Published by EISA
14 Park Rd, Richmond
Johannesburg
South Africa
P O Box 740
Auckland Park
2006
South Africa
Tel: 27 11 381 6000
Fax: 27 11 482 6163
Email: eisa@eisa.org
www.eisa.org

© EISA 2022

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of EISA.
First published 2022

Layout and printing by Corpnet, Johannesburg
CONTENTS

INTRODUCTION 4

DIGITAL POLITICS AND INTERNET PENETRATION IN AFRICA 4

DIGITAL CENSORSHIP IN AFRICA 5

POLICY ALTERNATIVES GOING FORWARD 7

CONCLUSION 8

REFERENCES 10

Michael Asiedu
INTRODUCTION

In February 1996, the Zambian government achieved its objective of removing a banned edition of The Post from the newspaper’s online platform (website) (Bureau of Democracy, Human Rights, and Labor 1997; Burnheim 1999, p. 2). It embarked on this process by threatening to press charges against the country’s main internet service provider (ISP), Zamnet. This edition of The Post was banned under Zambia’s Preservation of Public Safety Act for allegedly covering leaked documents exposing the government’s secret plans for a referendum to adopt a new constitution. This case is one of the early instances of digital (internet) censorship in Africa. The phenomenon of digital censorship has since grown significantly both in its use by public authorities as an authoritarian tactic and in terms of its impact as felt by citizens across Africa as far as democratic governance is concerned.

This policy brief is set out in three parts to contribute to the growing conversation on the topic. It does so by first examining digital politics and internet penetration as well as the relationship between the internet and democracy in Africa. The second part delves into some instances of digital censorship in Africa alongside a digital censorship toolkit which contains methods usually used by public authorities in carrying out this practice. Subsequently, laws in selected countries that are set up in order to enable digital censorship are explored. This is further complemented by acknowledging the difficulties the Covid-19 pandemic has added to the phenomenon of digital censorship. A clear understanding of this toolkit used for censorship, as well as the context within which these tactics are used, is necessary for considering a framework for dealing with these trends going forward. The third and final part of the brief lays pathways in the form of policy recommendations, where ultimately it will be the collective efforts of civil societies and an awakened citizenry backed by legislation to check abuse of the digital sphere by leaders with authoritarian tendencies.

PART ONE

DIGITAL POLITICS AND INTERNET PENETRATION IN AFRICA

Digital politics is the way internet technologies have increased the complex interplay between political actors and their constituencies (Vaccari 2013; Miller 2016). Digitalization has changed and is changing the way politics is done both globally and in Africa. Every major political institution (government institutions, political parties etc.) in Africa has an online presence, be it a social media platform or its unique website, to reach a much broader audience than just the non-voting population. Citizens and individuals (residents) alike also have a personal online presence, most especially via social media platforms such as Facebook, Twitter, YouTube, WhatsApp etc. These have heightened both online public discourses across Africa and how citizens respond to government policies. In fact, the internet penetration rate in Africa stood at 39.3% in 2020, a significant increase on the less than 1% in 2000. This means about four in 10 individuals have used the internet (web) in Africa, although this lags the global internet penetration average of 60% (Faria 2020). In terms of country demographics, Kenya has the highest internet penetration rate in Africa of about 85.2%, with Eritrea and Western Sahara having 6.9% and 4.6% respectively – the lowest in Africa. About 75% of all this web traffic is via mobile phones with the rest via personal computers (PCs), an indication that mobile phones are much cheaper and more easily accessible in comparison to PCs (Johnson 2021). Has this increasing internet penetration dramatically changed the dynamics of democracy on the continent?

