Digital Rights in Africa:
Challenges and Policy Options

March 2019

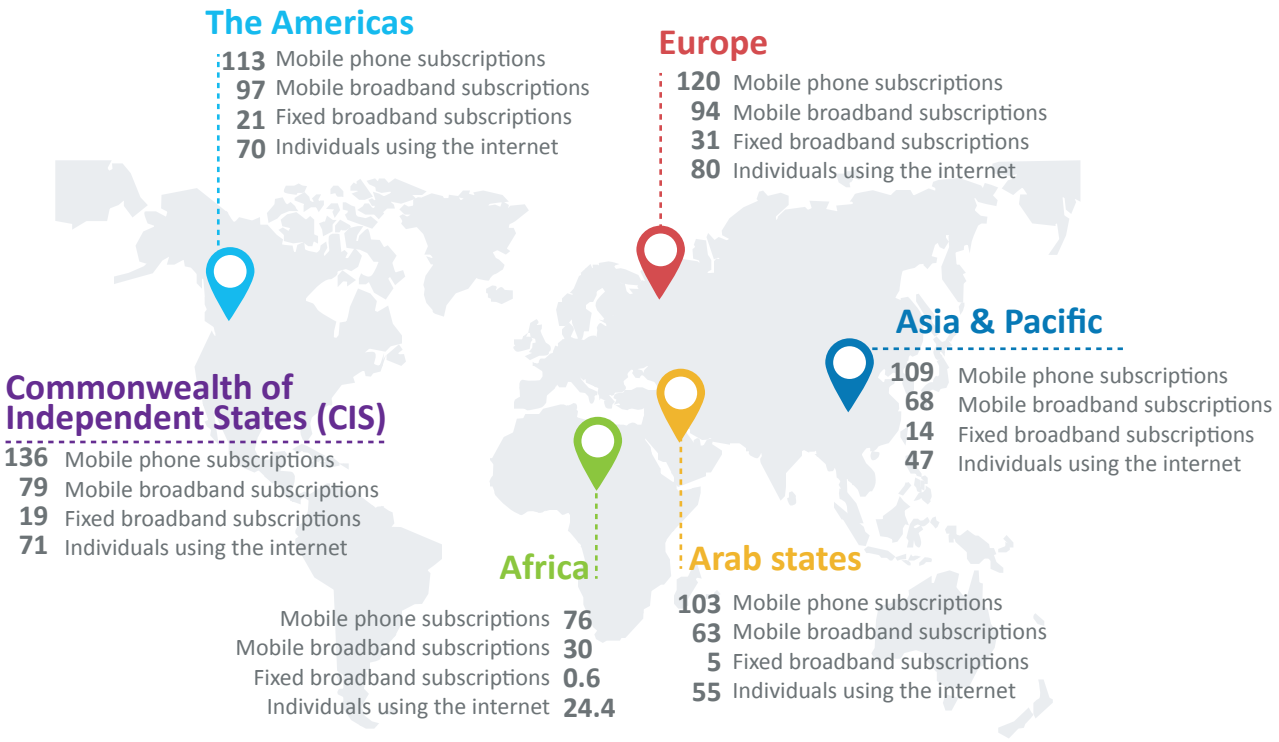
CIPESA

#InternetFreedomAfrica

Introduction

A growing number of citizens in Africa are using Information and Communications Technology (ICT) on a regular basis, which has made digital technologies pivotal to the enjoyment of their rights and improvement of their livelihoods. However, many governments are taking steps that undermine internet access and affordability, and weaken the potential of digital technologies to catalyse free expression and civic participation or to drive innovation.[1] There has been an increase in digital rights violations such as arrests and intimidation of online users, internet blockages, and a proliferation of laws and regulations that undermine the potential of technology to drive socio-economic and political development on the continent.

Africa has the lowest ICT usage figures compared to other regions and also experiences a deep digital divide (See comparative usage numbers in table below). The moves seen in some countries which hamper access and affordability, and which unduly restrict citizens' rights to free speech, privacy and access to information, therefore undermine efforts to bridge the digital divide. Moreover, they forestall the meaningful uptake of ICT and thus undercut the potential of ICT to improve governance and promote development.



