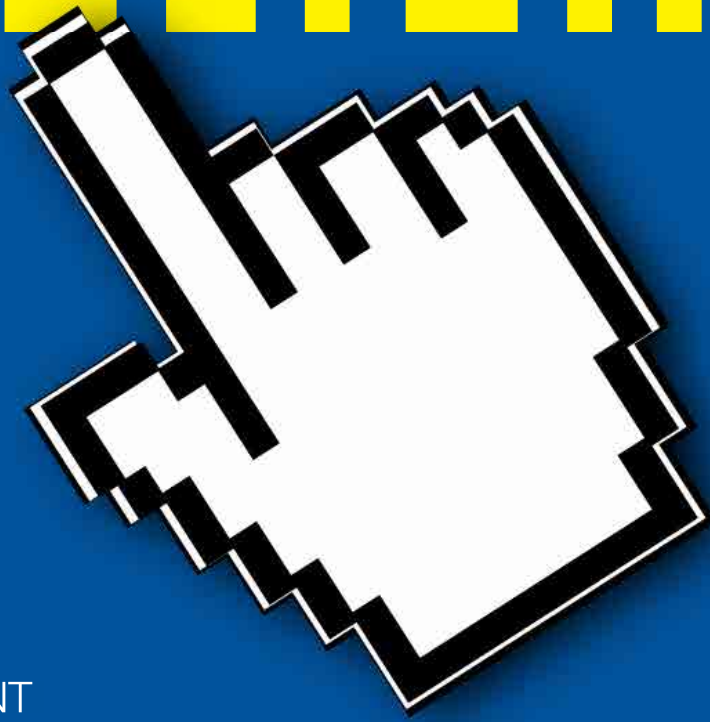


BEYOND A CLICK



REGIONAL
ASSESSMENT
ON STATE OF
DIGITAL RIGHTS

SOUTHERN AFRICA

Published by

Media Institute of Southern Africa Zimbabwe Chapter
Harare, Zimbabwe
Telephone: +263242776165/ +263242746838
www.zimbabwe.misa.org

Funder

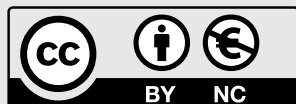


Konrad
Adenauer
Stiftung

Report prepared for Misa by
Cade Zvavanjanja**Design and Layout**

OnaDsgnStudio*
hello@onadsgnstudio.com

ISBN
9781779065353



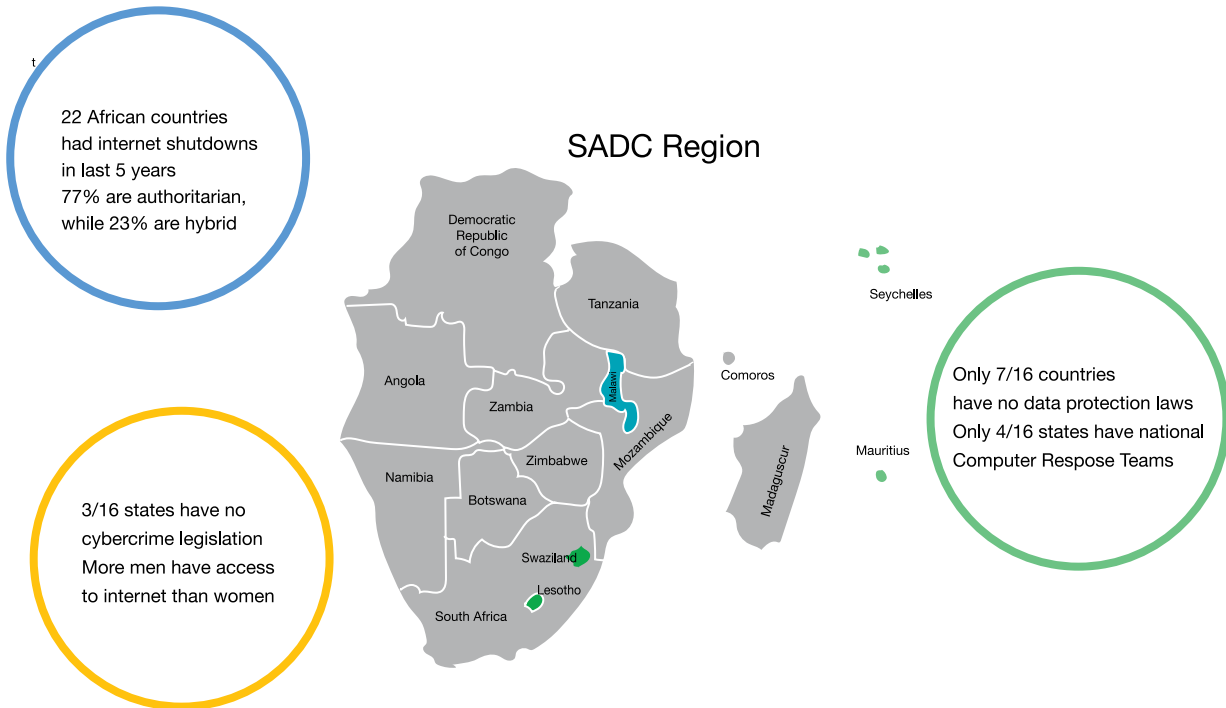
This work is licensed under a Creative Commons
Attribution-NonCommercial 4.0 International License.

1.0	Key Highlights	04
2.0	Objective(s)	05
	2.1 Methodology	
3.0	Background	06
4.0	Digital rights are human rights	08
5.0	Freedom Online	08
6.0	Internet Access and Affordability	10
	6.1 Connections Trends for Selected SADC member states	
	6.2 Barriers to internet access and freedom of expression and access to information through mobile phone	
	6.3 Affordability of internet	
	6.4 Taxation of social media and content	
	6.4.1 Case Study of Tanzania – Taxation of Online Content	
	6.4.2 Case study of Zambia – Taxation of ‘Social Media’ Calls	
	6.5 Sub-standard service delivery	
	6.5.1 Zambia Case Study – Sub-Standard Standard Service Delivery	
	6.5.2 Zimbabwe Case Study - Sub-Standard Standard Service Delivery	
	6.5.3 Tanzania Case study	
	6.8 Other Barriers	
7.0	Internet Shut down(s)	22
	7.1 Democratic Republic of Congo Case Study – Internet Shutdown	
	7.2 Zimbabwe Case Study – Internet Shutdown	
8.0	Just in Time temporary service disconnections	23
	8.1 Namibia and Swaziland Case Studies – Just in time disconnections	
9	Potential of more shut downs in Southern Africa	24
10	Privacy, Data protection and Cybersecurity	25
11.0	Constitutional Provisions of Digital Rights	27
	11.1 Case of Zimbabwe - Constitutional Provision	
	11.2 Case of Tanzania - Constitutional Provision	
	11.3 Case of Democratic Republic of Congo - Constitutional Provision	
	11.4 Case of Malawi - Constitutional Provision	
12	Impact of HIPSSA SADC Model Law on Digital Rights	28
13	Data protection	31
	13.1 The AU Data Protection Convention	
14.0	Privacy and Personal Data Protection Cases of Concern	32
	14.1 SIM card registration	
	14.2 Surveillance	
	14.2.1 Case of South Africa - Surveillance	
	14.2.2 Case of Tanzania - Surveillance	
	14.2.3 Case of Zimbabwe - Surveillance	
	14.3 Dataveillance	
15	Internet Governance	36
16	Attacks on Journalist	37
17	Overall Recommendations	38
18	Conclusion	39

Key Highlights

2 SADC states had total Internet shutdown in 1st quarter of 2019
There is significant potential of more shutdowns in the region as:

- a. Only 1/5 sampled states are consider free (internet freedom)
- b. Half (8/16) states have elections in 2019
- c. Non is considered to have full democracy (Democracy index)



Only 2/16 states have cyber security legislation
Only 5/16 states data privacy protection laws
Only 7/16 states have National Internet Governance Forums (NIGFs)

Assult and detainment are the top attack against Journalist

Objective(s)

The overall objective of this analytical paper is to improve the understanding of digital rights in **Southern Africa region**¹, by evaluating the status quo, identifying gaps and proffer research based recommendations to stakeholders in the region and beyond.