THE INTERNET AND DEMOCRACY IN AFRICA

The internet and its impact on democracy has received the attention of many researchers in developed countries both conceptually and theoretically (see for example Nam 2017; Pirannejad 2017; Shen 2017; Evans 2018a etc.). Prior to the 2000s, researchers revealed that the internet was an insignificant predictor of democracy; however, it has since become a strong predictor of democracy post the 2000s (Best & Wade 2009). Using a panel data analysis model for the period 2000-2014 Pirannejad (2017) ascertained that internet extension has a significant and positive impact on democracy promotion. For his part, Salgado (2012) demonstrates in his research that the internet has indeed impacted civil society in places like Angola and Mozambique positively through the promotion of participation and the creation of new independent media, in the form of journalists using the internet to express their opinions and the intention of different actors in the public sphere. These benefits associated with increased internet penetration is applicable to other African countries as well. Nisbet et al. (2012) in turn found that internet usage enhances higher citizen commitment to democratic governance in Africa. Finally, empirical evidence on the internet and democracy in Africa suggests that internet usage and democracy are highly interrelated to each other in Africa (Olanji 2018). Thus, Africa has been moving towards a new stage where the internet will lead to improved levels of democracy and digital politics, at least at the macro level (Olanji 2018). Given this development, control over the internet by certain governments has become a notable trend. In particular, there have been numerous and increasing instances of government over-reach and censorship in an attempt to both gain and retain power.
Digital censorship toolkit

i. Domain name system (DNS): with this tampering of the web, instructions can be given to deregister a domain that is hosting any objectionable content according to public authorities. The website can therefore become invisible to users because it fails to translate domain names into the internet protocol (IP) address. An example would be receiving the wrong phone digits of the person you intend to call.

ii. Filtering: There is keyword filtering, which restricts only websites that are plainly blacklisted or those that share the same server. For instance, a government intending to block content on Subject Y will target such websites only. This is a tricky exercise, since it does not prevent the creation of new websites with similar content. A more advanced scenario is using the Uniform Resource Locator (URL) filtering mechanism, which looks for targeted words and simply restricts their connections. Packet filtering also serves as a handy strategy. It scans the contents of an actual page for banned keywords and gives users error messages (server not found) on their browsers without any indication that they are being censored.

iii. Internet protocol (IP) blocking also blacklists addresses of websites that governments do not like. Here the connection is dropped by the internet service provider (ISP). This method requires surveillance computers which check an internet search request against blacklisted IP addresses.

iv. Throttling: This restricts traffic to specific websites, giving the impression that the internet service is slow thereby discouraging access. This is trickier, since it is difficult to verify whether the websites are being deliberately restricted or whether the connection is

PART TWO
DIGITAL CENSORSHIP IN AFRICA

Digital censorship falls into the broader concept of “digital authoritarianism”, which can include governments using technologies to surveil their citizens (Yuan 2018) – thus, the opposite of digital democracy where a participatory use of the internet space is encouraged as far as opinions on public issues are concerned (Figueiredo 2016). This has become the main trend given that traditional means of censorship are increasingly becoming extinct. Traditionally, when there were few news outlets – in the form of newspapers, magazines, broadcasts etc. – governments were able to ban the release of these or redact questionable content before it was made public (Bennet & Naim 2015). Increased digitalization has made such attempts almost impossible – hence the resort to digital censorship. Not only are news outlets targeted, but any online user could be targeted. Digital censorship at its core refers to the means employed by governments to prevent information from reaching users, some of which are explained below.

Digital censorship toolkit

i. Domain name system (DNS): with this tampering of the web, instructions can be given to deregister a domain that is hosting any objectionable content according to public authorities. The website can therefore become invisible to users because it fails to translate domain names into the internet protocol (IP) address. An example would be receiving the wrong phone digits of the person you intend to call.

ii. Filtering: There is keyword filtering, which restricts only websites that are plainly blacklisted or those that share the same server. For instance, a government intending to block content on Subject Y will target such websites only. This is a tricky exercise, since it does not prevent the creation of new websites with similar content. A more advanced scenario is using the Uniform Resource Locator (URL) filtering mechanism, which looks for targeted words and simply restricts their connections. Packet filtering also serves as a handy strategy. It scans the contents of an actual page for banned keywords and gives users error messages (server not found) on their browsers without any indication that they are being censored.

iii. Internet protocol (IP) blocking also blacklists addresses of websites that governments do not like. Here the connection is dropped by the internet service provider (ISP). This method requires surveillance computers which check an internet search request against blacklisted IP addresses.

iv. Throttling: This restricts traffic to specific websites, giving the impression that the internet service is slow thereby discouraging access. This is trickier, since it is difficult to verify whether the websites are being deliberately restricted or whether the connection is

v. Internet shutdowns (blackouts): This is the most extreme form of all these methods, and at least 100 internet shutdown cases were experienced in Africa between 2018 and 2021. Also, Africa has the greatest number of internet disruptions in the world after Asia (Access Now 2021). Governments have used internet disruptions involving some of the methods explained above reactively during socio-economic protests in places such as Zimbabwe, civil unrest in Ethiopia, Egypt, and Sudan, and in the lead-up to elections in places such as Uganda, Tanzania, Malawi etc. Modus operandi of governments (public authorities)