Comparative ICT figures (subscriptions/ usage per 100 inhabitants) | Source: ITU[2]

1 *CIPESA, State of Internet Freedom in Africa 2018, https://cipesa.org/?wpfb_dl=278*

2 *ITU, World Telecommunication/ICT Indicators database, Nov 2018, https://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx*

More than a dozen African countries have recently experienced internet or social media shutdowns, with some countries suffering disruptions to communications on more than one occasion. There is also increasing data collection and misuse amidst a shortage of privacy and data protection laws. This is worrying, as it comes while many governments are raising surveillance capacity even when there are insufficient independent safeguards to guide interception of communications or user information requests.

This issue paper presents four key illustrative issues on challenges to digital rights on the continent, and suggests some actions that should be undertaken to address them.

Regressive online content regulation and taxation

In purported efforts to fight hate speech, misinformation (fake news), among others, it has become common practice across the region to pass legislation that is stringent and restricts online content. Tanzania, Uganda, DR Congo, Burundi and Zambia are among the countries in Africa which in 2018 proposed or passed laws and regulations that undermine public confidence in the use of online platforms and could lead to increased self-censorship by media, civil society groups and individual citizens, as well as to their withdrawal from online discourse.

In March 2018, the Uganda Communications Commission (UCC) issued a notice to all online data communication service providers, including online publishers, online news platforms and online radio and television operators advising them 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).[3]

In the same month, the Tanzania Communications Regulatory Authority (TCRA) introduced a new regulation which requires online content creators[4] to pay application fees of US$ 43.7, initial three year license fees of US$ 437 and renewal fees of a similar amount. The penalty for non-compliance is a fine of US$ 2,186. The licensing requirements under the Electronic and Postal Communications (Online Content) Regulations are vague, the fees prohibitive, and the fines for non-compliance equally stiff.[5] As of November 2018, the TCRA had issued 224 licences under these regulations.[6] However, many independent bloggers, who can not afford the licence fees and other stringent licencing requirements have ceased operations altogether. Under the regulations, content providers must "have in place mechanisms to identify source of content" and are required to swiftly terminate or suspend subscriber accounts and remove content if found in contravention of the regulations, if directed by TCRA or by an affected person.

In the same vein, the DR Congo also issued regulations in 2018 that require online content producers to register, although these have to-date not been implemented – unlike in Tanzania and Uganda.

3 The Registration Of Online Data Communication And Broadcast Service Providers notice is available at http://www.ucc.co.ug/wp-content/uploads/2018/03/UCC_ONLINE-DATA-COMMUNICATIONS-SERVICES.pdf

4 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.

5 The Electronic and Postal Communications (Online Content) Regulations are available at https://www.tcra.go.tz/images/documents/regulations/SUPP_GN_NO_133_16_03_2018_EPOCA_ONLINE_CONTENT_REGULATIONS_2018.pdf; See also Ashnah Kalemera, "Tanzania Issues Regressive Online Content Regulations," CIPESA, April 12, 2018, available at https://cipesa.org/2018/04/tanzania-enacts-regressive-online-content-regulations/

6 Licensed online content services providers by 12th November, 2018, https://www.tcra.go.tz/index.php/licensed-online-content-services-providers-by-31st-july-2018

In Kenya, a cybercrimes law was enacted in May 2018, which human rights defenders say contravenes rights to freedom of expression, privacy, association. The Act introduced offences such as publication of false information, cyber harassment, unauthorised interference and unauthorised interception, which "are phrased so vaguely that it is impossible to tell the conduct targeted by these sections." After civic groups filed a suit, the High Court suspended the implementation of several clauses in the new law.[7] The case remains in court. Kenya already has a history of stifling online critics[8] of both state and non-state actors, as echoed by James Wamathai, the Director of Partnerships at the Bloggers Association of Kenya (BAKE). In a statement, Wamathai said: "In the past several years, there have been attempts by the government to clamp down on the freedom of expression online. This Act is a testament of these efforts, especially after other sections were declared unconstitutional by the courts.[9]

BAKE also said in court papers that in 2016, 60 Kenyan bloggers were arrested for exercising their freedom of expression online. In mid-2018, Kenya also raised data prices, and hinted at slapping licence fees on online video creators.

