of 2002 law, interception of communications may be conducted on grounds such as: safeguarding of the public interest; prevention of the violation of the fundamental and other human rights and freedoms of any person from terrorism; prevention or detecting the commission of any offence; and safeguarding the national economy from terrorism.[75] Amendments to the act were made in 2017 to include broad criminalisation of terrorism to inlcude 'indirect' involvement in terrorist activities and the 'unlawful possession of materials for promoting terrorism, such as audio or video tapes or written or electronic literature.'[76]

Similarly, Ethiopia's Anti-Terrorism Proclamation of 2009 was widely misapplied and abused to enforce censorship, silence dissidents and unduly compromise fundamental rights and freedoms.[77] The law authorises interception of communication of the individual under Article 14 including of telephone, fax, radio, internet, electronic, postal and similar communications. Communication service providers are required to cooperate when requested by the NISS to conduct the interception. Those who fail to cooperate can be imprisoned for between three and 10 years.

In Zimbabwe, former editor at the state-owned Sunday Mail newspaper, Edmund Kudzayi, was arrested in June 2014 on accusations of running the 'Baba Jukwa' Facebook account, on charges of intention to subvert the government through waging "cyber-terrorism" through the Facebook account and was released two weeks later on a USD $5,200 cash bail.[78] At the same time, a controversial yet popular page, Mugrade Seven was also deactivated.[79]

In response to the growing criticism from Cameroonians abroad for shutting down the internet in 2011, Issa Tchiroma, the Minister of Communications labelled Cameroonians abroad as 'cyber-terrorists' claiming that the government was a victim of cyber-terrorism. In November 2016, the President of the National Assembly also labelled internet users "traitors of the cyberspace" and called social media users "terrorists". Government officials accused social media users spreading rumours and being a threat to a peaceful Cameroon. The labelling of critics as terrorists points to the possible use of terrorism legislation against critics.

---

[72] Electronic Transaction and Cyber Security Act, 2016; https://bit.ly/2Cjmsy0
[73] Loi n° 2017-27 du 13 juillet 2017 portant Code de la Presse http://www.jo.gouv.sn/spip.php?article11233.
[74] Loi n° 2016-30 du 08 novembre 2016 http://www.jo.gouv.sn/spip.php?article11002
[75] The Anti-terrorism Act No.14 of 2002, "http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf
[76] https://ulii.org/ug/legislation/act/2017/4
[77] The Terrorism of 'Counterterrorism': The Use and Abuse of Anti-Terrorism Law, the Case of Ethiopia http://eujournal.org/index.php/esj/article/view/9348/8911
[78] Charles Laiton, "Sunday Mail Editor 'is Baba Jukwa," The Standard, June 22, 2014, http://bit.ly/1Lyv02G
[79] Mugrade Seven was also a pseudonymous Facebook character with over 200,000 followers, who referred to him/herself as a 'Fearless Journalist' who was in the business of 'informing the nation nonstop, 24/7'. The page notoriously used to publish damaging information about prominent government officials.

Silencing Dissent and Criticism through Criminalising Free Speech

The systematic use of criminal law to prosecute and punish critics has become a trend in different countries. This includes the introduction of provisions in laws that require individuals to declare their sources of information, such as in Cameroon. Other legal provisions introduced allegedly to tackle fake news require persons to only publish true and authenticated information, or be held liable. The use of arrests and intimidation of journalists and the online community was reported in several countries.

Enforcing Insult Laws

One of the emerging methods has been the use of 'insult' laws. In December 2014, outspoken Kenyan blogger Robert Alai was arrested and charged under section 132 of the Penal Code[80] for undermining the authority of a public officer because of remarks he had made on social media concerning President Uhuru Kenyatta. He posted the statement "Insulting Raila is what Uhuru can do. He hasn't realised the value of the Presidency. Adolescent President. This seat needs Maturity" which authorities found were calculated to bring into contempt the lawful authority of the President. Alai made a constitutional challenge to the arrest and argued that the provision was vague, uncertain and an unjustifiable limitation to freedom of expression, as well as violating basic criminal law principles. The High Court in April 2017 found the provision invalid and declared that its continued enforcement was unconstitutional and a violation of the fundamental right to freedom of expression.[81]

Uganda's Computer Misuse Act 11, which criminalised cyber harassment (section 24) and "offensive communication under section 25, has been used to arrest and charge government critics. On August 1, 2019, Ugandan Dr. Stella Nyanzi, an academic and human rights activist, was convicted for cyber harassment (and acquitted of offensive communication) against president Yoweri Museveni under sections 24 (1) and (2)(a) of the Computer Misuse Act 2011.[82] Nyanzi's use of metaphorically worded poetry which has often criticized Museveni's reign over Uganda were used against her in court. Nyanzi was arrested in November 2018 for publishing a poem in which she referred to Museveni's existence, his mother and the deterioration of public institutions during his leadership. She stated, "I wish the acidic pus flooding Esiteri's (the president's mother) vaginal canal had burn up your unborn fetus. Burn you up as badly as you have corroded all morality and professionalism out of our public institutions in Uganda."

The Zimbabwe Lawyers for Human Rights (ZLHR) have since July 2014, reported to have provided legal aid to more than 200 people arrested for posts made on social media sites like Facebook and Twitter. The charges have mainly related to the 'insult law'. In November 2017, Martha O'Donovan, an American working in Zimbabwe was arrested for calling former President Robert Mugabe a "sick and selfish man" on Twitter.[83] She was detained and charged with subversion and attempting to overthrow the Mugabe government, an offence which carries a sentence of up to 20 years in prison.

In Tanzania, Section 16 of the Cybercrime Act, 2015 makes it an offence to publish information, data or facts presented in a picture, text, symbol or any other form in a computer system, where such information, data or fact is false, deceptive, misleading or inaccurate. The political opposition, national and international human rights groups challenged the constitutionality of the law, but the Chief Justice, Mohammed Chande Othman, defended the law in a speech saying it was enacted in good faith, to safeguard the right to privacy of Tanzanians.[84]

---

[80] IN 2017, the provision was invalidated by a High Court decision.
https://www.article19.org/resources/kenya-win-for-freedom-of-expression-as-penal-provision-declared-unconstitutional/
[81] Robert Alai v The Hon Attorney General & another [2017] eKLR http://kenyalaw.org/caselaw/cases/view/135467/
[82] Al Jazeera, "Ugandan academic Stella Nyanzi jailed for 'harassing' Museveni," August 3, 2019, available at
https://www.aljazeera.com/news/2019/08/ugandan-academic-stella-nyanzi-jailed-harassing-museveni-190803141817222.html
[83] An American was just jailed in Zimbabwe for mean tweets about Mugabe
https://www.washingtonpost.com/news/worldviews/wp/2017/11/04/an-american-was-just-arrest-in-zimbabwe-for-mean-tweets-about-mugabe/?noredirect=on&utm_term=.1b57067c02a0
[84] Why cybercrime act is not easy to defend and justify
https://www.thecitizen.co.tz/oped/Why-cybercrime-act-is-not-easy-to-defend-and-justify/1840568-3206562-sp7m5f/index.html

Several people have been arrested in Tanzania under this Act. Colloquially termed as the "Jamii Law", a law that authorises law enforcement to jail those who publish "offensive" content or "false" information online. Rights groups and activists believe the law was aimed at popular online Swahili based forum, Jamii Forums, which has increasingly suffered the wrath of the authorities. Digital rights activist and JamiiForums proprietor, Maxence Melo, tasted the acrid side of the law when he was jailed for failure to disclose Jamii Forums user data.[85] Other cases under this law include the arrest and charge of Sospiter Jonas in Dodoma in October 2015 with "misuse of the internet" after posting on Facebook that Tanzanian Prime Minister Mizengo Pinda "will only become a gospel preacher". [86]

In Senegal, Article 254 of the Penal Code creates the offence against the President of the Republic. The law does not define the "offence" against the Head of State yet the law has been used to arrest and detain people. Several activists have been arrested for speech on social networks for the "offence to the Head of State" and "attack on the security of the State"[87] For example, Adama Gaye, journalist and activist, was arrested in July 2019 for making remarks on Facebook deemed insulting to the President Macky Sall and undermining the security of the state.[88] His posts related largely to governance, official corruption and the management of the country's oil resources. Earlier in December 6, 2017, a writer Patrice Nganang was arrested soon after making several posts on his Facebook account criticizing President Paul Biya and his government.

Senegal's 2008 Cyber Crimes Law,[89] under Article 431-59, criminalises the public dissemination of immoral objects or images through print, broadcast, or digital communication. In 2017, Zimbabwe introduced a draft Computer Crime and Cybercrime Bill which proposes to introduce the offence of harassment utilising means of electronic communication, which could be used to silence critics online.[90] The law also does not provide for judicial oversight on the implementation of warrants.

False News / Misinformation

In Zimbabwe, the 2002 Access to Information and Protection of Privacy Act (AIPPA) became the leading weapon of the government and the ruling ZANU-PF party in their campaign to stifle the opposition Movement for Democratic Change (MDC) and independent media reporting. The law granted wide-ranging powers to the government-controlled Media and Information Commission, imposed registration and licensing requirements on media outlets, and imposed strict content restrictions on the media by introducing section 64 on "Abuse of freedom of expression", and section 80, on "Abuse of journalistic privilege". Within 10 weeks of AIPPA being enacted, 13 journalists were arrested, and by the end of 2002, 44 media practitioners had been arrested. Section 80 was amended in October 2003 and its application limited, making it an offence to publish false information if the author knew it was false or did not have reasonable grounds for believing it is true and if published recklessly, or with malicious or fraudulent intent.

In May 2015, Nigeria introduced the Cyber Crime (Prohibition, Prevention etc) Act meant to provide a framework for the prohibition, prevention, prosecution and investigation of cybercrimes. Section 24 of the law 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." This provision has been used to arrest several bloggers and online journalists on charges of "cyberstalking" stemming from articles critical of government.[91]

In May 2018, Kenyan President Uhuru Kenyatta assented to the Computer Misuse and Cybercrimes Act, 2018, which introduced offences such as false publications, publication of false information, cyber harassment, and unauthorised interference and unauthorised interception. Following a petition by the Bloggers Association of Kenya (BAKE) and the Kenya Union of Journalists (KUJ), the High Court suspended the implementation of 26 provisions of the law.[92]

85 CIPESA, "UPDATE: Maxence Melo Charged with Obstruction of Investigations and Operating a Domain Not Registered in Tanzania," December 16, 2016, available at https://cipesa.org/2016/12/update-maxence-melo-charged-with-obstruction-of-investigations-and-operating-a-domain-not-registered-in-tanzania/

86 Two Tanzanians accused of False Information Face Charges under new Cyber Crimes Law https://advox.globalvoices.org/2015/10/19/two-tanzanians-accused-of-posting-false-information-face-charges-under-new-cybercrime-law/

87 Senegal: "Justice wants to keep Adama Gaye in prison as long as possible" https://www.jeuneafrique.com/811477/politique/senegal-la-justice-veut-maintenir-adama-gaye-en-prison-le-plus-longtemps-possible/.

88 Senegalese journalist Adama Gaye arrested: yes, freedom of expression has limits! https://lecourrier-du-soir.com/arrestation-du-journaliste-senegalais-adama-gaye-oui-la-liberte-dexpression-a-des-limites/.

89 Law No. 2008-11 of 25 January 2008 on cybercrime (JORS, no. 6406 of 03 May 2008, p. 419) (Appendix 1).

90 Text of the bill: https://www.techzim.co.zw/wp-content/uploads/2016/09/Zimbabwes-draft-Computer-Crime-and-Cybercrime-Bill-16-September-2016-version.pdf

91 How Nigeria's cybercrime law is being used to try to muzzle the press https://cpj.org/blog/2016/09/how-nigerias-cybercrime-law-is-being-used-to-try-t.php

92 Petition 206 http://kenyalaw.org/caselaw/cases/view/159286

In March 2005, Tanzania passed the Statistics Act, which criminalises the publication of official statistics without authorisation, and which was widely criticised, including for having provisions which "which are out of line with international standards such as the UN Fundamental Principles of Official Statistics and the African Charter on Statistics."[93]

In the DRC, publishing information relating to the situation of soldiers could be considered incitement of members of the armed forces and law enforcement agencies to divert them from their duties.[94] Despite its recent progress to reform several laws, the Ethiopian government is considering a new hate speech law that would unduly criminalise and broaden the definition of hate speech and the dissemination of fake news.