The specific objectives of the study are as follows:

1. Undertake a comprehensive research on the current progress on the internet growth in the SADC region vis-à-vis freedom of expression and access to information
2. Locate key trends pertaining to digital rights in the region and their implications to expression and access to information
3. Regional comparative analysis on how other countries are faring pertaining to the promotion and enjoyment of digital rights in the region
4. Outline the legal and statutory environment defining digital rights in the region and how the internet is being regulated
5. Evaluate the impact of the African Union on Cyber Security and Personal Data Protection & the SADC Cyber Security Model Law on enjoyment of digital rights in the region.
6. Analyse What the trends pertaining to surveillance; privacy and data protection; freedom of expression and Cyber security
7. Come up with policy proposals for the government and the stakeholders

2.1 Methodology

To achieve the aforementioned objective(s), we have adopted the following methodology: explore key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet; Mapping of existing policies², trends and stakeholders actions, experiences and aspirations regarding digital rights; and, analysis of regional case studies .Data was sought through a

desktop research based mainly from secondary sources³ and some primary source data. The primary data was collected from submissions and reports to MISA. Also, as part of the primary data collection some network availability tests were undertaken. Secondary sources used included various journals, court proceedings and reports, regulators reports, policy documents, position papers, news articles and related other literature.

¹ Southern Africa working definition for this paper is: "states and territories covered by the sixteen member states of SADC" . see <https://www.sadc.int/member-states/>

² See <https://dictionary.cambridge.org/dictionary/english/policy>

³ See <https://www.statisticshowto.datasciencecentral.com/primary-data-secondary/>

Background

Digital age⁴ has brought many opportunities and challenges. The key challenges are: how to harness the opportunities while enjoying and protecting human rights; and, how to translate ‘traditional’⁵ offline rights into online rights. The key question is ‘how to guarantee and protect human rights online? The nature of digital age and globalization has broken geographical boundaries, legal territories and jurisdictions. Africa and specifically Southern Africa as part of the global digital village has not been spared by the dilemma of technology and human rights.

Digital rights are an extension of ‘human rights in the offline’ world as recognised, protected and promoted by international laws and conventions⁶. These include the right to freedom of expression, the right to privacy, and the right to freedom from censorship and online surveillance, to name a few⁷. These rights are in line with the Universal Declaration of Human Rights (UDHR)⁸. The UN Human Rights Council has affirmed in a number of resolutions that “the same rights that people have offline must also be protected online.”⁹



⁴ See <https://www.igi-global.com/dictionary/digital-age/7562>

⁵ Approaches, regulations, treaties and provisions instituted pre-internet, see <https://www.entrepreneur.com/article/330023>

⁶ https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyInDigitalAge/A_HRC_39_29_EN.docx

⁷ See <https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression>

⁸ See <http://www.un.org/en/universal-declaration-human-rights/>

⁹ See <https://www.article19.org/resources/unhrc-significant-resolution-reaffirming-human-rights-online-adopted/>

There over twenty frameworks to build on, made up of regional treaties, charters, resolutions, declarations and protocols specifically produced to ensure and protect the protection of human rights¹⁰ in the digital era, mainly online, key ones are as follows:

1. The African Declaration on Internet Rights and Freedoms¹¹
2. Banjul Charter: African Charter on Human and Peoples' Rights (1981)¹²
3. APC Internet Rights Charter¹³
4. UN General Assembly resolution of 2013 on The right to privacy in the digital age¹⁴;
5. The Internet and Human Rights; the United Nations Guiding Principles on Business and Human Rights¹⁵;
6. Johannesburg Principles on Freedom of Expression and National Security¹⁶;
7. The Manila Principles on Intermediary Liability¹⁷.
8. SADC declaration¹⁸ on the role of information and communication in building the
9. Southern African development community
10. Windhoek Declaration on Promoting an Independent and Pluralistic African Press (1991)¹⁹,
11. African Charter on Broadcasting (2001)²⁰
12. Declaration of Principles on Freedom of Expression in Africa of 2002, amendment (2012)²¹
13. African Platform on Access to Information Declaration of 2011²²
14. African Union Convention on Cyber-security and Personal Data Protection of 2014²³;
15. Joint Declaration of 2011 concerning Freedom of Expression and the Internet by the four Special Rapporteurs on Freedom of Expression²⁴

10 See <http://africaninternetrights.org/articles/>

11 See <https://africaninternetrights.org/about/>

12 See <http://www.achpr.org/instruments/achpr/>

13 See <https://www.apc.org/en/pubs/about-apc/apc-internet-rights-charter>

14 See <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx>

15 See https://www.ohchr.org/documents/publications/GuidingPrinciplesBusinesshr_eN.pdf

16 See <https://www.article19.org/wp-content/uploads/2018/02/johburg-principles.pdf>

17 See https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf

18 https://www.sadc.int/files/8113/5340/6247/DECLARATION_ON_THE_ROLE_OF_INFORMATION_AND_COMMUNICATION.PDF.pdf

19 See <http://hr.library.unn.edu/achpr/expressionfreedomres.html>

20 See http://portal.unesco.org/en/ev.php-URL_ID=47094&URL_DO=DO_TOPIC&URL_SECTION=201.html

21 See <http://www.achpr.org/sessions/51st/resolutions/222/>

22 See <http://whk25.misa.org/media-law/african-platform-for-access-to-information-declaration-2011/>

23 See https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

24 <https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=15921&LangID=E>

United Nations Human Rights Council resolution of 2012 on The promotion, protection and enjoyment of human rights on the Internet²⁵; It is important to note that while these 'frameworks', be it, UN and/or regional resolutions urge member states to protect and promote human rights on the internet, there are not all legally-binding²⁶ and are continuously challenged by governments, private companies in many countries around the world, hence the need for domestication, continuous monitoring, gap identification, evaluation

and advocacy for observance and adherence to the letter and spirit of the framework(s).