Irrespective of the method in the digital censorship toolkit, the modus operandi of public authorities is similar. An order (directive) is usually given to an ISP, especially with internet shutdowns, to cut off internet connections either in a targeted manner (restricting access to a particular geographic area) or total service restrictions (these could affect the internet services of an entire country). The leading three reasons given by governments or public authorities for these internet disruptions are: national security, public safety and checking the spread of illegal content (Access Now 2021). Below I give a snapshot of how some governments use the law to monitor the digital space in Africa.

Monitoring the digital space using the law in Africa

a. Ethiopia, which has experienced a series of internet shutdowns, has a Freedom of Mass Media and Access to Information Act, 2008, as well as an Anti-Terrorism Proclamation Act, 2009, that has enabled it to exercise strict control over the internet with the use of internet filtering, content blocking and surveillance (Yohannes 2011). Consequently, bloggers and journalists have been prosecuted in court due to their writings online. TOR, an open-source internet anonymizer (it makes a user anonymous), reported that the country’s then only telco, Ethio Telecom, used deep packet inspection (DPI) to block access to TOR service in 2012 (Ashford 2012). The country also passed a rule for internet café owners mandating that they report content making computer screens visible to internet café owners. In 2020 the country also passed a hate speech law, where a $3,100 fine or a three-year jail term lay in prospect for anyone judged guilty of spreading hate speech online (Wanyama 2020).

b. Zimbabwe has a Postal and Telecommunications Act, 2000, which permits government to observe email usage and demands that ISPs provide information to public authorities upon request. Although the country’s Supreme Court has rendered this Act to be ultra vires (unconstitutional), Zimbabwe introduced the Interception of Communications Act, 2007, which enabled the establishment of a “Monitoring and
has its Digital Code Act, 2018, which indicates that such rights may be restricted as far as necessary in a democratic society to safeguard national security, public order health and safety as well as public morals, etc. The twist as learnt from the above is how some African governments have exploited this to abuse Africa’s blossoming digital sphere. The Covid-19 pandemic, which can be classified as a public health emergency, has not helped either as far as digital censorship is concerned.

Digital censorship and Covid-19 in Africa

Data on how African governments have dealt with Covid-19 remains relatively sketchy. However, evidence abounds on how governments have used the pandemic to control the digital space of journalists, human rights defenders etc. – especially those critical of how certain governments handled the pandemic. For instance, in March 2020, Cyprian Nyakudi, a Kenyan blogger, was arrested for posting on Twitter that a senior Kenya Revenue Authority official had travelled out of Kenya and failed to self-quarantine upon return (Ombati 2020). Egypt also expelled Ruth Michaelson, a Guardian reporter from in March 2020: her reportage had questioned the authenticity of Egyptian government official Covid-19 statistics. Subsequently the State Information Service revoked the credentials of The Guardian and demanded an apology while also warning The New York Times over its reportage on the government alongside the newspaper’s social media posts on Twitter about the Covid-19 pandemic (Committee to Protect Journalists 2020). Countries such as Somalia, Ghana, Rwanda, Nigeria, Tanzania, Burundi etc. all had similar instances where a journalist or a citizen in the news business etc. was arrested during the pandemic (CIPESA 2020). A lingering problem relates to what will happen with data gathered by public authorities through the Covid-19 tracing applications (apps) used. In order to check some of these excesses as far as the digital space is concerned, concrete policy measures are needed, some of which are explained below.