On May 30, 2018 Uganda's parliament passed a widely opposed amendment to the Excise Duty Act, introducing an excise tax of Uganda Shillings (UGX) 200, equivalent to USD 0.05 per user per day for use of Over the Top (OTT) services such as WhatsApp, Facebook and Twitter. The law became effective on July 1, 2018. The tax rendered the internet less affordable for Ugandans, particularly low income earners. Indeed, three months after the tax was introduced, the number of internet users in the country had declined by five million, thereby cutting the internet penetration rate from 47% to 35%.[10] By the same law, a 0.5% levy was imposed on all mobile money cash withdrawal transactions, an issue that has equally caused public outcry[11] and undermined financial inclusion for the poorest. Research by the communications regulator shows that majority of Persons with Disabilities (66%) reduced their use of social media use with the introduction of the OTT tax, while 26% were no longer using social media.[12]

Meanwhile, Zambia's cabinet in August 2018 endorsed the introduction of a daily tax equivalent to USD0.03 on Voice Over Internet Protocol (VoIP) calls, although this is yet to be implemented. Also in August 2018, Benin had introduced a similar levy but backtracked after a backlash from citizens.[13]

8 Maureen Kakah, "High Court suspends portions of cybercrime law," Daily Nation, May 29, 2018, available at https://www.nation.co.ke/news/Court-suspends-portions-of-cybercrime-law/1056-4585936-thh4s5/index.html

9 New Year, Old Habits: Threats to Freedom of Expression Online in Kenya, https://cipesa.org/2016/01/new-year-old-habits-threats-to-freedom-of-expression-online-in-kenya/ https://www.blog.bake.co.ke/wp-content/uploads/2018/05/BAKE-petition-Cybercrimes-act.pdf

10 Social Media Tax Cuts Ugandan Internet Users by Five Million, Penetration Down From 47% to 35%, https://cipesa.org/2019/01/%EF%BB%BFsocial-media-tax-cuts-ugandan-internet-users-by-five-million-penetration-down-from-47-to-35/

11 Ibid.

12 UCC, Access and usage of Information and Communications Technologies (ICTs) by People with Disabilities (PWDs) in Uganda, https://www.ucc.co.ug/wp-content/uploads/2017/09/Final-Report-on-Access-and-Usage-of-ICTs-by-PWDs_Public-Dissemination.pdf

13 https://internetwithoutborders.org/benin-government-repeals-social-media-tax/

Network Disruptions

In the last four years, more than 20 African countries have ordered disruptions to the internet, with popular social media platforms such as Facebook, WhatsApp, Twitter among the services targeted. Disruptions to Short Messaging Services (SMS) have also been commonplace, while some countries have ordered a slowdown of the overall internet. Internet disruptions are mostly ordered by governments eager to curtail citizens' access to information in order to limit what the citizens can see, do, or communicate. In ordering such shutdowns, governments often cite digital technologies' increasing usage to spread disinformation, propagate hate speech, and fan public disorder and undermine national security.

As of January 2019, internet disruptions were being experienced in five African countries - Chad, Democratic Republic of Congo (DR Congo), Gabon, Sudan and Zimbabwe. The disruptions were related to elections, protests against government policies, and, what seemed like a coup attempt. In Gabon the 28-hour total internet shutdown was ordered by the government when some soldiers announced on national radio that they were spearheading a coup.[14] In DR Congo, social media access was disrupted on December 31, 2018, as citizens were electing a replacement for a president who had been in power for 17 years. The disruptions in Sudan and Zimbabwe were ordered as citizens demonstrated against unpopular government policies.