Striking the critical and delicate balance of state power and rights of citizens is the ultimate icon of democracy and a symbol for generation to come. The more internet-based innovation are adopted and used the more easier means to exercising offline and online rights such as freedom of speech, right of expression, freedom of association and assembly. Social media for example has made it far easier to enjoy

freedom of association and self-expression. As a counter to the growing adoption of technology and easier ways to enjoy rights, some governments intending to limit the rights and maintain control, have set out legislative contingencies that allow them intercept, block and prosecute activities and traffic on the internet in the veil of national security, emergency management and protection of citizens. Many a times these situations in which a government can exercise this power are often not recorded, reported and monitored enough.²⁷

4.0

Digital rights are human rights

United Nations Human Rights Council resolution of 2012 brought about prominence of 'digital rights', when it resolved that the "same rights that people have offline must also be protected online." This means that the rights that are enshrined in most constitutions, like free speech and freedom to assembly also exist in the online world. The advent of the internet and exponential growth in access to the internet and other information and communications technologies (ICTs), digital rights have become indispensable to the way in which people around the world exercise and enjoy

their fundamental rights. It is now firmly entrenched by both the African Commission on Human and Peoples' Rights²⁸ (ACHPR) and the United Nations²⁹ (UN) that the same rights that people have offline must also be protected online, in particular the right to freedom of expression, rights to privacy and access to information.

Digital rights can therefore be defined as the rights that are implicated in the access to and use of the internet and other ICTs³⁰. The right to freedom of expression applies regardless of frontiers, through any media of one's choice.³¹ With the

relationship and equality of rights³², it has been seen that 'digital rights' and other 'fundamentals rights' are inherently linked; there is an array of other rights that are also implicated when digital rights are affected, including the right to life, rights to equality, education, freedom of assembly, healthcare and ultimately life. The exercise of digital rights also enables access to a range of services, such as, financial services, financial inclusivity, utilities, governance, health and education.

25 See <https://www.osce.org/fom/250856>

26 See <https://www.dfa.ie/our-role/policies/international-priorities/international-law/how-international-law-works/>

27 See the Article 35 of the International Telecommunication Union (ITU) Constitution http://www.itu.int/dms_pub/itu-s/oth/02/09/S02090000115201PDFE.PDF

28 See <http://www.achpr.org/>

29 See <http://www.un.org/en/>

30 <https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf>

31 See <http://www.un.org/en/universal-declaration-human-rights/>

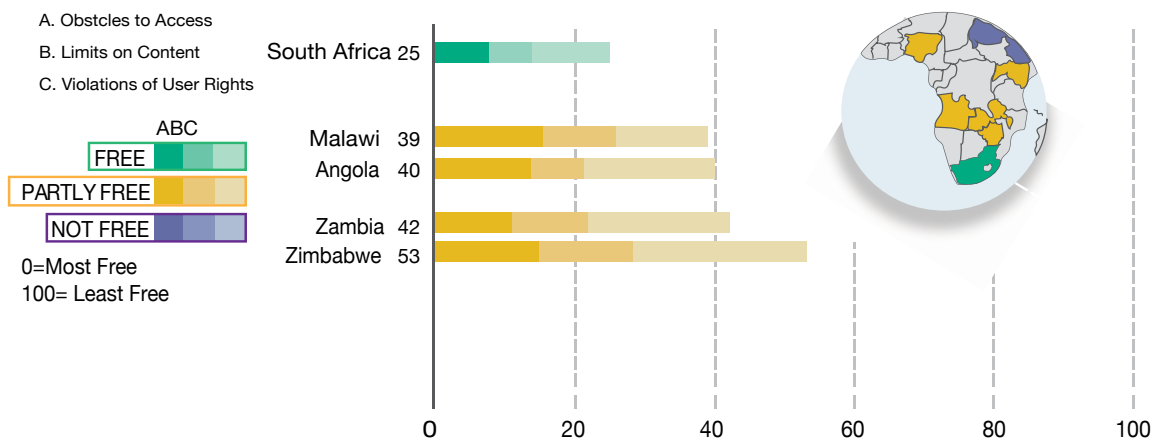
32 See <https://www.equallyhumanrights.com/en/human-rights-act/article-11-freedom-assembly-and-association>

Freedom Online ^{33 34}

All the states in the region are parties³⁵ to the International Covenant on Civil and Political Rights and to the African Charter on Human and Peoples' Rights³⁶. In keeping with their obligations under these human rights treaties, most states in the sub-region have constitutions³⁷ which protect and provide for enjoyment of fundamental human rights. Four states in the southern African sub-region have separate constitutional articles which specifically protect the right to information in some form.³⁸ In some constitutions freedom of information is not specifically mentioned, while in others the right to seek and/or receive information is spelt out within the general freedom of expression article.

According to a research by Freedom house³⁹ "The internet is growing less free around the world, and democracy itself is withering under its influence." "Disinformation and propaganda disseminated online have poisoned the public sphere. The unbridled collection of personal data has broken down traditional notions of privacy. And a cohort of countries is moving toward digital authoritarianism by embracing the Chinese model of extensive censorship and automated surveillance systems. As a result of these trends, global internet freedom declined for the eighth consecutive year in 2018". **Figure 2** below shows the 'state of internet freedoms'⁴⁰ in selected five countries in the region:

Figure 2: Internet Freedom status for Some Southern Africa Countries



Source: Own illustration based on data from Freedom House (2019)⁴¹

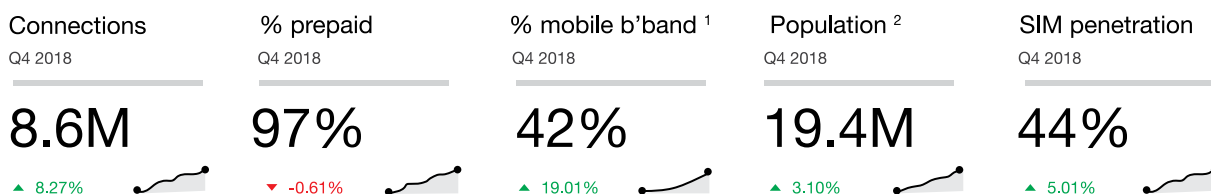
The above status quo of internet freedom in the region is of huge concern⁴². There is urgent need to address obstacles to access, reduce limits on content and aim for zero violations of user rights.

33 Resolution on the Right to Freedom of Expression on the Internet in Africa – ACHPR/Res. 362(LX) 2016 – adopted by the African Commission on Human and Peoples' Rights (ACHPR) in Banjul on 4 November 2016.
 34 Everyone has the right to hold opinions without interference. Everyone has a right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds through the Internet and digital technologies and regardless of frontiers. The exercise of this right should not be subject to any restrictions, except those which are provided by law, pursue a legitimate aim as expressly listed under international human rights law and are necessary and proportionate in pursuance of a legitimate aim.
 35 https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=en&mtdsq_no=IV-4&src=IND
 36 See <http://www.achpr.org/instruments/achpr/ratification/>
 37 See <https://academic.oup.com/icoor/article/11/2/414/753618>
 38 Malawi, South Africa, Mozambique and Tanzania.
 39 https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf
 40 Freedom on the Net measures the level of internet and digital media freedom in 65 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of FREE (0-30 points), PARTLY FREE (31-60 points), or NOT FREE (61-100 points). Ratings are determined through an examination of three broad categories: A. OBSTACLES TO ACCESS: Assesses infrastructural and economic barriers to access; government efforts to block specific applications or technologies; and legal, regulatory, and ownership control over internet and mobile phone access providers. B. LIMITS ON CONTENT: Examines filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism. C. VIOLATIONS OF USER RIGHTS: Measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity.
 41 https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf
 42 of the five countries studied under internet freedom 2018, by Freedom house only 1 is free