Criminal Defamation

Criminal Defamation laws have been used against government critics. The Kenya Information and Communication Act, 2009 under the now repealed section 29,[95] which made it an offence to send, through a licensed telecommunication system, a message that is grossly offensive or of an indecent, obscene or menacing character; or to send a message that one knows to be false for the purpose of causing annoyance, inconvenience or needless anxiety to another person. Several bloggers and journalists were threatened, arrested and detained over this offence.[96]

In 2011, Ugandan journalist, Timothy Kalyegira was arrested and charged with criminal defamation[97] for an article he had published on his online newspaper - the Uganda Record, questioning the involvement of the Somalis in the July 2010 twin bombings in Uganda. In 2014, the Cameroon government continued its history of media suppression and several journalists including Guy Nsigue,[98] Zacharie Ndiomo[99] and Amungwa Tanyi Nicodemus[100] were arrested and convicted for criminal defamation. Nicodemus, publisher and editor of the private weekly The Monitor, was sentenced to four months in prison and ordered him to pay 10 million CFA francs in damages (US$21,000).

The Ugandan government and its proxies have unsuccessfully attempted to block Tom Voltaire Okwalinga (TVO), a vocal pseudonymous critic of the government who publishes frequently on Facebook. In April 2018, a Ugandan lawyer Fred Muwema lost an appeal case against a ruling by the High Court of Ireland, where Facebook is headquartered, which refused the attempt to force Facebook to reveal TVO's identity and location who allegedly defamed him in a number of Facebook posts in 2016.[101] While the infringing posts were removed, TVO's identity was not revealed on the basis that they would be exposed to arrest and ill-treatment at the hands of the Ugandan authorities. Facebook had provided evidence from a Ugandan civil society organisation, Chapter Four whose representative, Nicholas Opiyo, said a man called Shaka Robert, who was widely believed to be TVO, had been subjected to abuse of his rights by the Ugandan authorities over online activism.[102]

In Botswana, a tabloid journalist Daniel Kenosi, was arrested and charged with defamation and the unlawful distribution of obscene material contrary to section 16 of the Cybercrime and Related Crimes Act, in connection with social media posts implicating a government minister in a sex scandal that the journalist had published in early 2015.[103]

[93] World bank Statement on the amendments to the Tanzania Statistics Act
https://www.worldbank.org/en/news/statement/2018/10/02/world-bank-statement-on-amendments-to-tanzanias-2015-statistics-act
[94] Internews and Albany Associates, Revue de la Législation sur les medias en RDC, Juin 2012, p.5.
http://www.smartcomms.org/wp-content/uploads/2011/07/Revue-de-la-l%C3%A9gislation-sur-les-M%C3%A9dias-en-RDC.pdf
[95] Why Justice Mumbi Ngugi declared Section 29 of KICA Unconstitutional
https://www.ifree.co.ke/2016/05/justice-mumbi-ngugi-declared-section-29-kica-unconstitutional/
[96] Bake Condemns The Arrest And Intimidation Of Kenyans Online
https://www.blog.bake.co.ke/2016/01/24/bake-condemns-the-arrest-and-intimidation-of-kenyans-online/
[97] Timothy Kalyegira remanded over libel allegations https://ugandaradionetwork.net/story/timothy-kalyegira-remanded-over-libel-allegations
[98] Joseph Owona orders the arrest of sports journalist Guy Nsigué
https://www.camerounweb.com/CameroonHomePage/NewsArchive/Joseph-Owona-orders-the-arrest-of-sports-journalist-Guy-Nsigu-313214#
[99] 2014 prison census - Cameroon: 'Flash' Zacharie Ndiomo https://www.refworld.org/docid/54980512e.html
[100] Cameroonian newspaper editor jailed for defamation https://cpj.org/2014/04/cameroonian-newspaper-editor-jailed-for-defamation.php
[101] Mary Carolan, "Court refuses to compel Facebook to disclose blogger's identity and location," April 19, 2018,
https://www.irishtimes.com/news/crime-and-law/courts/court-refuses-to-compel-facebook-to-disclose-blogger-s-identity-and-location-1.3467309
[102] Ibid.
[103] Freedom House (2017) Freedom of the Press 2016/Botswana https://freedomhouse.org/report/freedom-press/2016/botswana

Excessive and Punitive Responses

Early civic action in the continent was focused largely on civil and political rights as political actors demanded space to exercise their freedoms. In the post-2000 era, there appears to be a shift to focus not just on civil and political rights, but a greater emphasis on economic, social and cultural rights. This shift, has led to increased demands for government accountability on key issues such as corruption, fiscal transparency and accountability in areas such as education, health and social security. Some of the journalists and bloggers who have been targeted are those that have been outspoken on such issues. When governments have responded, the measures have often been excessive and unreasonable.

The year 2005 marked a turning point for Ethiopia, setting the tone for its subsequent repressive actions in the years that followed. Following the controversial May 2005 general election and the unrest that ensued, the government commenced a widespread crackdown and meted violence on protesters, leading to serious human rights violations[104] including extra-judicial killings of 193 and the injury of 763 persons, arbitrary arrests, unlawful detention and torture of tens of thousands of people, including opposition leaders, by Ethiopian security forces.[105]

The censorship in Ethiopia was in turn part of broader limits to free expression and the freedom to assemble and associate, and also the enactment of restrictive laws such as the Proclamation on Broadcasting Services in 2007;[106] the Proclamation to Provide for Freedom of the Mass Media and Access to Information adopted a year later further limited freedom of speech, right to access information and press freedom in the country.[107] Moreover, the Proclamation to Provide for the Registration and Regulation of Charities and Societies enacted in February 2009, restricted NGOs that received more than 10% of their financing from foreign sources from engaging in essentially all human rights and advocacy activities, leading to the closure of several organizations.

The DRC government in November 2011 banned the Future Channel Radiotélévision (CFTV) from broadcasting following a decision taken by the Higher Council for Audiovisual and Communication (CSAC).[108] The station, which is owned by a politician, Vital Kamerhe, was accused of spreading statements with unproven accusations against a political opponent. The ban is yet to be lifted. Similarly, in December 2013, the provincial coordination of the CSAC Kisangani the bi-monthly newspaper Kisangani News for three months. The editor of the newspaper, Mr. Sebastien Mulumba, claimed the suspension was politically motivated.[109]

Malawi initiated a media crackdown on media covering live demonstrations in 2011.[110] The government also enforced article 46 of the Penal Code which empowers the minister responsible, to prohibit the publication or importation of publications considered to be contrary to the public Interest.[111] In 2013, the Kenyan government introduced amendments to the Kenya Information and Communication Act to establish a Multimedia Appeals Tribunal, which could impose fines of up to KShs 20 million shillings (USD 20,000) if a person is found culpable under the law. While media bodies lodged a court case arguing that these two laws were oppressive and unlawful,[112] in May 2016, the High Court found the laws to be constitutional.[113]

[104]   Ethiopia row over 'massacre' leak http://news.bbc.co.uk/2/hi/africa/6067386.stm; Ethiopian protesters 'massacred'http://news.bbc.co.uk/2/hi/africa/6064638.stm

[105]   Ethiopia: Crackdown Spreads Beyond Capital https://www.hrw.org/news/2005/06/15/ethiopia-crackdown-spreads-beyond-capital; Why We Don't Hear About the Conflict in the Ogaden https://slate.com/news-and-politics/2007/09/why-we-don-t-hear-about-the-conflict-in-the-ogaden.html

[106]   533/2007 A Proclamation On Broadcasting Service

[107]   590/2008 A Proclamation to Provide For Freedom Of The Mass Media And Access To Information

[108]   RDC: 3e anniversaire de la fermeture de Radiotélévision Canal futur
https://www.radiookapi.net/actualite/2014/11/29/rdc-4e-anniversaire-de-la-fermeture-de-radiotelevision-canal-futur.

[109]   RD Congo : le journal Kisangani News suspendu pour trois mois,available at
https://www.agenceecofin.com/gestion-publique/1712-16010-rd-congo-le-journal-kisangani-news-suspendu-pour-trois-mois

[110]   Malawi Cracks Down on Media Covering Protests: 21st July 2011; 22nd July 2019: https://bit.ly/2Yp1QAJ

[111]   Malawi Amendment bans news 'not in public interest'; 1st February; https://bit.ly/2GpWwTz

[112]   Media bodies move to court to challenge new law https://www.nation.co.ke/news/Media-moves-to-court-to-challenge-new-law/1056-2156004-mhm6p6z/index.html

In Nigeria, 8 social media users, activists, and journalists were arrested under the Cybercrime Act between August 2016 to July 2017 for their online posts.[114] In August 2019, Omoyele Sowore, a publisher of Sahara Reporters and an opposition presidential candidates during the February 2019 presidential elections, was arrested and remains in custody for treasonable felony for using his social media and online platforms to call for protests in August 2019 against bad governance under the #RevolutionNow movement.[115]

Malawi's Electronic Transaction and Cyber Security Act, 2016 requires online content providers to conspicuously display on their webpage their full name, domicile, telephone number, and email address, of the editor if a natural person; and in case of a legal entity, corporate name, postal and physical address of the registered office, telephone number, email address, authorised share capital, and registration number, of the editor.[116] This in effect limits anonymity. The penalty for non-compliance is a custodial sentence of 12 months and a fine of K5,000,000 (USD 6,600).

In January 2016, Cameroonian journalists Baba Wame, president of the Association of Cyber Journalists, Rodrigue Tongue, a reporter who formerly worked for the privately owned daily Le Messager, and Félix Cyriaque Ebolé Bola, a reporter for the privately-owned daily Mutations, were charged before a Cameroon military court for failing to disclose information and sources that could harm national security.[117] The journalists who were first charged in October 2014, denied the charges, and faced jail terms of between one to five years and a fine between 50,000 and 5 million Central African Francs (US$83 to $8,257). However, the trio were acquitted of the charges in October 2017.[118]

Pastor Evan Mawarire who was one of the leaders of the successful #ThisFlag cyber movement in Zimbabwe, was arrested in June 2016 for "inciting violence and disturbing the peace" and "overthrowing or attempting to overthrow the government by unconstitutional means," but the court acquitted him of the charges.[119] The prominent Pastor was arrested again in January 2019 and released on a USD 2,000 bail, but faces charges of subversion and incitement to violence, punishable by up to 20 years in prison.[120]

In August 2017, controversial Kenyan blogger Robert Alai was arrested and forced to remove content from his Facebook platform.[121] The blogger posted photos of members of President Kenyatta's relatives mourning the death of a family member at a Nairobi hospital. In 2019 Robert Alai was again arrested and forced to delete content that he had posted on his Facebook page. The content related to photos of police officers who had been killed in a terrorist attack in Wajir County.[122] The government officials condemned the action and termed the move as "irresponsible" and accused the blogger of "glorifying terrorism". Alai responded stating that the post was justified and he was speaking for the poor police officers who are neglected, and their allowances taken by "wakubwa". On both incidents, Kenyans quickly took to social media demanding his freedom with the hashtag #FreeAlai in support of once fierce government critic, who despite becoming a Jubilee government supporter, had fallen victim to his masters.

113 Blow to media as court declares 'draconian laws' constitutional
https://www.the-star.co.ke/news/2016-05-27-blow-to-media-as-court-declares-draconian-laws-constitutional/
114 Freedom of the Net Nigeria https://freedomhouse.org/report/freedom-net/2018/nigeria
115 DSS arrests AAC presidential candidate, Omoyele Sowore https://punchng.com/dss-arrests-aac-presidential-candidate-omoyele-sowore/
116 Electronic Transaction and Cyber Security Act, 2016; https://bit.ly/2Cjmsy0
117 Three journalists face military trial in Cameroon https://cpj.org/2016/01/three-journalists-face-military-trial-in-cameroon.php
118 Cameroon: 03 years later, Rodrigue Tongué, Baba Wame and Félix Cyriaque Ebole acquitted by justice
https://www.lebledparle.com/societe/1103674-cameroun-affaire-des-3-journalistes-et-autres-rodrigue-tongue-baba-wame-et-felix-cyriaque-ebole-declares-non-coupables
-et-acquittes
119 Zimbabwe activist pastor Evan Mawarire walks free from court after charges dropped
https://www.dw.com/en/zimbabwe-activist-pastor-evan-mawarire-walks-free-from-court-after-charges-dropped/a-19398310
120 Zimbabwe pastor Evan Mawarire leaves prison on bail
https://www.dw.com/en/zimbabwe-pastor-evan-mawarire-leaves-prison-on-bail/a-47302613
121 Why Statehouse Operative Ordered CID Police to Arrest Blogger Robert Alai
https://www.kenya-today.com/politics/statehouse-operative-ordered-cid-police-arrest-blogger-robert-alai-arrested
122 Blogger Robert Alai arrested for posting gory photos
 https://www.capitalfm.co.ke/news/2019/06/blogger-robert-alai-arrested-for-posting-gory-photos/

Nigeria has made a series of attempts to regulate social media, including the adoption of the Cybercrime (Prohibition, Prevention etc) Law. In 2015, Nigeria attempted to pass the controversial Frivolous Petitions Prohibition Bill which was withdrawn in May 2016, following protests by citizens and advocacy by civil society organisations. In March 2018, Nigeria introduced a widely controversial Hate Speech Bill before the Senate to tackle hate speech and defamation online. The move raised concerns of the possibility of its usage to stifle freedom of expression and silence government critics. In June 2018, the Nigerian Senate announced the introduction of a new bill to regulate social media use.[123]

The announcement came months after the Senate had passed the Digital Rights and Freedom Bill first proposed in April 2015, which in March 2019, Nigeria's President Buhari declined to assent to. This was despite the Bill having been approved by the House of Representatives in December 2017 and the Senate in March 2018.[124] The Bill sought to provide for the protection of the human rights online, to protect internet users in Nigeria from infringement of their fundamental freedoms and to guarantee the application of human rights for users of digital platforms and/or digital media and for related matters. The president in a letter to the Senate stated that the bill covered too many technical subjects and failed to address any of them extensively. It remains to be seen whether the Senate will address the Presidents concerns and return the Bill for assent.