PART THREE

Policy alternatives going forward

Civil society and the use of courts

Telcos and ISPs are licensed by governments agencies, which means they encounter difficulty in renewing their licences when they overtly challenge government directives for internet disruptions. The onus therefore lies on internet freedom organizations, media organizations, journalists as well as concerned citizens to challenge these illegal internet disruption orders using the court system. Fortunately, there have been some positive victories in Zimbabwe, Sudan, and Togo through the court system on illegal internet shutdown orders. This paves way for jurisprudence building around digital censorship (Asiedu 2020).
Telcos/ISPs, political parties and electoral bodies

For Telcos and ISPs to stand up to incumbent governments will be difficult, because in some instances governments have major stakes in them. However, a three-pronged approach could be pursued. Political parties in respective countries should team up with electoral bodies as well as civil societies etc. to sign a memorandum of understanding (MoU), especially in the lead-up to elections, campaigning periods, and declaration of results, that there should be no internet disruptions. Again, in instances where governments have significant control over political institutions this will be difficult, but this will kickstart the conversation that will lead up to a potential legislation on internet openness in and around electioneering periods in African countries.

Access and private sector collaboration

Access in terms of internet infrastructure should be expanded with buy-in from the private sector, not thwarted by governments. Irrespective of the significant increase in internet penetration over the years in Africa there is still a huge gap to be filled, since the continent remains the least connected. Those offline are relatively absent from participation in digital democratic spaces. The consensus has been that the right to communicate is a human right; for instance, as far back as December 1997, the UN General Assembly endorsed a statement enjoining the UN system to pursue the goal of universal access to basic communication and information services in order for all to secure sustainable human development. Thus, in terms of access, the information poverty gap should be bridged rather than deliberate measures implemented that aim to curtail it through digital censorships.

VPN for good

VPNs are used in countries where the internet is partially cut off – for instance, if social media platforms are shut down – but rendered useless if there is a total blackout. Civil societies must begin listing proven VPNs on their websites for the public good. Caution must, however, be taken, as governments can instruct VPNs to be blocked. They are usually less inclined to do so as this may sometimes trouble big companies and foreign diplomats which use them because they offer additional security protocols.

CONCLUSION

In terms of digital censorship, it must be emphasized that no African government has the technical capacity to surveil or control the entire internet service in their respective jurisdictions – unless a total internet shutdown order is given. This is the reason why attempts to segment and curtail parts of it should be confronted head on by both concerned citizens, civil societies, private companies and other concerned stakeholders, as the internet is the currency for digital democracy. With the combined efforts of civil society, public institutions such as courts, electoral bodies and an awakened citizenry, pragmatic steps could be taken (some of which have been proposed above) in challenging,remedying or preventing some of this digital censorship, especially with Africa’s digital democratic future in perspective. Finally, African citizens in the diaspora must keep on monitoring digital rights issues on the continent and add their voices to the conversation whenever abuses occur, since some of them tend to be in relatively more stable democracies. This is what happened in the case of Zamnet in Zambia: a resident in the US posted the banned edition of The Post on his website. This meant anyone with internet could still access it, thereby promoting the freedom to share and access information, which is one of the cornerstones of digital rights.
References


Pirannejad, A. 2017. ‘Can the Internet promote democracy? A cross-country study based on dynamic panel data models’. Information


Since its inception in July 1996 EISA has established itself as a leading institution and influential player dealing with elections and democracy related issues in the African continent. EISA has past and/or current field offices in 20 African countries. The organisation's Strategic Goals are:

- Electoral processes are inclusive, transparent, peaceful and well-managed;
- Citizens participate effectively in the democratic process;
- Political institutions and processes are democratic and function effectively; and
- EISA is a stronger and more influential organisation

The vision of EISA is "an African continent where democratic governance, human rights and citizen participation are upheld in a peaceful environment". This vision is executed through the organisational mission of "striving for excellence in the promotion of credible elections, participatory democracy, a human rights culture, and the strengthening of governance institutions for the consolidation of democracy in Africa".

Having supported and/or observed over 100 electoral processes in Africa, EISA has extensive experience in formulating, structuring and implementing democratic and electoral initiatives. It has built an internationally recognised centre for policy, research and information and provides this service to electoral management bodies, political parties, parliaments, national and local governments and civil society organisations in a variety of areas, such as voter and civic education and electoral assistance and observation. Besides its expanded geographical scope, the Institute works in the in-between election areas along the electoral and parliamentary cycle, including constitution building processes, legislative strengthening, conflict management and transformation, political party development and strengthening and supporting capacity building for members of parliament and parliamentary structures. EISA also provides technical assistance to continental and regional inter-governmental institutions, Election Management Bodies and Civil Society Organisations.
This publication and series are made possible through the generous financial support of the Government of Sweden through the Swedish International Development Cooperation Agency (Sida).