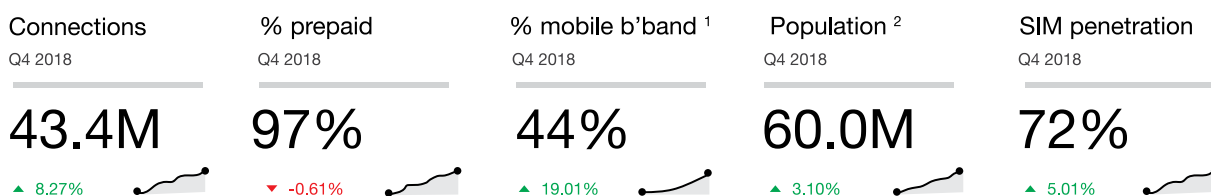
6.1 Connections Trends for Selected SADC member states

Fig 3: Connections Trends for Selected Countries:

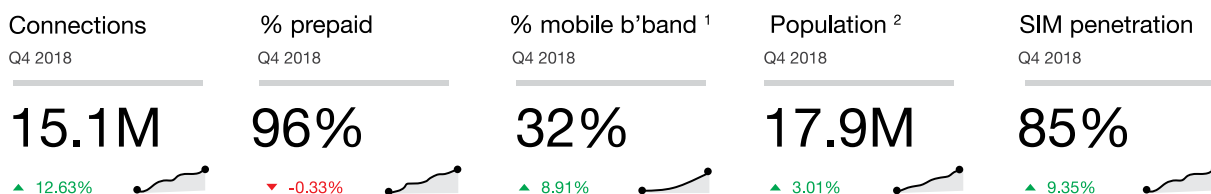
6.1.1 Malawi



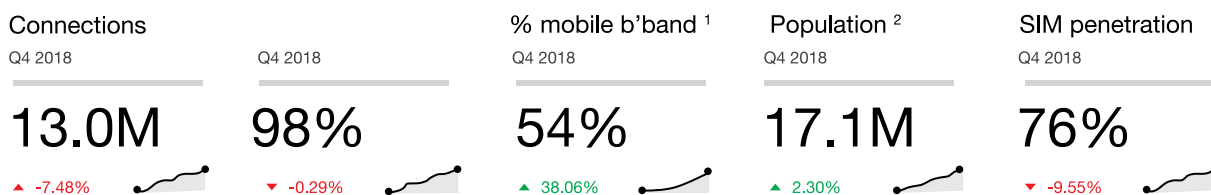
6.1.2 Tanzania



6.1.3 Zambia



6.1.4 Zimbabwe



Source: GSMA⁴⁶

⁴⁶ See GSMA Wireless Intelligence : <https://www.gsmaintelligence.com/>

From the sampled countries the data show an upward trend, the uptake of broadband Internet services is showing a slower trend in growth as shown in Figure 4 below. Regional totals and percentage of mobile Internet subscribers (smartphones and tablet devices) as a share of total unique mobile subscribers is increasing throughout Africa and mainly in Southern Africa as in figure 5 below. The data below show that Southern Africa in particular is experiencing slow growth. Demographic factors, such as income level and geographic location, are likely hampering uptake in the region as opposed to developed world, which has higher average income. A comparison of mobile subscriptions across African Regions is given in figure 4:

Fig 4: Total Unique Mobile Subscriptions, 2008–18

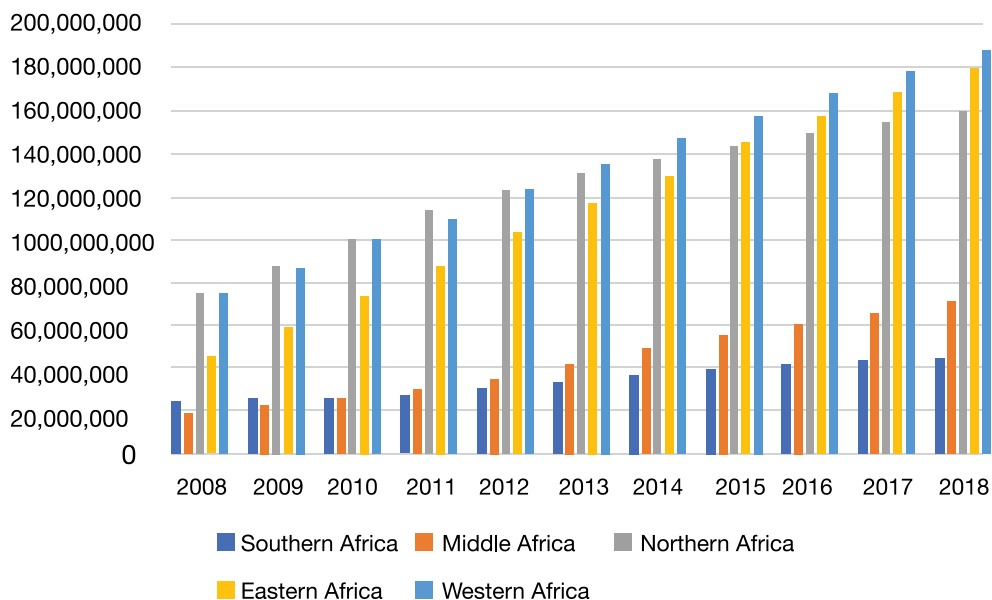
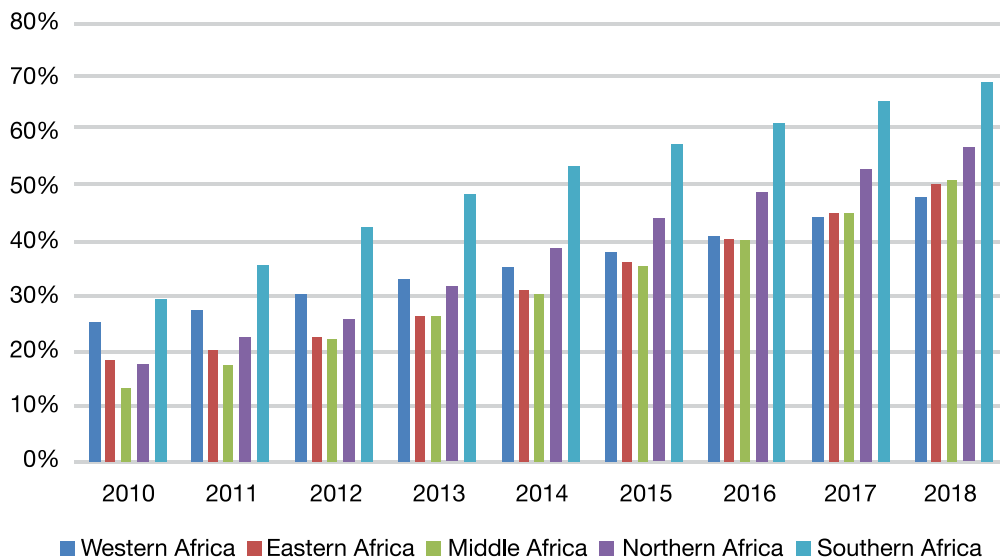


Fig 5: Mobile Internet Subscribers as a Share of Total Mobile Subscribers, 2010–18