In February 2019, the Zimbabwean Cabinet approved the Maintenance of Peace and Order Bill, to repeal the Public Order and Security Act (POSA), a controversial and draconian law to align it with the constitution[125] as well as to respond to court rulings which declared some of its provisions unconstitutional.[126] However, the bill has been criticised as portraying only a titular change as opposed to substantive reform, as it has retained the vast majority of the provisions of POSA thus it is likely to sustain the legislative assault on democratic freedoms despite claiming the contrary. [127]

123 Nigeria and the Obsession to Regulate Social Media http://www.mfwa.org/issues-in-focus/nigeria-and-the-obsession-to-regulate-social-media/
124 Nigeria's president refused to sign its digital rights bill, what happens now?
 https://techpoint.africa/2019/03/27/nigerian-president-declines-digital-rights-bill-assent/
125 Media Reform Bill Approved by Zimbabwean Cabinet
https://www.prnewswire.com/news-releases/media-reform-bill-approved-by-zimbabwean-cabinet-300852354.html
126 Bills Digest On The Maintenance Of Peace And Order 2019 Https://Www.Parlzim.Gov.Zw/Component/K2/Bills-Digest-On-The-Maintenance-Of-Peace-And-Order-2019
127 An Analysis of the Maintenance of Peace and Order Bill, 2019 https://www.thezimbabwean.co/2019/07/an-analysis-of-the-maintenance-of-peace-and-order-bill-2019/

4.1.2 Disrupting Networks – From SMS Censorship to Social Media Blockage to Internet Throttling

Over the years, network disruptions have emerged as a major technique which various African governments have employed to stifle digital rights. The disruptions are mostly ordered by governments eager to disrupt communications and curtail citizens' access to information in order to limit what the citizens can see, do, or communicate. The disruptions have mostly been initiated around election times, public protests, and during national exams. In a number of cases, security agencies work with national communications regulators to order the disruption, mostly citing national security or public order considerations, and referencing the regulator's powers to order service providers to interrupt services.[128]

Early Years of SMS Blockage

Among the countries under study, the first recorded network disruption was in 2005, following the May post-election unrest in Ethiopia, when the government turned off SMS, claiming the opposition had been using SMS to organise protests. The service was unblocked after more than two years. The government also blocked access to independent websites and some popular blogging sites in the face of protests by the opposition.[129] Tests conducted between 2008 and 2010 on websites and blogs found extensive evidence of filtering of political content,[130] implying that the network disruption was part of a larger campaign by the Ethiopian government to thwart opposition organising through digital mediums.

Instructive also is that at the time, more African governments were moving to control ICT use during elections through other means than network disruptions. For instance, in February 2006, Uganda's communications regulator instructed ISPs to block access to www.RadioKatwe.com, a website that published anti-government gossip. Authorities alleged that the website was publishing "malicious and false information against the ruling party NRM and its presidential candidate." The February 2006 election was won by the incumbent, Yoweri Museveni.[131]

In Kenya, following the 2007 post-election violence, the government blamed communications mediums such as broadcast media and SMS for fanning the violence. It banned live broadcasting prior to the announcement of election results citing "public safety and tranquillity", prompting citizens to turn to SMS and social media to circumvent the traditional media blackout. The   Kenya government also disabled bulk SMS to prevent people from sending "provocative messages" or "hate speech".[132] The government thereafter established the National Cohesion and Integrated Commission (NCIC) in 2008 to aid in fighting online and offline hate speech.[133]

The obsession with repressive internet control measures picked up steam after the Arab Spring civilian uprisings in North Africa and Middle East countries, such as Tunisia, Syria, Libya, Yemen, and Egypt. The wave of demonstrations, uprisings, and riots that started in Tunisia in December 2010 and spread to other Arab states, had by February of 2012 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, by instigating citizens to mobilise and safely share information about the uprisings.

128   CIPESA, A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa, https://cipesa.org/?wpfb_dl=252
129   Bogdan Popa, Google Blocked in Ethiopia, http://news.softpedia.com/news/Google-Blocked-In-Ethiopia-53799.shtml
130   CIPESA,State of Internet Freedom in Ethiopia, https://cipesa.org/?wpfb_dl=178
131   CIPESA, Uganda's Assurances on Social Media Monitoring Ring Hollow, https://cipesa.org/2013/06/ugandas-assurances-on-social-media-monitoring-ring-hollow/
132   Social Media and Post-Election Crisis in Kenya https://repository.upenn.edu/cgi/viewcontent.cgi?article=1012&context=ictafrica
133   Footprints of peace https://www.cohesion.or.ke/images/docs/FOOTPRINTS-OF-NCIC.compressed.pdf

The year 2011 appeared to mark the start of a new and wide range of network disruptions that were related to elections in countries like Cameroon, DRC, and Uganda. In February 2011, the Uganda Communications Commission (UCC) directed telecom companies to block and regulate text messages that could instigate hatred, violence and unrest during the presidential election period. The regulator issued 18 words and names, which mobile phone SMS providers were instructed to flag if they were contained in any text message. These words included 'Tunisia', 'Egypt', 'Ben Ali', 'Mubarak', 'dictator', 'teargas', 'kafu' (it is dead), 'emundu' (gun), 'gasiya' (rubbish), 'army/ police/UPDF', 'people power', and 'gun/bullet'. Two UCC spokesmen confirmed the directive to local media, saying the aim was "to ensure free, fair and peaceful elections."[134] The head of the UCC said that "messages containing such words when encountered by the network of facility owner or operator, should be scrutinised and if deemed to be controversial or advanced to incite the public, should be stopped or blocked." Two months later in April 2011, UCC ordered the shutdown of access to social media platforms such as Twitter and Facebook in April 2011 during the "walk to work" protests led by the runner-up in the presidential poll, and were brutalised.[135]

In the DRC, the first shutdown of SMS services was witnessed in December 2011 following the disputed November 2011 election. The government claimed the move was necessary to prevent the spread of fake results online prior to the official announcement of results by the electoral commission.[136] The SMS disruption lasted 25 days.[137] In subsequent years, the DRC government ordered various other network disruptions that went beyond SMS, including in 2015, 2016, and 2018.

Continuing the trend of SMS blockage that year, in March 2011, Cameroonian authorities suspended mobile Twitter SMS services.[138] Telecom provider MTN Cameroon stated at the time that it had been informed that the suspension was because of what government officials termed "security reasons". It appears that the government was wary of a possible Arab spring uprising in the county following the annual commemoration of the hunger riots first held in February 2008 dubbed the "martyr's week" planned to take place when the suspension notice was issued.[139] The service was restored after ten days, following protests by Cameroonians.

In 2019, the verified Twitter account of a vocal Tanzanian opposition leader Zitto Kabwe was compromised, and several tweets posted from the account pledging Zitto's support to President John Magufuli. However, his wife immediately clarified that her husband had no access to his laptop or mobile phone, which was then confirmed by Zitto Kabwe himself later the same day.[140] Although no one took credit for the leakage of the hack, it shows possible pro-government hacking capacity.

Network Shutdowns Become Endemic

The year 2015 marked the start of widespread internet shutdowns and the practice has since been on the upswing well into the second half of 2019. Since 2015, the countries that have ordered network disruptions include Algeria, Burundi, the Central African Republic (CAR), Cameroon, Chad, DRC, Congo (Brazzaville), Egypt, Eritrea, Equatorial Guinea, Gabon, Ethiopia, Libya, Mauritania, Niger, Togo, and Zimbabwe. Others are Uganda, Mali, Morocco, the Gambia, Sierra Leone, Somalia, and South Sudan.[141] Most shutdowns affected the entire country, but in some instances, such as in Ethiopia and Cameroon, the disruptions targeted only regions affected by civic dissent and citizens' protests. In Gabon in 2016, following a total shutdown, the government subsequently instituted a 12-hour-a-day curfew on internet access.[142]

134 Uganda bans SMS texting of key words during poll,
http://www.reuters.com/article/2011/02/17/ozatp-uganda-election-telecoms-idAFJOE71G0M520110217
135 CIPESA (2016) State of Internet Freedom in africa https://cipesa.org/?wpfb_dl=225
136 Chris Welch, SMS and social media banned in Congo, deaf residents lose critical means of contact,
https://www.theverge.com/2011/12/19/2646721/sms-social-media-banned-congo
137 Arsene Tungali, The Evolution of Internet Shutdown in the DRC: https://cipesa.org/2017/03/the-evolution-of-internet-shutdowns-in-dr-congo/
138 Joshua Keating, Cameroon bans mobile Twitter service, https://foreignpolicy.com/2011/03/09/cameroon-bans-mobile-twitter-service/
139 MTN Cameroon asked to block Twitter
 https://www.iol.co.za/business-report/technology/mtn-cameroon-asked-to-block-twitter-1043582
140 @BwanaAnna on Twitter https://twitter.com/bwanaanna/status/1144168848926621696
141 CIPESA 2019: 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/
142 Under the Radar: Gabon's risky internet curfew, the world's first since 2011, http://globalriskinsights.com/2016/09/gabon-internet-curfew/

The use of internet control measures such as filtering, blocking, throttling and complete internet shutdown was reported in a number of countries in what appeared as attempts by governments to limit or control conversations online and prevent mobilisation for potential pro-democracy protests.

In 2010, the Burundi president sought to enhance his control of the regulator, ARCT. Through Article 1 of Law 100/47 of 15 November 2010, he removed the supervision of the ARCT from the telecoms ministry and transferred it to the Presidency.[143] Following this, in April 2015 the ARCT instructed all telecom operators providing mobile Internet to block access to social media platforms such as Facebook, Twitter, WhatsApp and Telegram for around 10 days.[144] The move was intended to bar protesters against the bid by President Pierre Nkurunziza for a new term in office in the July 2015 elections from using these platforms for mobilisation and the spread of hate speech.

Similarly in 2015, the DRC government ordered a shutdown of SMS and the internet in response to protests against a proposed Electoral Bill. The services were reinstated to banks and government agencies after four days, while access to the general public was restored after three weeks.[145] The following year, 2016, the DRC experienced another network disruption on the day president Joseph Kabila was expected to step down as president. The government ordered telecom operators to block social media sites in an attempt to thwart mobilising by protestors against the president's continued stay in power beyond his two-term limit.[146] In August 2017, telecoms regulator authority head issued a signed letter to operators stating that a shutdown was necessary "in order to prevent the exchange of abusive images via social media."[147] In December 2018, the DRC witnessed another internet disruption which lasted 20 days. The disruption occurred during the election period and commenced a day after general elections on December 31, 2019. It was lifted on January 19, 2019, the day the Constitutional Court was to announce the final results of the general election.