In June 2016, the United Nations Human Rights Council passed a resolution castigating internet shutdowns. It condemned "unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and called on all States to refrain from and cease such measures."[15] Increasingly, it is also recognised that network disruptions are not a necessary and proportionate measure, as they affect users' fundamental human rights, such as the right of access to information and freedom of expression and association. Moreover, they have perverse negative social and economic costs. As noted by the Global Network Initiative (GNI), whereas governments have a legitimate role to protect public safety, disruptions can have an adverse effect on that very objective, preventing citizens' access to vital emergency, payment and health services, suspending business operations, and cutting off people's contact to family and friends.[16]

Further, the economic impact of a network disruption persists far beyond the days on which access is blocked due to systemic effects that harm efficiency throughout the economy. Internet shutdowns, however short-lived, undermine economic growth, and erode business confidence.[17] Indeed, a study found that the internet and social media shutdowns that were ordered in 10 Sub-Saharan African countries between 2015 and 2017 cost an estimated US$ 237 million. Thus, as noted by the #KeepItOn campaign, internet shutdowns pose a threat to human rights around the world, as "they harm everyone: businesses, emergency services, journalism, human rights defenders, and demonstrators" and "they don't help victims or restore order."[18]

14 BBC, Gabon coup attempt: Government says situation under control, January 7, 2019, https://www.bbc.com/news/world-africa-46779854

15 Human Rights Council Thirty-second session, https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

16 GNI, The Consequences of Network Shutdowns and Service Disruptions: A One-page Guide for Policymakers, https://globalnetworkinitiative.org/the-consequences-of-network-shutdowns-and-service-disruptions-a-one-page-guide-for-policymakers /

17 CIPESA, Calculating the economic impact of internet disruptions in Sub-Saharan Africa, https://cipesa.org/?wpfb_dl=252

18 #KeepItOn campaign, https://www.accessnow.org/keepiton/

Surveillance and Data Privacy

Privacy is fundamental to the enjoyment of freedom of association and of assembly. However, there is a challenge of upholding the right to privacy and protection of personal data. Up to 23 African countries have data protection frameworks. Yet in many countries on the continent, both law and practice fall short of complying with international best practices. Nonetheless, this has not stopped many states from embarking upon mass personal data collection drives and, increasingly, the nature of personal data being collected is expanding, to include biometric data, for instance.

Majority of African countries have mandatory SIM card registration where subscribers are required to furnish telecom companies with extensive personal details, including names, home addresses and their National Identification Numbers (NINs). Moreover, several government bodies collect information (as do private sector entities) with no safeguards for the safekeeping of such information. Without a comprehensive data protection law (and an accompanying practice by government agencies and the private sector which robustly protects such data), users' personal data is at a big risk of abuse by state and non-state actors. The misuse of personal data by security and intelligence agencies amidst inadequate judicial and parliamentary oversight over surveillance activity is one such example. Of note is that in many countries, telecoms and ISPs are required by law to comply with information requests or requests for surveillance assistance, including the common requirement to install software with technical capacity to conduct surveillance and to enable active communications monitoring. In some countries still, various government officials and offices can demand for users' data from telecom operators, which also creates latitude for violating user's privacy.

Proposed Remedial Actions

From the foregoing discussion, it is evident that the state of internet freedom in Africa is worrying, and could yet get worse. Below, we suggest some actions by state and non-state actors to address some of the more pressing challenges in the region.

Greater role for private sector actors

Private sector actors, particularly in the ICT industry,

1. Should make their content moderation policies better known to the public and implement them judiciously. If private actors have fair and widely known policies and implement them fairly, it might reduce the need for governments to promulgate regressive laws and regulations to address what they see as ills of use of ICT.
2. Should support initiatives that promote digital rights, speak out about any licencing obligations and government practices that undermine privacy and freedom of expression, protect users' data, and align with initiatives that grow access, affordability, and innovative use of digital technology.
3. Issue periodic transparency reports on government shutdown orders, demands for users' data, and requests for interception of communications support. Presently, the largest telecom operators in Africa, such as MTN and Airtel, do not issue transparency reports with any such information. Moreover, where such reports are issued – primarily by multinationals that have operations in Africa, such as Orange, Millicom and Vodafone – they are often heavily redacted, making it difficult to see how they are protecting the privacy of their users and promoting freedom of expression.[19]