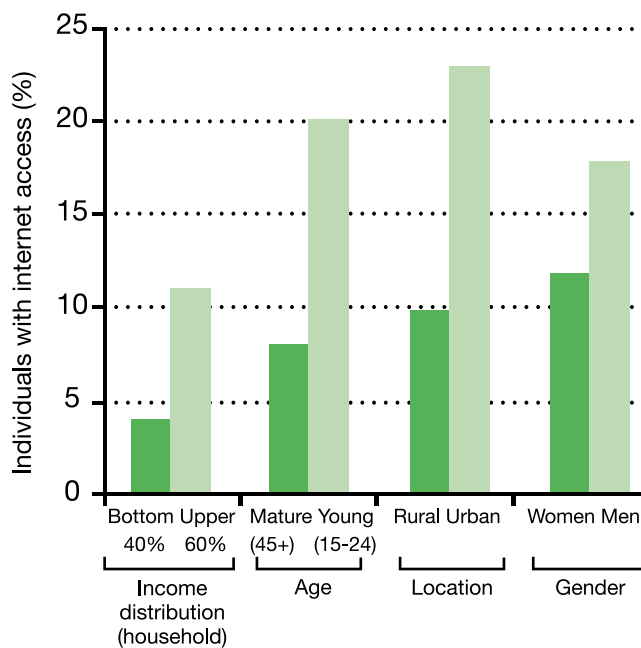


Source: GSMA⁴⁷

47 See GSMA Wireless Intelligence : <https://www.gsmaintelligence.com/>

6.2 Barriers to internet access and freedom of expression and access to information through mobile phone

Fig 6: Internet Access based on different social groupings: Digital divide.



Comment:

Income, age, location and gender are some of the key factors affecting internet access. Upper income, Youth (15-24 years) and Urban people have over double numbers of people in low income, mature (45+ years) and rural respectively. Men have more access than women. To achieve full digital rights the digital divide needs to be closed through multi-stakeholder participation and efforts. Policies, technical support and legislation toward equal and equitable access are needed.

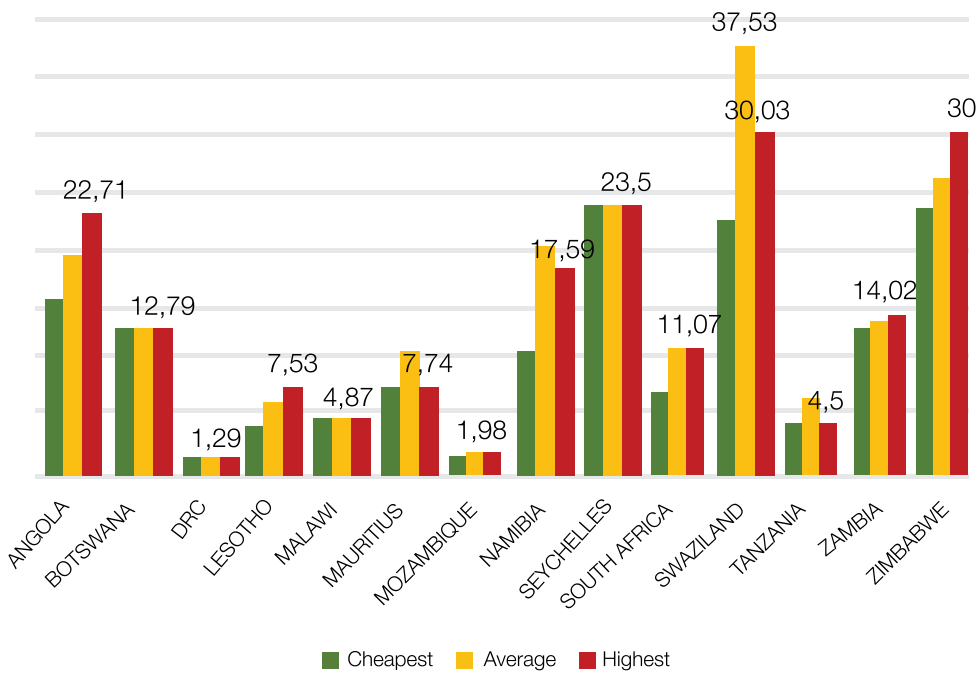
Source: World Bank⁴⁸

48 documents.worldbank.org/curated/en/806971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf

6.3 Affordability of internet

Affordability is the top barrier preventing mobile ownership for both men and women across the region. The main issue is the price of handsets and data which, despite coming down, can still be prohibitively expensive for the remaining unconnected population, even for low-cost devices. As with gender, income levels and location, the digital gap can be explained by unaffordable services and Internet-enabled devices. The pricing information from **figure 7** below shows that the cost of 1 GB of prepaid mobile data in the SADC region is higher than in the best-performing countries with only two countries, Mozambique and Tanzania, being among the best-performing countries as shown in **figure 7** below:

Figure 7: Cost of Internet in SADC member States












Source: Independent Communications Authority of South Africa (ICASA) 2018⁴⁹

⁴⁹ See <https://www.icasa.org.za/uploads/files/cost-to-communicate-programme-briefing-to-the-PPCTPS.pdf>

The cost of 1GB of data in Malawi, Namibia and South Africa costs six times more than the cost of the same amount of data in the best-performing country: Egypt (USD1.24)⁵⁰. Swaziland is the worst-performing country in the region, with 1GB of data being 25 times the price of 1GB in Egypt, and over 15 times that in Mozambique. The high cost of data in the SADC region is one of the main contributors to digital inequality in the SADC region. Over 10 countries as shown in **Figure 8** below have 1GB costing over 5% of average income, which is very high

Figure: 8 Cost of data to Income⁵¹

Country ¹	100MB	500MB ¹	GB 2	GB 5	GB 1	0GB
	GNI ² /C G	NI/C ³ G	NI/C G	NI/C G	NI/C G	NI/c
 Angola	1.17%	2.35%	5.87%	11.75%	29.37%	29.37%
 Botswana	0.98%	1.56%	1.56%	2.38%	7.78%	11.06%
 Comoros	9.60%	9.60%	9.60%	14.62%	31.34%	36.56%
 D.R. Congo	22.86%	22.86%	53.33%	53.33%	108.67%	100.00%
 Lesotho	4.60%	4.60%	4.60%	7.88%	17.05%	26.28%
 Madagascar	8.57%	11.01%	21.41%	21.41%	NA	NA
 Malawi	6.70%	13.40%	18.24%	26.05%	54.71%	80.78%
 Mauritius	0.70%	0.70%	0.70%	1.00%	1.67%	3.15%
 Mozambique	1.40%	6.01%	10.01%	14.01%	23.35%	46.71%
 Namibia	1.17%	2.88%	2.88%	2.88%	14.29%	14.29%
 South Africa	0.45%	1.63%	2.30%	3.28%	6.16%	9.25%
 Tanzania	2.88%	2.88%	7.41%	7.41%	17.28%	20.16%
 Zambia	3.88%	3.88%	3.88%	7.76%	7.76%	15.52%
 Zimbabwe	3.95%	16.95%	19.78%	39.56%	39.56%	79.12%