While the DRC ranks highly in the number of internet disruptions ordered, Cameroon earned its disrepute for ordering one of the longest-running disruptions in Africa. The Cameroon government ordered a 93-day internet shutdown nationwide between January and April 2017. This was in response to a series of peaceful protests by teachers, students, and lawyers between October and November 2016 against unfavourable government policies, including the alleged marginalisation of Anglophone regions of the central African country. The internet had been instrumental in mobilising for the protests. At the time of ordering this shutdown, the communications ministry sent mass SMS to mobile phone users across the country warning them of imprisonment for propagating false information on social media. Cameroon does not have a specific law on social media, but uses Law No. 2010/012 on cybersecurity and cybercrime through which one can be held criminally liable if they cannot attest to the veracity of information published online.[148]

In the lead up to the disputed October 2018 election, the online environment in Cameroon featured incidences of propaganda, hate speech and incitement, further fuelling the Anglophone crisis that began in October 2016.[149] Meanwhile, between October 2017 and February 2018, parts of Cameroon yet again experienced a complete internet shutdown, while others had unstable mobile telephone network and limited internet access, with access to Facebook and WhatsApp slowed down considerably on Election Day. It was revealed that the government had met with Facebook representatives to seek assistance to tackle the spread of rumours, misinformation and 'fake news', yet it was also perpetrating the same online. [150]

[143]   Decree N ° 100/47 OF 15 November 2010 Establishing the "ARCT" Telecommunication Regulation and ControlL Agency Under the Tutelage of the Presidency of the Republic, http://www.presidence.bi/spip.php?article884#

[144] Update on the State of Internet Freedom in Burundi https://cipesa.org/2015/06/update-on-the-state-of-internet-freedom-in-burundi/

[145] Tungali (ibid)

[146] Congo asks companies to block social media before anti-Kabila protests :https://www.reuters.com/article/us-congo-politics-telecoms-idUSKBN14420M

[147]   Patient Ligodi, "Congo orders internet slowdown to restrict social media: telecoms source," https://www.reuters.com/article/us-congo-violence-internet-idUSKBN1AN2DE

[148] Text of the law: https://www.minpostel.gov.cm/images/Les_textes/Lois/Loi_2010-012_cybersecurite_cybercriminalite.pdf

[149] Internet Without Borders, Elections in Cameroon: Ideas to fight disinformation online and hate speech, http://bit.ly/2lD8TE4

[150] Daniel Finnan, Cameroon 'fake' election observers mask the truth about reality of presidential polls, http://bit.ly/2lCATrK

Ethiopia is another country that has over the years experienced multiple and long-running network disruptions. Following uprisings in some regions, the government continuously blocks social media sites and carried out national and regional internet blackouts, often claiming national security threats or the need to stem cheating during national exams.[151] More than 12 government-ordered internet disruptions have been recorded in Ethiopia over the last couple of years.[152] In Uganda, the government ordered the shutdown of internet access on the eve of the presidential elections voting day, citing "national security", as well as during the inauguration in May 2016, affecting social media platforms including Facebook, Whatsapp, Twitter and mobile money transfer services.[153]

In January 2019, Zimbabwe ordered a countrywide internet shutdown following massive protests against a 150% fuel price hike and the struggle for economic justice.[154] President Mnangagwa justified the shutdown on Twitter stating that: "social networks (were) being used to plan and incite disorder and to spread misinformation leading to violence. In response, the decision was taken to temporarily restrict access to prevent the wanton looting and violence, and to help restore calm."[155] In July 2016 the government had ordered telcos and ISPs to block access to social media platforms, as a way to disrupt online organising and strikes organised by the #ThisFlag social movement.

In November 2017, Nigerian internet service providers blocked 21 websites at the request of NCC and the national security adviser. Following tests done by Paradigm Initiative and the Open Observatory of Network Interference (OONI), it was discovered that the blocked sites largely promoted the independence of Biafra, the region that attempted to secede from Nigeria in 1967 in the Biafran War. The common techniques adopted by ISPs included TCP/IP blocking by Globacom, DNS tampering by MTN and blocking the HTTP layer by Airtel.[156] In Rwanda, a number of independent online news outlets and critical blogs remained unavailable between 2014 and 2015, joined by three BBC websites in October 2014 following the government's outcry against the television broadcast of the documentary, "Rwanda, The Untold Story. "[157]

151   Freedom of the Net Report 2017, https://freedomhouse.org/report/freedom-net/2017/ethiopia
152   Access Now Shutdown Tracker,https://internetshutdowns.in/
153   Social Media Blocked in Uganda Ahead of President Museveni's Inauguration,
https://advox.globalvoices.org/2016/05/11/social-media-blocked-in-uganda-ahead-of-president-musevenis-inauguration/
155   First total internet shutdown in Zimbabwe, https://bulawayo24.com/index-id-news-sc-national-byo-153712.html
156   President Mnangagwa Justifies Internet Shut Down, Although "He Deeply Believes In Freedom Of Speech And Expression",
https://www.techzim.co.zw/2019/01/president-mnangagwa-justifies-internet-shut-down-although-he-deeply-believes-in-freedom-of-speech-and-expression/
157   Measuring Internet Censorship in Nigeria, https://internetinitiative.ieee.org/newsletter/december-2018/measuring-internet-censorship-in-nigeria
     Freedom House (2015) Freedom of the Net 2015/Rwanda https://freedomhouse.org/report/freedom-net/2015/rwanda

4.1.3 Surveillance Galore: The Build-Up of States' Capacity

Despite the existence of several provisions within the legal and policy frameworks, by 2005 reports of surveillance and interception of communication in the study countries were few. However, governments have in successive periods continued to enhance their technical capacity to intercept and conduct surveillance. Part of the lessons have been from each other, and from world super powers such as the US, Russia and China, from whom they purchase the technologies.

Going High-Tech to Implement Surveillance

Buoyed by an enabling legal framework, several governments moved to enhance their technical capacity for surveillance and interception of communication through the installation of software with capacity to surveil online, ordering communication service providers to monitor and intercept private communication. In 2006, the Ethiopian government established the Information Network Security Agency (INSA), and set up the country's first cyber intelligence unit. The national security and intelligence apparatus consistently targeted opposition groups, activists, journalists, and researchers with malware attacks for years.

In 2011, the Ethiopian government established the Federal Police Commission with power to investigate crimes relating to information network and computer system and install CCTV cameras. This move facilitated mass surveillance of citizens, in the absence of clear information as to the capabilities of the system and general oversight. In 2013, the government re-established the National Intelligence and Security Services with a ministerial status and as an autonomous body of the federal government.[158] In March 2012, Kenya's telecommunications regulator, the Communication Authority wrote to internet service providers seeking their cooperation in the installation of Network Early Warning System (NEWS) tool in order to detect cyber threats and respond to cyber incidents by monitoring network traffic.[159]

In Uganda, the government is reported to have enhanced its mass surveillance capacity through the use of spyware, intrusion malware, and intelligent network monitoring systems.[160] A Privacy International report showed that around 2012, the government collaborated with 21 hotels in Entebbe, Kampala, and Masaka thronged by key opposition leaders, diplomats, and journalists to install FinFisher, a Wi-Fi and desktop intrusion malware in the hotels' business centres.[161] Leaked emails of the correspondence between Hacking Team, a malware manufacturer, and Uganda Police Force (UPF) between April and July 2015, revealed plans to procure Hacking Team's premium Remote Control System (RCS) creatively named Galileo, or sometimes Da Vinci.[162]

In June 2014, the Kenyan government awarded Safaricom, the largest mobile phone services provider, a tender to set up a communications and security surveillance system at a cost of 14.9 billion shillings ($14.9 million). The CCTV system installed outside public places and key roads was procured from Huawei, and provides a direct link all security agencies electronically to a central command centre.[163] The controversial system was installed in the absence of a privacy law, which has seen footage from the cameras shared on social media. Moreover, it heightened fears of the public of the country turning into a police state.

In April 2014, Rwanda's abuse of its surveillance powers was revealed in the trial against popular singer Kizito Mihigo, private WhatsApp and Skype messages with alleged opposition critics in exile were used against him as evidence to convict him of conspiracy to overthrow the government. He was sentenced in February 2015 to 10 years in prison.[164]

158   804/2013 A Proclamation To Re-establish The National Intelligence and Security Service
159   CCK to spy on Internet users
https://www.nation.co.ke/news/CCK-to-spy-on-Internet-users-/1056-1370842-dux0xd/index.html
160   Privacy International, "State of Privacy Uganda," January, 2019, available at
https://privacyinternational.org/state-privacy/1013/state-privacy-uganda#commssurveillance
161   Privacy International, "For God and My President: State Surveillance In Uganda," October, 2015, available at
https://www.privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf
162   Daniel Mwesigwa, "Leaked Emails: How Hacking Team and Uganda government want to spy on you," July 22, 2015, available at
https://www.dignited.com/14494/leaked-emails-how-hacking-team-and-uganda-government-want-to-spy-on-you/
163   Safaricom reveals Huawei involvement in CCTV tender https://www.standardmedia.co.ke/article/2000125287/safaricom-reveals-huawei-involvement-in-cctv-tender
164   Freedom House (2015) Freedom on the Net 2015/Rwanda https://freedomhouse.org/report/freedom-net/2015/rwanda

In Botswana, rather than being a tool for public good, the country's security intelligence services and especially the DISS were used as ideological state apparatuses.[165] They served the interests of the elites, notably the president and his ruling colleagues. During this period, DISS and the Military Intelligence Unit are suspected to have acquired state of the art surveillance equipment from Israel in the run up to the 2014 general election, with capability to spy on both the internet and telephone conversations and jam radio and mobile signals acquired from Israel. The country's military intelligence unit is also believed to run a separate surveillance operation.

The then President Ian Khama was in 2014 blamed for transforming Botswana "into a surveillance state" leading to "fear and paranoia" and the loss of "the very peace of mind he claimed to be protecting."[166] The Parliamentary Committee of the Intelligence and Security (PCIS) was criticised for being weak in its oversight role, as its members are appointed by the President, hence it lacks independence from the executive, and that it lacked access to critical information relating to DISS thus was rendered clueless on DISS operations. In February 2015, it was revealed that DISS had spent USD 64.7 million on reconnaissance equipment from a German based company to spy on the opposition politicians, journalists and human rights lawyers.[167] The surveillance technology called FinSpy Mobile and FinSpy PC are capable of infecting computers and mobile phones on a mass scale with malware and allow remote monitoring of user activity and to siphon data from the devices.

In January 2015, Zimbabwe's former president Robert Mugabe received a 'gift' from Iran comprising various cyber-surveillance technologies, including International Mobile Subscriber Identity (IMSI) catchers.[168] The equipment was said to aid the government to keep its foreign policy foes at bay, and ratchet up suppression and snooping on political opposition and other organisations it considered a national security threat. Similarly, in Malawi, MACRA's decision to introduce Consolidated ICT Regulatory Management System (CIRMS) "spy machine" in 2011 was seen as an attempt to introduce spying in Malawi. MACRA argued that the system was intended to aid the monitoring the quality of telecommunication services and to protect the public from overcharging by the telecommunication companies. The implementation of the system was however challenged in court which ruled that the implementation of the machine as the court ruled that it indeed had the potential to violate article 21 of the constitution.[169] However, the same was later approved for implementation in 2016 following an appeal by MACRA to the country's Supreme Court.[170]

Tanzania's interest in advancing its surveillance was revealed in a Wikileaks report in July 2015. The report revealed communication between a Tanzania Statehouse official Eliezer Mabula and Emad Shehata, a key account manager of Hacking Team planning a visit to HackingTeam offices in Milan, Italy.[171] Hacking Team sells offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations.[172]

In April 2017, Tanzania signed an agreement with South Korea to enhance Tanzania's cyber capabilities. Under the five-year Memorandum of Understanding (MoU), the Korea Internet & Security Agency (KISA) would offer Tanzania expertise, monitor the security of the cyber infrastructure as well as put money into the sector.[173] In March 2018, Israel and Tanzania entered into military training and intelligence gathering and sharing agreement. The countries agreed to intensify their collaboration in key defense and security matters, particularly in troops training, cyber and inter-territorial security as well as improved military technology.[174]

165 Branston, G. and Stafford, R. (1996), The Media Student's Book. London and New York: Routledge

166 KHAMA TURNS BOTSWANA INTO A SURVEILLANCE STATE http://www.sundaystandard.info/khama-turns-botswana-surveillance-state

167 Botswana Guardian (2015), 'DIS launches massive surveillance operation', Feb. 23:
http://www.botswanaguardian.co.bw/news/item/1284-dis-launches-massive-surveillance-programme.html

168 Iran gives Mugabe Spy-Technology https://bulawayo24.com/index-id-news-sc-national-byo-61558-article-iran+gives+mugabe+spy-technology.html

169 Spy-Machine Brings Telecoms Fear, November 2011; http://bit.ly/2LkSUnD

170 "Spy-Machine" ready August, July 2019; http://bit.ly/2NGD4Go

171 I: RE: R: RE: R: R: R: INVITATION TO VISIT HACKING TEAM OFFICES
https://wikileaks.org/hackingteam/emails/emailid/16764

172 Hacking Team https://en.wikipedia.org/wiki/Hacking_Team; @Hackingteam https://twitter.com/hackingteam?lang=en

173 Dar Seoul team up against rising cases of cybercrimes https://www.dailynews.co.tz/news/dar-seoul-team-up-against-rising-cases-of-cybercrimes.aspx