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

Litigation for digital rights

Promoters of internet freedom should actively challenge laws and practices that stifle digital rights through courts of law. Indeed, there has been litigation against shutdowns in such countries as Cameroon, Chad, Gambia, Togo, Uganda, and Zimbabwe. A recent highlight of this was the January, 21, 2019 court ruling that declared the Zimbabwe shutdown illegal. This was after the judge determined that the minister of state for national security lacked the authority to issue any directives under the Interception of Communications Act, under which he had ordered the shutdown. The litigation should target specific laws or regulations as well as practices, such as arrests and prosecution of ICT users. To gain more mileage, the litigation should draw in multiple actors - both local and international - as a measure to strengthen advocacy and awareness-raising of various digital rights issues. Besides national courts, repressive laws and practices should also be challenged in regional courts and the African Court on Human and People's Rights.

Ramp up advocacy work

It is crucial to grow awareness about digital rights and the importance of observing them. This awareness is needed among both non-state actors (citizens, media, private sector, civil society groups) and state agencies (law enforcement, the judiciary, legislature, and communications regulators).

Multi-stakeholder and cross-country advocacy campaigns should be encouraged. There have been instructive examples, such as the #KeepItOn coalition against internet shutdowns; #NoToSocialMediaTax in Uganda that opposed imposition of OTT taxes; #BringBackOurInternet which advocated for an end to a long-running network disruption in Cameroon, and #InternetFreedomAfrica that raises awareness on internet freedom issues in Africa. In Benin, where the government had introduced a tax on social media, the offline and online #TaxePasMesMo advocacy campaign prompted the country's leaders to suspend its implementation. Key to note is that these advocacy efforts need to be informed by robust and independent digital rights research, which explains the problem at hand and succinctly suggests practical solutions.

Digital safety and digital literacy

Whereas safety tools can be crucial in securing communications, enhancing mobilisation, and effectuating support systems, there is often a low level of digital safety skills among the at-risk users. With increasing digital connectivity among the at-risk users comes new threats, unless they embrace diligent digital safety practices and adhere to them. Poor digital security skills, including on social media, have often resulted in blackmail and extortion of critical internet users, and in cyber harassment, and sometimes physical attacks.

There is therefore need for digital security training and digital literacy campaigns, and for increased use of tools of anonymisation and circumvention. Moreover, civil society actors need to cooperate more on building mechanisms to support at-risk activists and critical users in a coordinated, multi-faceted manner that could include physical security support, legal support, awareness raising, and digital security support.

Increase citizens' role in promoting digital rights

African countries need legislative and policy environments that enable the digital society to thrive – be it in the areas of innovation, affordable access or enjoyment of digital rights. Currently, there is limited citizens' participation in making laws and regulations around the use of the internet and associated technologies. This could be attributed to weak consultative mechanisms by policy makers who often give limited time for feedback on the draft laws and, where feedback is offered, it is often disregarded. Citizens are thus encouraged to be more proactive in the policy making processes in addition to offering alternative positions to governments rather than only offering criticism. Policy makers should also be more transparent in the policy-making process by offering more time for consultations and meaningfully considering the inputs they receive from citizens and other interested parties.

'

Digital rights actors also need to adopt a multi-stakeholder approach in the promotion digital rights. This includes involving traditional human rights organisations, women's rights organisations, and private sector actors, among others, in campaigns to advance digital rights.

Increase state actor's respect for digital rights

State actors should appreciate that undue restrictions to ICT access and usage, be it network disruptions, unwarranted content regulations, or disappropriate digital taxation, have far-reaching impacts on individuals' livelihoods and the health of the national economy. They thus undermine governments' efforts to solve development challenges and achieve the 2030 Agenda for Sustainable Development as stipulated in the United Nations General Assembly resolution 73/218. State actors are also reminded to uphold citizens' rights by recognising that the same rights that apply offline also apply online as stipulated by the United Nations Human Rights Council in June 2016 and also reaffirmed in July 2018.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org