Source: Alliance for affordable Internet (2018)⁵²

50 See <https://png.org.za/committee-meeting/25343/A>

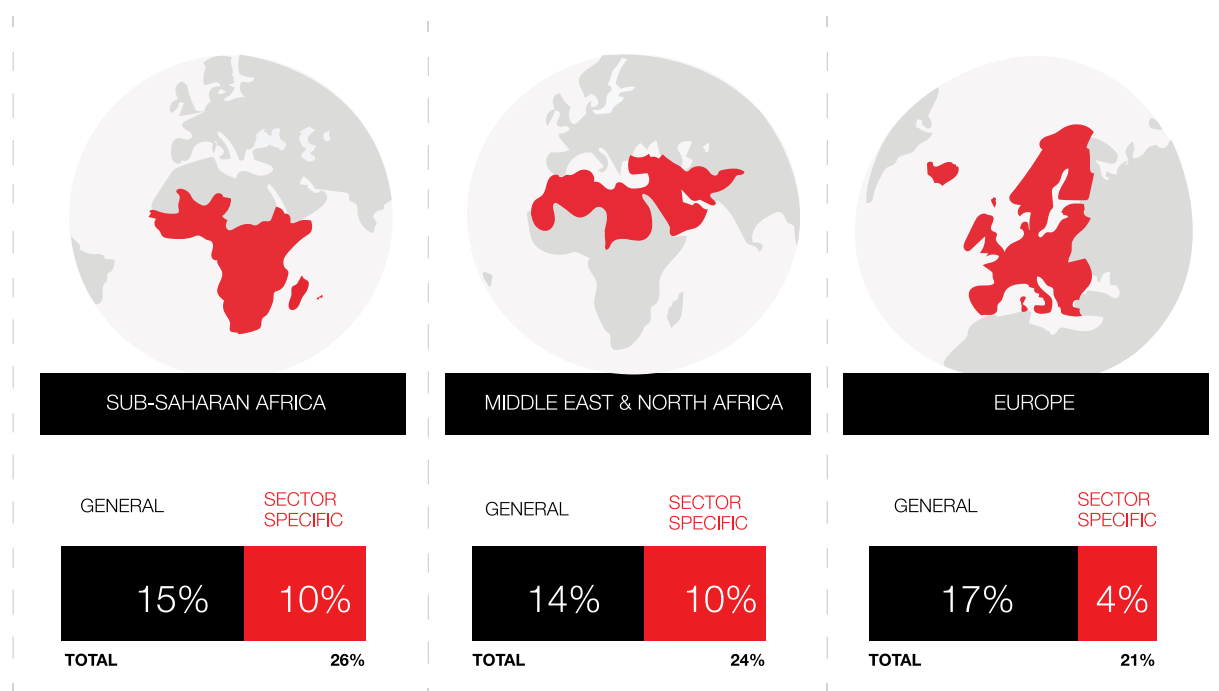
51 For Average Income See: <https://www.worlddata.info/average-income.php>

52 See https://a4ai.org/extra/mobile_broadband_pricing_gnicm-2018Q4

6.4 Taxation of social media and content

As aforementioned, mobile is the main gateway to the internet for consumers in many parts of the world today, particularly in developing countries. Despite this, governments in many of these countries are increasingly imposing as shown in Figure 9 below – in addition to general taxes – sector-specific taxes as shown in figure 10 below on consumers of mobile services and devices and on mobile operators. This poses a significant risk to the growth of the services among citizens, limiting the widely acknowledged social and economic benefits associated with mobile technology. Sector-specific taxes are not aligned with best practices in taxation, and can hinder development of the sector. Sector-specific taxes on mobile services and devices are not consistent with established principles to achieve efficient, equitable and simple taxation – as identified by international organisations such as the Introduction to Tax Policy Design & Development⁵³; Taxing Principles, IMF⁵⁴; Taxing Telecommunication ITU⁵⁵, Fundamental principles of taxation in addressing the tax challenges of the digital economy, OECD⁵⁶.

Fig 9: Comparison of taxation levels



Sources: GSMA⁵⁷

Sub-Saharan region has sector specific tax of 10% in comparison of Europe's 4%. Imposing sector-specific taxes generates five problems: Sector-specific taxes as (see figure 11, below) on mobile services and devices raise prices for consumers and costs for firms, which reduces the consumption and supply of mobile

services and devices. By reducing consumption of mobile services, sector-specific taxes constrain well acknowledged positive social and economic impacts of mobile technology. Sector-specific taxes discriminate against the mobile industry compared to other sectors, which can divert investments, and more generally have

⁵³ Introduction to Tax Policy Design & Development, Bird and Zolt, 2003

⁵⁴ Taxing Principles, IMF, 2014

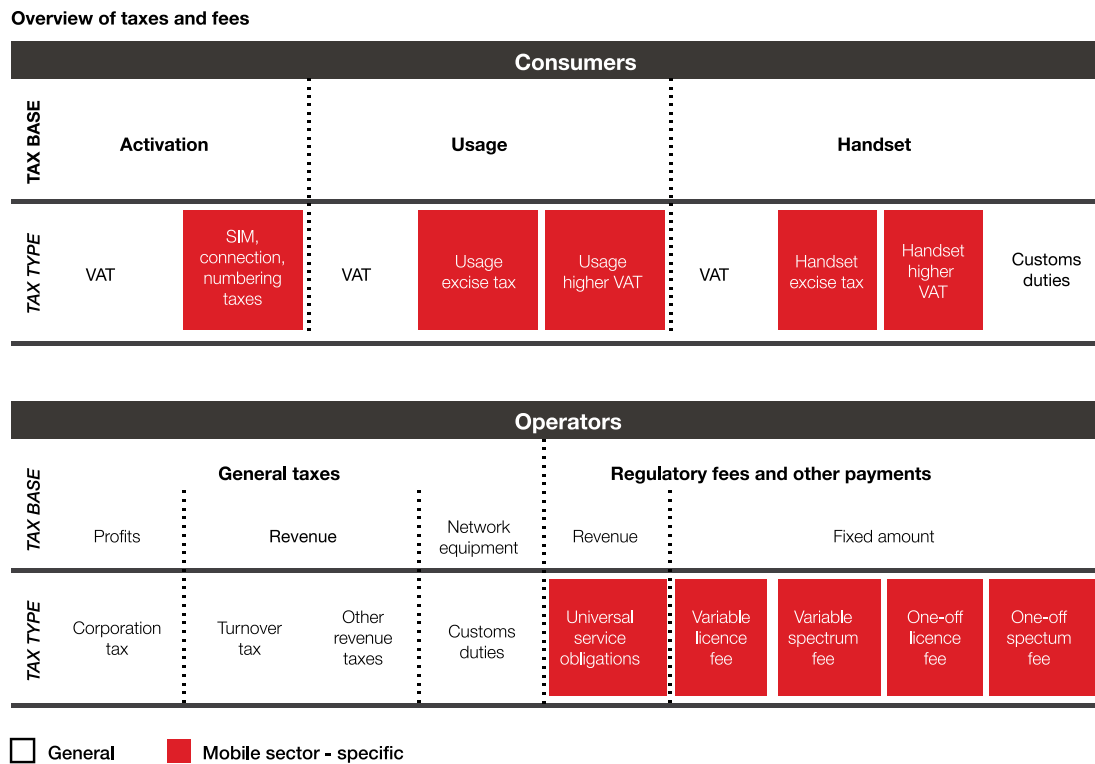
⁵⁵ Taxing Telecommunication/ICT services: an overview, ITU, 2013

⁵⁶ Fundamental principles of taxation in addressing the tax challenges of the digital economy, OECD, 2014

⁵⁷ <https://www.gsmaintelligence.com/research/?file=8f96cd1c58cd619d9f165261a5714a9&download>

a distortive impact. Sector-specific taxes can be regressive, i.e. fall disproportionately on poorest households, where they raise the price of mobile services across the population without regard for capacity to pay. Sector-specific taxation adds to the complexity and opacity of tax policy, increasing mobile operators' compliance costs and disincentivising investment – as well as meaning more costly enforcement for governments.