174 Tanzania And Israel Sign Military Training And Intelligence Gathering-Sharing Agreement
https://intelligencebriefs.com/tanzania-and-israel-sign-military-training-and-intelligence-gathering-sharing-agreement/

Following the political clash between high ranking officials of Tanzania's leading party Chama Cha Mapindizu (CCM) in 2019, audio recordings of phone conversations between senior government official were leaked and spread on social networks discussing their private matters where the president was insulted.[175] The source of the leak remains unknown but it suggests the capability of surveillance. The President has since forgiven the officials.[176]

In July 2018, the Uganda Communications Commission (UCC) installed an Intelligent Network Monitoring System (INMS) with the capacity to track all calls made on all networks, mobile money transactions, fraud detection and billing verification.[177] The system is hosted on communications infrastructure owned by mobile network operators, and the UCC will be able to monitor multi-vendor data, network performance, and customer experience records, among others.[178] The president had long accused telcos of tax evasion and under-reporting revenues to the government.[179] In January 2018, it was revealed that the UCC had set up a Centralized Equipment Identity Register system in a bid to identify, and stamp out fake and illegal mobile devices said to be hazardous to health and used to commit crime.[180]

Copying Models from Super Powers

The internet governance models in world powers such as China, US and Russia have influenced African governments in adopting digital authoritarianism. The autocratic Chinese model appears to be gaining acceptance in the continent. It comprises widespread and sophisticated automated surveillance, online content manipulation, arrests of critics, content removal, data collection, repressive laws to censor online media, violence against digital activists, technical attacks against dissidents, the great firewall blocking foreign social media, websites and messaging apps, revocation of mobile and internet connectivity.[181]

These measures by world powers have become attractive to African governments and many have embraced the examples to enable them to consolidate power and manage domestic instability. As argued in the Foreign Policy, states such as Tanzania apply the "...'rule by law' method, popularized by Vladimir Putin's regime in Russia, which allows leaders to manipulate legal processes for their own purposes while avoiding the international condemnation that typically comes with images of brutality."[182] The hardware and technology that is used to run the surveillance systems are not made in Africa. There are private firms around the world that are exporting dual-use surveillance technologies to enable censorship, surveillance and other similar practices.

Further, dual-use applications allow application in both civilian and security spaces, and as such, can be used legitimately to filter and block malware, and at the same time filter and censor online content.[183] African countries such as Angola, Ethiopia, South Africa, Rwanda and Egypt have imported such software from China. Further, Zimbabwe imported a dual-use AI based application from China. The use of AI has potential for more intelligent, automated censorship and surveillance. Moreover, countries like Tanzania and Nigeria have benefited from infrastructure build-outs from China that have resulted in its increased influence[184] and enhanced crackdown on internet content.[185] China was rated as the "worst abuser of internet freedom in 2018" by Freedom House.[186]

175 https://dev.invidio.us/watch?v=A0IdYOyy4lM; https://dev.invidio.us/watch?v=GdVc1ZTBWYU
176 President Magufuli says he forgave January Makamba and William Ngeleja https://www.thecitizen.co.tz/news/1840340-5260274-9btpfa/index.html
177 ITWeb Africa, Uganda's UCC, telcos clash over network monitoring technology, https://bt.ly/2NEMVON
178 Government installs system to track telecoms revenues, https://bt.ly/2OQDXU
179 All Africa, Uganda: Fight Over Shs44Trillion Mobile Money, https://allafrica.com/stories/201802260042.html
180 Unwanted Witness, Uganda Communication Commission sets up mobile phone monitoring system,
https://unwantedwitness.or.ug/uganda-communication-commission-sets-up-mobile-phone-monitoring-system
181 Freedom on the Net 2018 https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism
182 Hilary Matfesss and Jeffrey Smith, "Africa's Attack on Internet Freedom," July 13, 2018, available at
https://foreignpolicy.com/2018/07/13/africas-attack-on-internet-freedom-uganda-tanzania-ethiopia-museveni-protests/
183 The Long View of Digital Authoritarianism https://www.newamerica.org/weekly/edition-254/long-view-digital-authoritarianism/
184 Beijing Wants to Rewrite the Rules of the Internet https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/
185 Tanzania cyber law introduces $900 fees for bloggers, compulsory passwords
https://www.africanews.com/2018/04/12/tanzania-cyber-law-introduces-900-fees-for-bloggers-compulsory-passwords//
186 Freedom of the Net 2018 https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism

In 2017, Tanzania's Deputy Minister for Transport and Communications Edwin Ngonyani was quoted saying "Our Chinese friends have managed to block such media in their country and replaced them with their homegrown sites that are safe, constructive and popular. We aren't there yet, but while we are still using these platforms we should guard against their misuse".[187]

AI, the Game Changer

In 2018, Uganda, like Kenya before in 2017, commissioned the first phase of installation of CCTV cameras in Kampala capital city and surrounding areas is an attempt to curb the spate of assassinations and urban crime, at least according to Museveni.[188] However, the high-profile killings and cases of homicide remain at large. On August 15, 2019, The Wall Street Journal (WSJ) published an investigative piece on how "Huawei Technicians Helped African Governments Spy on Political Opponents".[189] The article detailed how Huawei had helped the Uganda Police Force infiltrate encrypted communication channels used by a key opposition leader. Notably, it also mentioned Uganda's plans to open a new six-story USD 30 million hub in November 2019, which will be linked to the over USD 104 million "Smart Cities" project implemented by Huawei. The project will utilise Huawei advanced facial-recognition (Artificial Intelligence) technology to "address crime and safety in Uganda". However, lack of data protection and privacy regulations and established codes of ethics and human rights concerning facial recognition based surveillance threaten the right to privacy and freedom of expression and assembly.

The use of Artificial Intelligence was also reported in Zimbabwe in March 2018, that the government had 'strategic' partnership with the Chinese company – Cloudwalk Technology, for the conduct of a large-scale facial recognition programme primarily used in traffic management, security and law enforcement and with the possibility to be extended to other public programmes. Under the project, the government will build a national facial database, and then share it with the Chinese government, to help it "train the racial bias out of its facial recognition systems." Similar deals have been signed in Angola and Ethiopia.[190]

There are no adequate checks and balances on the design, deployment and use of digital surveillance technologies that are currently in use.[191] While surveillance for example, is permitted in the legislation of the countries under the study, the risk is that the practice will go unchecked as the technologies become more sophisticated, undetectable and widespread. Further, it is more difficult to hold the governments or the companies that develop and sell such systems to governments accountable, owing to the secretive nature of their operations and their covert systems that continue to make it difficult to even establish their existence in telecommunications networks.

187 Tanzania: Govt Seeks Chinese Help in Social Media
https://www.theeastafrican.co.ke/news/Tanzania-seeks-Chinese-help-in-social-media/2558-4041306-d66m76z/index.html
188 Vision Reporter, "Museveni commissions CCTV cameras," October 9, 2018, available at
https://www.newvision.co.ug/new_vision/news/1487292/museveni-commissions-cctv-cameras
189 Joe Parkinson, Nicholas Bariyo and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," August 15, 2019, available at
https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017
190 Arthur Gwagwa and Lisa Garbe, "Exporting Repression? China's Artificial Intelligence Push into Africa." December 17, 2018, available at
https://www.cfr.org/blog/exporting-repression-chinas-artificial-intelligence-push-africa
191 Digital authoritarianism and the threat to global democracy https://thebulletin.org/2019/07/digital-authoritarianism-and-the-threat-to-global-democracy/

4.1.4 The Push Towards Determining Identity Amidst Poor Oversight

Once governments were able to intercept communication, resolving the identity question then remained just a matter of time. Measures have been introduced progressively in the countries under review to enable governments identify any telecommunication services user with precision. From SIM card registration, governments have since adopted digital identities and incorporated biometrics and artificial intelligence, albeit with poor or no oversight.

SIM Card Registration

This 2006-2010 period marked the introduction of massive personal data collection across several African countries. This was despite the absence of data protection laws. Countries such as DRC and Senegal introduced laws and requirements for communication service providers to register the SIM cards of all their subscribers.

In 2007, the DRC government issued Decision No. 005/ARPTC/CLG/2007 of 29 June 2007 requiring the telecoms regulatory authority to register mobile telephony services subscribers in the interest of national security.[192] in a subsequent Inter-Ministerial Order two years later, mobile operators were given six months to collect their subscribers' details, and were required to continue transmitting this information to the ARPTC, the regulator, every six months. Similarly, Senegal adopted Decree 2007-937 of 7 August 2007 requiring operators of public telecommunications networks to register SIM card buyers and users.[193]

Other countries were to follow suit, and by 2019, all the countries under review had introduced mandatory SIM card registration as part of their laws, including biometric registration for purposes of issuance of national identification. The personal information collected is similar in the countries. The consequence of non-registration of SIM cards has been their switch off.[194]

In April 2014, the Burundian government introduced Law No 100/97 of 18 April 2014, on conditions of exploitation of the electronic communication sector, an amendment to the Ministerial Law No 520/730/540/231 of 9 April 1999[195] which required telecommunication service providers under Article 29, to collect accurate and up-to-date information on the identity of subscribers and submit the same to the ARCT. This law was complemented by Order No 1 of 8 April 2014 by the ARCT which then required SIM card registration and personal information such as names, detailed address, places and dates of birth, a copy of national identity cards and passport photographs provided.[196]

Likewise, the Postal and Telecommunications Regulations Statutory Instrument 95 of 2014 (Subscriber Registration) of Zimbabwe requires all telecommunications companies to create a centralised subscriber database of all their users.[197] The database is managed by POTRAZ who claim to use it, among other things, to assist law enforcement agencies for safeguarding national security, as well as authorising access for the purposes of research in the sector. The government through POTRAZ in June 2016, issued threats to the public, highlighting the fact that perpetrators of "abusive and subversive materials" would be identified, disconnected and arrested.[198]

192　Decision on Identification of mobile phone users in the DRC (Regulatory Authority):
https://www.droitcongolais.info/files/73520_decision_du_29_juin_2007_de_lautorite_de.pdf

193　Decree No 2007 - 937 http://www.osiris.sn///IMG/pdf/document_Decret_relatif_a_lidentification_des_abonnes_153.pdf.

194　Edge, "Telecoms switch off sim cards, MTN appeals to clients," http://edge.ug/2017/05/20/telecoms-switch-off-sim-cards-mtn-appeals-to-clients/; see also Taddeo Bwambale, "Unverified SIM cards switched off," The New Vision, May 20, 2017, https://www.newvision.co.ug/new_vision/news/1453641/unverified-simcards-switched

195　Text of the law http://www.arct.gov.bi/images/decretslois/decret1.pdf

196　Order No 1 of 8 April 2014 http://www.arct.gov.bi/images/circulaires/circulaire2.pdf

197　Replaced Statutory Instrument 142 of 2013 "Postal and Telecommunications (Subscriber Registration) Regulations, 2013".

198　Nation heeds stay away call https://www.newsday.co.zw/2016/07/nation-heeds-stay-away-call/

In 2013, in an "explanatory note on the Subscriber Identification Project",[199] the Senegalese Telecommunications and Postal Regulatory Authority (ARTP) relaunched the SIM card registration project. The Authority did so under the pretext of fighting crime linked to the use of mobile telephones. Some of the information required included a family name, first name and CNI (ID) number. A similar project commenced under Decree No. 2007-937 of 07 August 2007 was not effective due to the resistance of both mobile operators and users. Kenya introduced SIM card registration in 2015 requiring all mobile network providers under rule 4 of the Kenya Information and Communications Act (Registration of SIM cards) Regulations, 2015 to register all SIM card subscribers.[200] Failure to provide the information as per SIM card regulations is an offence punishable by a fine of KES 300,000 (USD 3,000) or to imprisonment for a term not exceeding six months, or both.

In September 2015, Cameroon's Telecommunications Regulatory Board (ART) introduced a new decree to reinforce and clarify the procedures related to the identification of mobile subscribers in the country. The country's operators MTN, Orange, Viettel (Nexttel) and CamTel were required to update their subscriber databases, following which any unregistered SIM cards would be deactivated. The new rules also limited a subscriber's SIM ownership to three SIM cards per operator. In 2016, Malawi through MACRA started implementing mandatory SIM card registration, introduced under the Malawi Communications Act, 2016.[201] The details required included the full name of the subscriber; the identity card number, or any other official document; and the residential and business or registered physical address of the subscriber.[202]

In July 2019, the Cameroon Telecommunications Regulatory Board (ART) cracked down on mobile operators and fined them a combined FCFA 3.5 billion (USD 5.9 million) for failing to comply with SIM registration rules. Orange Cameroon was also fined FCFA 1.5 billion, while market leader MTN and Vietnamese-owned Viettel (Nexttel) were each fined FCFA 1 billion.