Figure 10: Taxation in telecommunications



Source: GSMA

6.4.1 Case Study of Tanzania – Taxation of Online Content

Tanzania's Electronic and Postal Communications (Online Content) Regulations (2018)⁵⁸, has introduced an indirect tax in the form of content fees, some of the issues covered are:

Regulations apply to online content including: (a) application services licensees; (b) bloggers; (c) internet cafes; (d) online content hosts; (e) online forums; (f) online radio or television; (g) social media; (h) subscribers and users of online content; and (i) any other related online content.

58 https://www.tora.go.tz/images/documents/regulations/SUPP_GN_NO_133_16_03_2018_EPOCA_ONLINE_CONTENT_REGULATIONS_2018.pdf

Tanzania Communications Regulatory Authority has the following powers in regulating online content services- (a) to keep register of bloggers, online forums, online radio and online television; (b) to take action against non-compliance to these Regulations, including to order removal of prohibited content; and (c) to conduct public awareness in relation to safe use of online content.

The fees are shown in figure 11 below:

Figure 11: Tanzania Online Content Services Fees

ONLINE CONTENT SERVICES FEES

\$No	Type of Licence	Application Fees	Initial Licence Fees	Annual Licence Fees	Renewal Fees	Duration of Licence
1	Online Content Services	TZS 100,000	TZS1,000,000	TZS1,000,000	TZS1,000,000	3 years
2	Simuleasting Television Licence (streaming content on the Internet)	TZS 50,000	TZS 200,000	TZS 200,000	TZS 200,000	3 years
3	Simuleasting Radio Licence streaming content on the internet	TZS 50,000	TZS 200,000	TZS 200,000	TZS 200,000	3 years

DODOMA,
13rd MARCH, 2018

HARRISON G MWAYEMBE,
Minister for Information, Culture, Arts and Sports

Exchange rate as of 23 March, 2019: 1 Tanzanian Shilling = 0.00043 United States Dollar ⁵⁹

Sources: TCRA ⁶⁰

6.4.2 Case study of Zambia – Taxation of ‘Social Media’ Calls

Zambian Cabinet on the 12th of August 2018⁶¹ approved a 30 ngwee (0.3 kwacha; \$0.03) daily tariff charged on online phone calls. Government said “about 80 per cent⁶² of Zambians are using WhatsApp, Skype and Viber to make phone calls”; “as a quick realisation by government that there is a huge revenue loss that comes with internet calls;” government claims that the move was aimed at protecting jobs in the telecommunication industry⁶³.

⁵⁹ <https://www.xe.com/currencyconverter/convert/?Amount=1&From=TZS&To=USD>

⁶⁰ https://www.tkra.go.tz/images/documents/regulations/SUPP_GN_NO_133_16_03_2018_EPOCA_ONLINE_CONTENT_REGULATIONS_2018.pdf

⁶¹ <https://www.usakatimes.com/2018/08/13/zambia-slaps-a-30-ngwee-a-day-tariff-on-internet-phone-calls/>

⁶² <https://www.theafrican.co.ke/business/Zambia-seeks-USD22-million-in-tax-on-internet-/2560-4713400-cmhq5lz/index.html>

⁶³ <https://www.usakatimes.com/2018/08/13/zambia-slaps-a-30-ngwee-a-day-tariff-on-internet-phone-calls/>

6.5 Sub-standard service delivery

SADC Protocol on Transport, Communications, and Metrology, which aims at developing a reliable, efficient, vibrant, consumer-driven telecommunications sector, is a key strategy for access to internet in the Region. One of the key impediments to access is substandard and poor service delivery by majority mobile network operators in the region, resulting in network failure, service unavailability, erratic service and unavailability of internet service. A number of the operators have been fined by local regulators as the following cases will show:

6.5.1 Zambia Case Study – Sub-Standard Standard Service Delivery

As part of protection of the rights and interests of consumers Zambia Information Communications Technology Authority (ZICTA)⁶⁴ fined mobile service providers Airtel, Zamtel and MTN for failure to meet benchmarks for service delivery. ZICTA penalized all the 3 mobile network providers 12.6 million⁶⁵ kwacha for failing to adhere to the quality of service parameters as outlined in the quality of service guidelines during the fourth quarter of 2017 and first quarter of 2018 respectively. The fines are more than double what the Telecommunications regulator fined the trio of 3.1 million kwacha last operating year⁶⁶. The failure to meet some of the set parameters on quality of service which include call set up success rate, mean opinion's call, successful sms rate, sms delivery time and http success log ins, http success rate as well as http down rate 2g and 3g is a key barrier to digital rights in the country.

6.5.2 Zimbabwe Case Study - Sub-Standard Standard Service Delivery

The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)⁶⁷ fined Zimbabwe's 3 mobile network operators \$93 353.24⁶⁸ for failing to meet quality standards hence poor service delivery.

In 2010 Econet Wireless, Zimbabwe's largest telecommunications provider, blamed power cuts⁶⁹ " In March 2019, Econet Wireless said⁷⁰ "The instability on our key network systems resulted in intermittent failure by customers to make calls, send SMSes (messages), browse mobile data or to use USSD for services such as EcoCash and to purchase product bundles across the network". According to Director General of POTRAZ, the outages were due to foreign currency challenges whereby Econet is failing to pay service providers to fix their network⁷¹.

6.5.3 Tanzania Case study – Sub-Standard Services

The mobile phone operators Airtel, Vodacom, Tigo, Zantel and Smart were sanctioned⁷² by the Tanzania Communications Regulatory Authority (TCRA) ⁷³for poor quality of service. The five telecom companies will have to pay for this purpose, a total of 112.5 million Tanzanian shillings (51,461 dollars).

According TCRA quality of services tests results⁷⁴, all operators did not met some quality of services parameters⁷⁵ contrary to regulation 9, 10 and 11 of the Electronic and Postal Communication (Quality of Service) regulation of 2011⁷⁶.

6.6 Other barriers

64 <https://www.zicta.zm/>

65 <https://zambiareports.com/2018/06/27/zicta-fines-3-mobile-service-providers-k12-6-million-poor-service-delivery/>

66 <https://www.usakatimes.com/2013/12/27/zicta-hands-poor-service-case-mobile-operators-dpp-prosecution/>

67 <http://www.potraz.gov.zw/>

68 <https://www.techzim.co.zw/2018/06/local-mobile-network-operators-paid-over-90-000-in-fines-last-year-due-to-poor-service/>

69 <https://www.newsdaily.co.zw/2010/06/30/econet-speaks-on-network-problems/>

70 <https://news.pindula.co.zw/2019/03/06/econet-explains-cause-for-network-problems/>

71 <https://news.pindula.co.zw/2019/03/09/network-disruptions-to-continue-due-to-forex-shortages/>

72 <http://extensia-ltd.com/tanzania-airtel-vodacom-tigo-zantel-smart-punished-poor-quality-services/>