While the commonly held view is that SIM registration is useful to prevent cybercrimes, attention is not paid to the potential of the use of the information for surveillance of key groups such as whistle-blowers, human rights defenders, the political opposition and the media.

Rapid Adoption of Biometric Data Collection

Following the controversial 2011 elections, Cameroon's Electoral Commission adopted the use of biometric technology in February 2012 for the management of the elections. Biometric voter registration commenced in April 2013 and is updated every year. In August 2013, the Ministry of Interior of Burundi announced the introduction of biometric ID cards to replace the traditional paper-based identity cards to provide more accurate information about individuals.[203]

Ethiopia introduced the Vital Events and Registration Proclamation in 2012.[204] The law proposed the introduction of national identity cards with identification numbers for citizens. It also requires the collection and storage of biometrics of citizens in a centralized system. Also, that the stored information could be disclosed to other organs for specified purposes such as national intelligence and security, crime prevention and investigation, tax collection, administrative and social services, implementation of financial risk management, and other purposes promulgated by law.

In February 2012, the Tanzania National Identification Authority (NIDA) began registering citizens' information for national identification cards (NIDs) issuance. In October 2015, Tanzania introduced a decentralized Biometric Voter Registration (BVR) process, coupled with the issuance of a voter's card.[205] The system enabled the data collectors to determine the eligibility of citizens in minutes, record their data (photo, fingerprints, signature) and immediately issue a secure voter card. The electronic identification cards was introduced to curb electoral fraud ahead of the 2015 general elections, which process saw the detection of 231,955 cases of multiple registrations.

---

199 Note explicative sur le projet de l'identification des abonnés
https://www.artpsenegal.net/sites/default/files/docs_basics/note_sur_le_projet_de_lidentification_des_abonnes_vf.pdf
200 Regulations https://ca.go.ke/wp-content/uploads/2018/02/Registration-of-SIM-%E2%80%93Cards-Regulations-2015-1.pdf
201 Communications Act 2016; https://bit.ly/2Oi6JYs
202 Be Patriotic, Register Your SIM Card, 2018; https://bit.ly/2y3oW1c; Over 6 million Malawians Registered in First Three Phases of Mass National Registration, 2017;
https://bit.ly/2Y8trCa
203 A biometric identity card soon to be functional in Burundi http://fr.igihe.com/spip.php?page=mv2_article&id_article=5986
204 Registration of Vital Events and National Identity Card Proclamation, Proclamation No.760/2012:
https://chilot.me/wp-content/uploads/2017/04/proclamation-no-902-2015-registration-of-vital-events-and-national-identity-card.pdf
205 Instant Issuance of 24 Million Voters Cards in Tanzania https://www.evolis.com/sites/default/files/atoms/files/evolis_success_story_tanzania_votercards-en_web_1.pdf

The use of cyber-attacks was noted in Botswana. In January 2016, Mmegi, an independent newspaper in Botswana, experienced a cyber-attack that destroyed a significant amount of its archived material.[210] Mmegi's editor claimed that the Directorate of Intelligence and Security Services (DISS) was behind the attack, and that it had been carried out as retaliation for an article claiming that the Directorate on Corruption and Economic Crime (DCEC) had questioned the former head of DISS about the wealth he had purportedly amassed.

In September 2017, the Ethiopian government, through the Ministry of Communication & Information Technology (MCIT), embarked on the process of registering mobile phones on Ethio telecom network which has over 50 million subscribers.[211] The system matches each mobile device with the SIM card of the particular user using IMEI, a unique number given automatically to identify GSM, WCDMA, and iDEN mobile phones, as well as some satellite phones. Mandatory SIM card registration in Ethiopia requires users to provide their names, photo ID, signature, relatives' phone numbers, and addresses.

In March 2018, the Tanzania Communications Regulatory Authority (TCRA) launched a project to register the owners of 43.2 million active SIM cards using biometric technology.[212] Following this, all SIM cards will have to be registered through biometric technology, using NIDA IDs or at least a NIDA registration number from May 1, 2019 and is expected to be completed by December 2019. Moreover, in January 2018, Tanzania commissioned a new electronic East African Community passport to replace the existing passport, set to be phased out by January 2020. The e-passport contains the holder's biometric information on a tamper-proof page, to curb fraud and ease clearance at immigration. The move followed a directive from the 35th EAC Council of Ministers meeting in April 2017 for member states to issue e-passports by January 2018. Kenya launched a similar document in September 2017.

In September 2018, Nigeria's Federal Executive Council (FEC) approved the immediate commencement of the implementation of a strategic roadmap for Digital Identity Ecosystem in Nigeria[213] According to the National Identity Management Commission (NIMC), the process will see the effective and efficient mass enrolment of Nigerians and legal residents in Nigeria into a centralized, secure National Identity Database where digital identities in the form of the National Identification Number (NIN) will be issued, and its use made mandatory for transactions from January 2019.[214]

Similarly, in January 2019, President Kenyatta announced the development of a central master population database, known as the National Integrated Identity Management Systems (NIIMS), which would be the authentic 'Single source of truth' on personal identity in Kenya.[215] The database is expected to replace the integrated Population Registration System (IPRS), and contain information on all Kenyan citizens as well as foreign nationals residing in Kenya. For each registration, the system will generate a unique identification number known as Huduma Namba.[216] The mass registration process was conducted in May 2019, and captured the details of 37.7 million people.[217]

206 The National Registration Identification System for Malawi; https://bit.ly/2GjevLp
207 Moving Towards Harmonised a National Identity System in Malawi; 29th October 2019: https://bit.ly/2M4pEDl
208 National Registration and Identification System; 1st November 2016; https://bit.ly/2SFt40V
209 Personal interview with Michael Kaiyatsa, CHRR's Programme Director, 23rd August 2019
210 Freedom House. (2016). Botswana : Freedom in the world. https://freedomhouse.org/report/freedom-world/2016/botswana
211 Ethiopia government in mobile phone registration drive to curb smuggling, fraud
http://aptantech.com/2017/09/ethiopia-government-in-mobile-phone-registration-drive-to-curb-smuggling-fraud/
213 Biometric Sim listing set to start https://www.thecitizen.co.tz/news/1840340-5075938-89eetq/index.html
214 FEC Approves Implementation of Strategic Roadmap for Digital Identity Ecosystem in Nigeria
https://www.nimc.gov.ng/fec-approves-implementation-of-strategic-roadmap-for-digital-identity-ecosystem-in-nigeria/
215 The Digital Identity Ecosystem https://www.nimc.gov.ng/digital-identity-ecosystem/
216 Speech by Uhuru Kenyatta
http://www.president.go.ke/2019/01/22/speech-by-his-excellency-hon-uhuru-kenyatta-c-g-h-president-and-commander-in-chief-of-the-defence-forces-of-the-republic-of-kenya-during-a-meeting-with-senior-security-officials-at-state-house-mo/
217 Huduma Namba http://www.hudumanamba.go.ke/
   Another Huduma Namba listing planned for those who missed out
   https://www.the-star.co.ke/news/2019-07-06-government-plans-for-another-huduma-namba-listing/

4.1.5   Enter The Era of Social Media and Data Taxation

One of the notable and concerning phenomena of the more recent years is the use of taxation to undermine citizens' use of the internet. In some instances, such measures have been designed partly as a clear measure to limit how many citizens can access digital technologies and use them to hold governments to account. In other instances, governments have been eager to increase revenues from the telecom sector, and particularly, from over-the-top (OTT) services, which they claim are eating into the revenues of licensed telecom operators. In the last two years, enhancing taxes on airtime, data bundles and social media access appears to be evolving as a pattern with the countries under review. These costs are usually passed on to consumers, thereby raising the cost of owning and using a mobile phone and the internet.[218]

Zimbabwe was an early adopter of such brazen measures, where in August 2016, the government increased mobile data prices overnight by 500%. The move was seen as part of government efforts to quash activism on social media around the #ThisFlag movement.[219] The government, through POTRAZ, also ordered mobile networks to suspend data bundle promotions until further notice.[220] In January 2017, the government increased the cost of the data tariffs by a further 2,500%.[221] The move was caused uproar amid speculation that it was part of the government's sinister way of forcing millions of users off social media platforms. It was criticised as retrogressive, insensitive and politically-motivated onslaught on freedom of expression ahead of the 2018 elections. In June 2018, the government almost 60% reduction in the cost of mobile data.[222] However, in August 2019,[223] NetOne a telecom company increased the cost of data bundles by 300% in August 2019. Operators had increased the cost of bundles in April 2019, citing the cost of doing business.[224]

In similar fashion, Tanzania adopted the Electronic and Postal Communications (Online Content) Regulations in March 2018 making it compulsory for bloggers and owners of other online forums such as discussion forums and online television and radio streaming services to register with the regulator. Online content creators[225] are to pay application fees of USD 43.7, initial three year license fees of USD 437 and renewal fees of a similar amount. The penalty for non-compliance is a fine of USD 2,186. and pay up to USD 900 for a license. Anyone convicted under the regulations faces a fine of at least 5 million shillings (USD 2,200), imprisonment for a minimum 12 months, or both. Subsequently, the TCRA warned that it would take legal action against all unlicensed websites if they did not comply with the law by June 15, 2018. The move led to the immediate suspension of all unregistered bloggers and online forums for fear of criminal prosecution.[226]

Similar tactics were replicated in Uganda in May 2018, when the government passed an amendment to the Excise Duty Act, introducing a mandatory tax of UGX 200 (USD 0.05) per user per day for access to OTT services such as WhatsApp, Facebook and Twitter. In the same amendment, a 1% levy was imposed on all mobile money cash withdrawal transactions, an issue that caused public outcry and prompted parliament to reduce the levy to 0.5%. In a letter to the Finance Minister on March 2018, the President Museveni wrote that the taxes were necessary as the country needed resources to cope with the consequences of "olugambo on social media (opinions, prejudices, insults, friendly chats) and advertisements by Google."[227]

218   Digital Inclusion: Mobile Sector Taxation 2015
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/06/Digital-Inclusion-Mobile-Sector-Taxation-2015.pdf
219   Zimbabwe data prices hiked by up to 500% to curb social media activism and dissent
https://mg.co.za/article/2016-08-05-zimbabwe-data-price-hiked-up-by-up-to-500-to-curb-social-media-activism-and-dissent
220   Mobile operators suspend data bundles promotions https://www.newsday.co.zw/2016/08/mobile-operators-suspend-data-bundles-promotions/
221   Uproar over data tariff rise https://www.newsday.co.zw/2017/01/uproar-data-tariff-rise/
222   MISA Zimbabwe Position on Reduced Mobile Data Rates http://kubatana.net/2018/06/20/misa-zimbabwe-position-reduced-mobile-data-rates/
223   Hard-pressed Zim telecos hike data bundle tarrifs
http://www.itwebafrica.com/ict-and-governance/273-zimbabwe/246257-hard-pressed-zim-telcos-hike-data-bundle-tariffs
224   Zimbabwe: Data Tariffs Soar As Crisis Bites
https://allafrica.com/stories/201904280094.html
225   The law applies to bloggers, internet cafes, online content hosts, online forums, online radio or television, social media and subscribers and users of the internet
226   CIPESA (2019) Shrinking Civic Space in East Africa https://cipesa.org/?wpfb_dl=299
227   Museveni slaps taxes on social media users
https://www.monitor.co.ug/News/National/Museveni-taxes-social-media-users-Twitter-Skype/688334-4366608-oilivjz/index.html

Earlier in April 2018, the Ugandan communications regulator directed online data communication service providers, including online publishers, online news platforms and online radio and television operators to apply and obtain authorisation from the commission within a period of one month or risk having their websites and/or streams being blocked by Internet Service Providers (ISPs).[228] The regulator later published a list of the licenced providers, who were each required to pay USD 20. Later in 2019, the Ugandan regulator announced that "online publishers and influencers who have reached a capacity of sharing communication content and also using the online publication for commercial business had to register with UCC and pay a USD 20 levy.[229]

In DRC, the government through Ministerial Order No.011/CAB/M-CM/LOM/2018 of 14 June 2018 introduced guidelines requiring any seeking to operate an online media to register and seek permission from the Minister.[230]

In July 2018, Kenya's Finance Act 2018 increased the excise tax on telephone airtime from 10% to 15%, and introduced a 15% excise tax on internet data services and fixed line telephone services.[231] The increases, which were passed on to consumers,[233] were seen as regressive in nature and construed by consumers as government's intention to discourage the use of mobile phone services. Kenya first introduced a tax on mobile phone airtime in 2003 via an excise tax rate of 10% and 16% Value-Added Tax (VAT) on mobile handsets.

In December 2018, Cameroon announced a new Law No. 2018/022 on finance which introduced a new tax to be levied by telecommunications companies of 200 francs (about US D 0.35) for each software application downloaded from outside the country into phones, tablets and computers etc. This would add an additional cost to mobile apps, making access more expensive. The move caused anger on social media. This tax appears to treat downloaded applications as imports, and while it is yet to come into force, its implementation may be difficult.

In March 2016, the Nigerian government introduced the Communication Service Tax Bill which proposed to impose a 9% tax on communication services, such as SMS, data, and voice services. However, civil society groups and social media users carried out online protests against the bill and it was shelved. However, a proposal for a similar tax was made in August 2019 by the Federal Inland Revenue Service seeking to enforce a 5% Value Added Tax (VAT) for online purchases with a bank card, planned to be in place by early 2020.[234] The proposal has not been well received by e-commerce companies.

228   See The Registration Of Online Data Communication And Broadcast Service Providers notice at
http://www.ucc.co.ug/wp-content/uploads/2018/03/UCC_ONLINE-DATA-COMMUNICATIONS-SERVICES.pdf
229   Apollo Mubiru and Lucy Kiiza, UCC registers online publishers and influencers,
https://www.newvision.co.ug/new_vision/news/1504833/ucc-registers-online-publishers-influencers
230   Ministerial Order No. 011 / CAB / M-CM / LOM / 2018 of 14 June 2018 amending and supplementing Order No. 0 / MIP / 020/96 of 26 November 1996 implementing
Act No. 96-002 22 June 1996 laying down the procedures for the exercise of the freedom of the press available
athttps://www.droitcongolais.info/7b-subdivision-rs-735-753.html
231   Taxing mobile transactions https://www.brookings.edu/wp-content/uploads/2019/08/Taxing_mobile_transactions_20190806.pdf
232   Safaricom increases voice, SMS and data prices to reflect 15pc Excise Duty
https://www.capitalfm.co.ke/business/2018/10/safaricom-increases-voice-sms-and-data-prices-to-reflect-15pc-excise-duty/
233   Article 8, Portant Loi de Finances de la Republique du Cameroun pour l'Exercice 2019
https://www.legicam.cm/media/upload/2018051/.pdf
234   Nigeria wants to start charging a tax on local online purchases, https://qz.com/africa/1681466/nigeria-proposes-5-percent-online-vat-purchase-tax/

4.1.6 Deploying Bots, Cyberattacks and Disinformation

A common excuse for curtailing internet freedom is the need to fight what countries variously term misinformation, disinformation, hate speech, or fake news, among other terms.

In Kenya, the government sought to control discussions on social media through their propaganda machinery. In the run-up to the 2017 general election, it recruited key online influencers such as Robert Alai, who was a fierce critic of the government to support government narratives online. Further, it is said to have recruited 36 bloggers and social media bots to drive government propaganda and influence conversations online.[235] Further, the ruling Jubilee party had during the same period hired embattled firm, Cambridge Analytica, a 'psychological warfare firm', to support its campaigns during the August 2017 election.[236] The company is reported to have rebranded the Uhuru's party, written their manifesto, done two rounds of 50,000 surveys, carried out analysis and research, developed its messaging including writing all the speeches, and staged every element of the campaign,

The use of propaganda was also noted in Zimbabwe. In August 2016 the state-owned Herald newspaper published a headline story with the title, "Social media terrorists exposed".[237] The 'social media terrorists' were three Zimbabweans exposed in the government's 'cyber-terrorism probe' whose preliminary findings unearthed 'subversive and inflammatory' messages allegedly originated by trio. The article was seen as a message communicating the possible start of a more targeted clampdown on social media users and to justify the stringent social media regulation through the Computer Crime and Cybercrime Bill.

In July 2018, there emerged several new social media accounts on Facebook and Twitter to advance the Zimbabwean government and ruling party ZANU-PF propaganda,[238] manipulate conversations, target and harass online activists and disrupt political conversations by the opposition. The influencers self-identifying as 'Team Varakashi'[239] are state propaganda machinery, who led a spirited dis-information campaign targeting both domestic and foreign audiences by amplifying and magnifying government talking points through hundreds of accounts.

---

[235]   Uhuru regime hires 36 bloggers as online war with opposition rages,
https://www.kenya-today.com/news/government-hires-36-bloggers-as-online-war-with-opposition-rages
[236] Revealed: Cambridge Analytica's agent in Uhuru's 2017 campaign,
https://www.the-star.co.ke/news/2019-07-17-revealed-cambridge-analyticas-agent-in-uhurus-2017-campaign/
[237] Social Media Terrorists Exposed, http://www.herald.co.zw/social-media-terrorists-exposed
[238] Video https://twitter.com/Wamagaisa/status/984637362020978689
[239] Loosely translated, 'rakasha' is a word in Shona language that means to attack and vanquish one's enemies.

4.2 Key Positive Developments

Despite the negative trends witnessed in the countries reviewed, there were notable developments that were indeed positive and that support the enjoyment of internet freedom. The three major developments included the robust advocacy and push-back by non-state actors, the adoption of progressive legislation and lastly, the repeal of repressive legislation.

4.2.1 Robust Advocacy and Push-back by Non-State Actors

Sustained civic action appears to be a formidable driver to help counter the internet control measures introduced by governments. Civil society continues to play a key role in resisting unconstitutional laws and practices by governments. In 2011, civil society in Malawi organised their first civic and political protest on Facebook against bad governance and poor service delivery in the country.[240] The organising took place online and on social media was used to mobilise protesters.[241]

In 2004, the Constitutional Court of Uganda in a landmark decision, declared null and void section 50 of the Penal Code which made the publication of false news a criminal offence.[242] In Kenya, constitutional challenges at the High Court spearheaded by civil society have over the past five years led to successes in repealing or suspension of unconstitutional legislation. In September 2015, the Tanzania Human Rights Defenders Coalition (THRDC), Legal and Human Rights Center (LHRC) and other groups challenged the constitutionality of the Cybercrime Act in the High Court.[243] In December 2016, the High Court overturned only Section 50 of the law while declaring the sections 19 of the 20 sections of the law constitutional, which decision, the organisations vowed to appeal.[244] In January 2019, the Zimbabwe chapter of the Media Institute of Southern Africa (MISA) successfully challenged internet shutdown in Zimbabwe, which the High Court ruled as illegal.[245]

In September 2019, the amaBhungane Centre for Investigative Journalism and journalist Stephen Patrick Sole sued the state at the High Court of South Africa in Pretoria, having learned that the journalist's phone had been spied on by law enforcement agents for at least six months in 2008. In a unanimous ruling, the Court declared that bulk surveillance activities and foreign signals interception by the South African National Communications Centre is unlawful and invalid.[246] The court also refuted pleas by the South African intelligence authorities that other states have similar practices.

In the DRC, the Congolese Association for Access to Justice (ACAJ) expressed concern on the mandatory SIM card registration implemented in December 2015, citing the potential misuse of this information by security services.[247] Further, several online media and journalists' organisations denounced the December 2016 shutdown of the internet and social media restrictions by the DRC government. They noted the restrictions would stifle online media and restrict freedom of expression as the country approached an election.[248] Advocacy efforts by civil society in Nigeria led to the development of the Digital Rights and Freedom Bill 2016, which despite obtaining Senate approval was returned to Senate following President Buhari's decision not to assent it to law.

---

240   Malawi Army Deployed Over Anti-Mutharika Protests,; https://bbc.in/2Gq1AY6

241 Malawi: Arab Spring Spreading South of the Sahara? https://bit.ly/2Y0frz5

242 Joseph Mulenga JSC in Charles Onyango Obbo and Andrew Mwenda vs. Attorney General S.C.C.A No. 2 of 2002 [2004]; Mulenga set the standard on protection of free speech https://www.monitor.co.ug/Magazines/PeoplePower/Mulenga-set-the-standard-on-protection-of-free-speech/689844-1492504-o6gw6lz/index.html

243 Parts of Cybercrime Act opposed in court, https://www.thecitizen.co.tz/news/Parts-of-Cybercrime-Act-opposed-in-court/1840340-2867400-fds9pbz/index.html

244 Activists to challenge ruling on cybercrime law, https://www.thecitizen.co.tz/news/Activists-to-challenge-ruling-on-cybercrime-law/1840340-3505144-n1il6mz/index.html

245 Zimbabwe High Court court rules internet shutdown illegal, https://www.iol.co.za/news/africa/zimbabwe-high-court-court-rules-internet-shutdown-illegal-18898174

246 Privacy International, "Bulk surveillance is unlawful, says the High Court of South Africa," September 16, 2019, available at https://privacyinternational.org/news-analysis/3212/bulk-surveillance-unlawful-says-high-court-south-africa

247 RDC: les sociétés cellulaires bloquent les numéros de téléphones non identifiés, https://www.radiookapi.net/2015/12/30/actualite/societe/rdc-les-societes-cellulaires-bloquent-les-numeros-de-telephones-non

248 La presse en ligne sous surveillance en RDC, https://www.bbc.com/afrique/region-44860197

In the wake of the national ID registration process in Malawi, civil society inOctober 2018 called upon the government to ratify the Malabo Convention on Cybersecurity and Data Protection so as to strengthen privacy and data protection in the country.[249] Meanwhile, Nigerian civil society including organisations such as Paradigm Initiative and Media Rights Agenda have filed cases and advocated against the draconian and restrictive legislation adopted by the government, such as the Cybercrime law. They have also formed coalitions, such as the Freedom of Information coalition, and organised trainings on digital rights including with law enforcement officials on the Cybercrime Act 2015.[250]

In Senegal, more than 300 civil society organisations conducted advocacy and awareness campaigns against the controversial Article 27 of Law no. 2018-28 of 12 December 2018 on the Electronic Communications Code. Despite their best efforts to oppose the proposed law before it was adopted, the state passed it.[251] The Minister for Communication, Abdoulaye Balde Bibi, argued that the law posed no threat to freedom of expression, as the problem was interpretation. Similarly, in Cameroon, the coordinated responses by different activists through online advocacy, including through the hashtag #BringBackOurInternet, helped to bring international attention to the internet shutdown in the country. The activists managed to rally the international community to the issue,building pressure that resulted in the restoration of internet connectivity in April 2017.

Some opposition leaders have also played key roles in promoting internet freedom in their countries. For instance, leaders of opposition parties in Burundi opposed the introduction of biometric ID cards prior to general elections, arguing that they would lead to rigging.[252] Further, political actors together with the Burundian Press Union successfully challenged a Press law before the constitutional court of Burundi and East African Court of Justice in January 2014, leading to the adoption of a new law in May 2015.[253] In Botswana, opposition leaders resigned from the parliamentary oversight committee on intelligence services, citing its lack of independence. They have also continued to call for greater accountability and reforms of the intelligence agency, DISS.

In October 2018, the World Bank blocked a USD $50 million fund meant for Tanzania, saying it was deeply concerned about restrictions that the government had placed on freedom of speech concerning publication of statistics.[254] This later led to amendments to the Statistics Act, 2018 to address the controversial provision.

249   A Call for Personal Data Protection Legislation in Malawi, a press statement by CHRR, 3rd October 2018
250 Nigeria: Trends in Freedom of Expression in the Telecommunications and the Internet Sect,
https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/ParadigmInitiativeNigeria.pdf
251 Telecommunication Code: Civil society vetoes, https://www.leral.net/Code-des-telecommunications-la-societe-civile-pose-son-veto_a238003.html.
252 La carte d'identité biométrique viole-t-elle notre vie privée? https://www.iwacu-burundi.org/inquietudes-suscitees-par-nouvelle-carte-identite-biometrique/
253 State of Internet Freedom in Burundi | 2016 https://cipesa.org/?wpfb_dl=230
254 World Bank blocks Sh110bn over Statistics Act https://www.thecitizen.co.tz/news/World-Bank-blocks-Sh110bn-over-Statistics-Act/1840340-4789448-1sv815/index.html

4.2.2 Adoption of Progressive Legislation

A number of countries under review have taken measures to develop and implement some progressive legislation. The DRC, Kenya, Tanzania, Burundi and Zimbabwe have adopted new constitutions since the year 2000, which have provided greater protection for human rights.

At the statute level, Burundi passed Press Law N° 1/025 of 27 November 2003, which was hailed as progressive.[255] Senegal passed the Law on the Protection of Personal Data in May 2008 establishing the Commission for the Protection of Personal Data (CDP) as an Independent Administrative Authority (AAI) to ensure oversight of personal data processing.[256] Ethiopia passed the Communication Regulatory Proclamation in June 2019 to facilitate the liberalisation of the telecom sector in the country, establish a sector regulator, allow the licensing of new operators, and end the state-owned Ethio Telecom's monopoly.[257] Nigeria adopted its Freedom of Information Act in 2011,[258] Malawi adopted its Access to Information Act in 2017,[259] while Kenya adopted the Access to Information Act, in 2016. However, the same are yet to be fully implemented and the Official Secrets Act remains in force in countries with access to information laws, such as Nigeria, Uganda and Kenya.

4.2.3 Repeal of Repressive Legislation

A number of countries under review such as Burundi, Ethiopia, Zimbabwe, Uganda and Tanzania have taken measures to repeal repressive legislation. Where they have not, courts have been at the forefront to ensure their repeal. In 2004, the Constitutional Court of Uganda declared null and void section 50 of the Penal Code which made the publication of false news a criminal offence.[260] The court held that, "extending protection of the freedom of expression to false statements does not necessarily defeat the objective of upholding the truth, because while truth and falsity are mutually exclusive, the purposes for protecting both are not."[261]

Similarly, in 2010, the Constitutional Court of Uganda declared sections 39 and 40 of the Penal Code which relate to sedition null and void. The petitioner had been charged for remarks made on a popular radio talk show alleging that Uganda was partly responsible for South Sudan president John Garang's death. The prosecution had stated that the remarks were intended to bring hate and contempt against the president, government, and constitution. The court stated that, "[sedition] is so wide and it catches everybody to the extent that it incriminates a person in the enjoyment of one's right of expression of thought. Our people express their thoughts differently depending on the environment of their birth, upbringing and education."[262]

In 2015, following a successful court case, Press Law No 1/15 of 9 May 2015[263] of Burundi was passed, amending the law of June 2013. It removed heavy fines against journalists, and allowed journalists to challenge the decisions of the CNC (National Commission in charge of Communication).

255   Dispositions Fondamentales, ES http://www.asclibrary.nl/docs/397737815-02.pdf
256   Law No. 2008-12 of 25 January 2008, on the protection of personal data (JORS, no. 6406, of 3 May 2008, p.434).
257   Text of proclamation, https://addisstandard.com/wp-content/uploads/2019/02/Draft-Communication-Serv-Proclamation-.pdf
258   The Freedom of Information Act 2011 (FOI) - What It Means For
Youhttps://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=article&id=165:the-freedom-of-information-act-2011-foi-what-it-means-for-you&catid=23&Itemid=179
259   Access to Information Act, 2017, February 2017; http://bit.ly/2HtgH3q
260   Charles Onyango Obbo and Andrew Mwenda vs. Attorney General (2004)
261   Joseph Mulenga JSC in Charles Onyango Obbo and Andrew Mwenda vs. Attorney General S.C.C.A No. 2 of 2002 [2004]
262   Charles Onyango Obbo and Andrew Mwenda vs. Attorney General, C.P. no. 12 of 2005 [2010]
263   State of internet Freedom in Burundi 2016 https://cipesa.org/?wpfb_dl=230

In February 2019, the Zimbabwean cabinet approved the repeal of the draconian Access to Information and Protection of Privacy Act (AIPPA),[264] to give way for the enactment of an Access to Information Bill, the Zimbabwe Media Commission Bill and the Protection of Personal Information and Data Protection Bill. In July 2019, the Zimbabwean government gazetted the Freedom of Information Bill which repeals sections of AIPPA.[265]

In June 2019, following complaints by stakeholders, Tanzania repealed a provision in the Statistics Act, 2018, which made it an offence to collect and publish statistics which contradicted those of the National Bureau of Statistics (NBS).[266] The offence was punishable by a USD 6,000 fine or a three-year prison sentence. In 2019, the Ethiopian government set-up a legal reform committee to oversee the reform of repressive laws in the country. The Charities and Registration Proclamation has already been amended. Others awaiting reform include the Anti-Terrorism Proclamation, the Freedom of the Mass Media and Access to Information Bill, and the Computer Crime Proclamation.

264 Zimbabwe: Cabinet Approves AIPPA Repeal https://allafrica.com/stories/201902130504.html
265 AIPPA repealed in new era for media https://www.herald.co.zw/aippa-repealed-in-new-era-for-media/
266 It is no longer a crime to publish statistics in Tanzania
https://www.thecitizen.co.tz/news/It-is-no-longer-a-crime-to-publish-statistics-in-Tanzania-/1840340-5174870-wjjdxhz/index.html

5 Conclusion and Recommendations

The study has found that African countries have broadened the range of measures that govern the use of digital communications including the internet. The implementation of oppressive laws and regulations is on the rise in the countries under review. It is evident that countries are using legislation to legitimise practices which are otherwise unlawful to impose restrictions and internet controls. While laws in place are touted as necessary towards fighting cybercrime or enhancing cybersecurity in the countries, they are largely directed towards stemming opposition, clamping down on criticism and quelling local dissent.

Increasingly, the countries reviewed appear to adopt a similar pattern of measures across the board, which have been increasing gradually since 1999, as the use of the internet continues to rise. The key reasons given by governments are the need to safeguard national security and maintain public order.

These controls collectively continue to undermine democracy and cement authoritarians hold on political power. Political censorship continues to be used by to block perceived offensive content in order to maintain the status quo and remain in power. Such measures have been more rampant during election periods and they include propagating set narratives, limiting the spread of information by their competitors, and blocking information that does not favour their positions. It appears that leaders continue to enact legislation and implement measures to safeguard their selfish political interests, sometimes clothed as legitimate public interests.

Moreover, impunity continues to reign supreme given the general failure to respect the rule of law, and the blatant disregard of constitutional and human rights standards. When the laws have been restrictive, or have not worked in favour of regimes in power, the solution has been to amend the laws to serve their interests. The legitimisation of surveillance and interception of communication through legislation is worrying.

Each successive period since 1999 came with some notable developments in internet controls. By 2000, there was little activity in the way of legislation, policy-making, or infringements of online freedoms. This can partly be attributed to the low spread of ICT at the time, during which the average internet penetration in Africa was 2%. In the countries under study, as of 2005 the internet penetration rate in Senegal, Rwanda, Malawi, Ethiopia, DRC, and Burundi, was less than 1%, and at 6.7%, only Zimbabwe had penetration rate higher than 5%.

Nonetheless, as of **2005**, a few regional countries were beginning to realise the need to intercept communications, including digital communications. The low digital activity at the time also implied that, between 1999 and 2005, there were hardly any cases of arrests or prosecutions of individuals over the use of ICT, and even blocking of websites was uncommon. Ethiopia was probably the first sub-Saharan African country to begin blocking internet sites, with the first reports of blocked websites appearing in May 2006 when opposition blogs were unavailable.[267] During this period, laws governing media and journalism were the main way to control freedom of expression, including of voices that questioned government actions.

---

[267] Human Rights Watch, "They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia, https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia

Between **2006 and 2010**, a number of governments started to take dedicated moves to regulate the digital sphere, including proscribing various actions related to the use of ICT. There was a flurry of legislation to enable the interception of communications, or to criminalise the use of certain services (as was the case with ethiopia's Anti-Terrorism Proclamation- No 652/2009, under which it is estimated that over 900 individuals were indicted over their online activity).[268] Some countries, such as Kenya, moved to regulate the transmission of SMS, particularly bulk SMS, and the propagation of online hate speech, at election time. This period also witnessed numerous cases of blockage of critical websites in countries such as Burundi and Uganda. Distinctly, this period saw the start of systematic disruption of communications and other internet freedom infringements during election periods, although the target was critical websites (such as in Ethiopia and Uganda) and short messaging services, for instance in Ethiopia and Kenya). In 2007, DRC and Senegal introduced mandatory SIM card registration, and within a few years the practice had spread all over the region.

The **2011-2015** period saw an increase in the measures which governments used to control internet activity, and could be said to be when most governments instituted dedicated efforts to regulate and to control citizens' online actions. Many more citizens were arrested and prosecuted over alleged offences and crimes committed through online mediums. More governments ordered disruptions to communications. More laws were enacted to govern digital communications. And there were dedicated efforts to grow governments' surveillance capacity.

Cybercrime laws enacted in this period (for example in Nigeria, Tanzania, and Uganda) became the main pieces of legislation used to undermine internet freedom through arrests and prosecution of ICT users. In Nigeria, Section 24 of the 2015 Cyber Crime law penalises "cyberstalking" and transmission of "false" messages that are intended to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another. This provision has been used to arrest several bloggers and online journalists. In the same period, specifically in 2012, Ethiopia enacted the Telecom Fraud Offences Proclamation, which became one of the pieces of legislation used to quash internet freedom.

The **2016-2019** period was the "golden era" of network disruptions (commonly known as internet shutdowns). During this period, nearly half the countries in Africa (at least 22 of them) experienced a government-ordered network disruption, with popular social media sites such as Facebook and Twitter being the main target.[269] Some countries also ordered blockage of SMS, or of the entire internet, and in Uganda's case, mobile money services. Within the first three weeks of 2019, network disruptions had been registered in five countries (Chad, Democratic Republic of Congo, Gabon, Sudan and Zimbabwe).

In conclusion, the overall effect is that internet freedom has been on the decline since 2000.

[268] Zelalem Kibret, The Terrorism of 'Counterterrorism': The Use and Abuse of Anti-errirism Law, The Case of |Ethiopia, http://eujournal.org/index.php/esj/article/view/9348

[269] CIPESA, Despots and Disruptions: Five Dimensions of Internet Shutdowns in Africa, https://cipesa.org/?wpfb_dl=283

6.2 Recommendations

The study makes the following recommendations targeting government, companies, civil society, media, technical community, and the academia.

Government
- Respect human rights and freedoms as enshrined in their constitutions and in international instruments that they have ratified.
- Stop the use of internet control policies, measures and practices.
- Adopt and promote the multistakeholder approach to ensure transparent, inclusive and open stakeholder engagement in the development of internet related policies and legislation.
- Define clearly in policies and laws the acceptable measures, terms, and circumstances in which internet controls may be applied, in line with constitutional and international human rights standards, and ensure there is transparency, accountability and judicial oversight.
- Ensure there are sufficient safeguards and principles including 'privacy by design' in laws and policies for the robust protection of the right to privacy and personal data.

Companies
- Adopt and implement the UN Business and Human Rights principles and safeguard the rights of customers by default.
- Require that government requests for internet controls comply with the rule of law and due process.
- Adopt terms and conditions of privacy and data usage must be clear, open and agreements must be honoured.
- Develop clear due diligence mechanisms to respond to information requests or other internet controls.
- Adopt the use of technologies that make it difficult to carry out surveillance, interception of traffic and internet shutdown.

Media
- Collaborate with other stakeholders in the promotion of internet and press freedom.
- Challenge laws that limit self-censorship and press freedom.
- Promote digital safety and the protection of journalists.
- Report, cover and highlight incidents relating to threats to internet freedom.
- Inform, educate and mobilise the public to practise and realise their rights and internet freedom.
- Build their capacity and knowledge on internet freedom issues.

Academia
- Conduct evidence-based policy and legal research.
- Disseminate research findings and recommendations to promote internet freedom.
- Include internet freedom in their curriculum to ensure students are made aware of the issues.
- Collaborate with other stakeholders in the promotion of internet freedom.

Technical Community
- Design technologies that are rights respecting.
- Educate stakeholders on the impact of new technologies on internet freedom.
- Develop and promote local platforms to promote public engagement and internet freedom.
- Develop and promote innovative technologies to circumvent internet control restrictions and surveillance.
- Create awareness and digital safety training for the public e.g. on the use of virtual private networks (VPNs), encryption, anonymous browsing, malware and spam etc.
- Collaborate with other stakeholders in the promotion of internet freedom.

Civil Society

- Collaborate to promote internet freedom through active monitoring, advocacy, research and public interest litigation.
- Create awareness, build capacity and sensitize the public and key stakeholders through innovative initiatives to create greater understanding of internet freedom issues and on best practices.
- Mainstream human rights organizations should incorporate internet freedom in their programming, and collaborate better with specialised organizations working on internet freedom.
- Monitor and expose government collaboration, including projects, developments, procurement and trainings with foreign governments e.g. China, US and Russia that could potentially violate human rights and threaten internet freedom.
- Advocate against government adoption of foreign-inspired censorship, data collection and surveillance methods and technologies.
- Advocate and remind states of their obligations under international human rights instruments.
- Build stronger multistakeholder coalitions locally, regionally, and globally to push-back against internet controls and promote internet freedom.