73 See <https://www.tcra.go.tz/>

74 <https://technology.ihc.com/594344/tanzanias-mobile-operators-fined-again>

75 <https://allafrica.com/stories/201704140062.html>

76 See <https://www.tcra.go.tz/index.php/regulations>



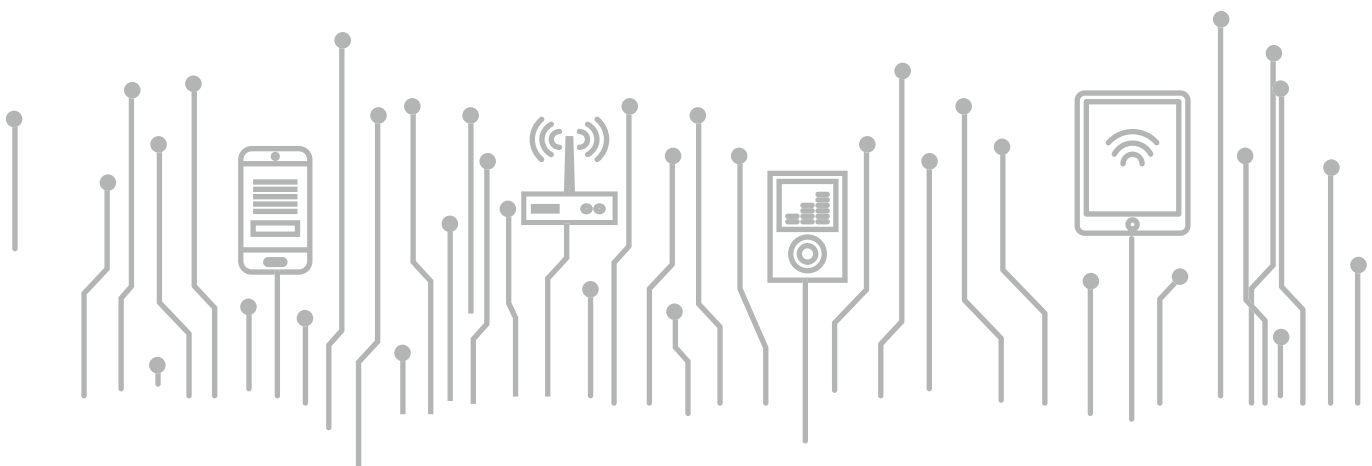
Literacy and digital skills are barriers to mobile ownership across the countries surveyed. Both factors are important considerations in most markets. The remaining unconnected population is disproportionately illiterate or has low levels of literacy, so ensuring that handsets are usable and accessible for less literate users is important.

Gender digital divide: A comparatively stronger patriarchal background in the Southern Africa region is one of the key factors that contributes to the gender digital divide in the region; Women are often less confident and sometimes denied access or finances to independently acquiring the digital skills required to use a mobile phone, and are more concerned with the consequences of making mistakes and gender segregation.

Safety and security concerns are the third most important barrier overall. They are also important issues, it a factor preventing potential user from owning a mobile phone.

Relevance is an important barrier to mobile ownership across southern Africa. The perception that mobile would not be relevant or helpful in one's life can prevent non-owners from seeing the value for money in buying a mobile, even if they can afford one.

Accessibility-related barriers, such as mobile coverage, access to phone charging and family approval, are too disparate to accurately group into one category. While accessibility-related barriers are rarely identified as the top barriers to mobile ownership for either men or women in developed world, they are emerging as important factors in rural Southern Africa markets.



“

Despite the fact that the Internet plays a role of catalyst for economic activity, there have been several network shutdowns by public authorities in recent times. Restricting connectivity or shutting down the network has the potential to reverse the impacts that the Internet ecosystem has on the wider economy

Internet Shut down(s)⁷⁷

Despite the fact that the Internet plays a role of catalyst for economic activity, there have been several network shutdowns by public authorities in recent times. Restricting connectivity or shutting down the network has the potential to reverse the impacts that the Internet ecosystem has on the wider economy. Of the twenty two (22) African countries where internet disruptions were ordered in the last five years, 77% are authoritarian⁷⁸ and the rest are hybrid or semi-authoritarian regimes⁷⁹, two (2)⁸⁰ of these countries are in Southern Africa. These disruptions not only directly infringe people's fundamental right to receive and impart information or the right to express themselves but it also prevents them from associating and assembling with like-minded individuals or groups online and offline. The United Nations Human Rights Council has spoken out strongly against internet shutdowns, the Council⁸¹ passed by consensus a resolution on freedom of expression and the internet with operative language on internet shutdowns. The resolution⁸² "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures."

The Council intended this clear declaration to combat the blocking and throttling of networks, applications, and services that facilitate the freedoms of expression, opinion, and access to information online. In 2015, various experts⁸³ issued an historic statement declaring that internet "kill switches" can never be justified under international human rights law, even in times of conflict. General Comment 34 of the UN Human Rights Committee, the official interpreter of the International Covenant on Civil and Political Rights, emphasizes that restrictions on speech online must be strictly necessary and proportionate to achieve a legitimate purpose. Shutdowns disproportionately affect all users, and unnecessarily restrict access to information and emergency services communications during crucial moments.

In Southern Africa the trend of internet shut down is raising on a deplorable trend with regards to digital rights. The first two months of 2019 have seen total shutdowns in Zimbabwe and Democratic Republic of Congo.

7.1 Democratic Republic of Congo Case Study – Internet Shutdown

In the DRC, the Government blocked the internet and social media on 31 December 2018⁸⁴, following the conduct of polls on 30 December. These services were not restored fully until 20 January 2019⁸⁵ when the Constitutional Court confirmed the win of Felix Tshisekedi as president elect.

Special Rapporteur⁸⁶ on the promotion and protection of the right to freedom of opinion and expression: Statement of Democratic Republic of Congo statement⁸⁷ (Verbatim) – "GENEVA (7 January 2019) - A United Nations expert has called on the Government of the Democratic Republic of Congo to restore internet services in the country. General elections were held on 30 December and the next day all primary telecommunications were shut down ahead of the announcement of the results. "A general network shutdown is in clear violation of international law and cannot be justified by any means," said David Kaye, the UN Special Rapporteur on freedom of expression.

"Access to information is crucial for the credibility of the ongoing electoral process. Shutdowns are damaging not only for people's access to information, but also for their access to basic services," the expert said. A senior government official said that internet and SMS services were cut to preserve public order after "fictitious results" began circulating on social media, and that the disconnections would remain until the publication of results on 6 January. Reports indicate that the shutdown is hindering electoral observers and witnesses in relaying information from rural polling stations to the local centres for compiling results. It is also hampering the UN mission's (MONUSCO) ability

⁷⁷ For definitions and scope see: <https://www.internetsociety.org/wp-content/uploads/2017/11/ISOC-PolicyBrief-Shutdowns-20171109.pdf>

⁷⁸ See <https://www.eiu.com/topic/democracy-index>

⁷⁹ See https://cipesa.org/?wpfb_d=283

⁸⁰ Zimbabwe and Democratic Republic of Congo

⁸¹ In its 32nd Session, in July 2016 See: <https://undocs.org/A/HRC/RES/32/13>

⁸² A/HRC/RES/32/13 : ibid

⁸³ from the United Nations (UN) Organization for Security and Co-operation in Europe (OSCE), Organization of American States (OAS), and the African Commission on Human and Peoples' Rights (ACHPR)

⁸⁴ See <http://www.achpr.org/press/2019/01/d440/>

⁸⁵ See <https://www.article19.org/resources/africa-increasing-internet-shutdowns-and-media-bans-limiting-access-to-information/>

⁸⁶ The Special Rapporteurs and Independent Experts are part of the Special Procedures of the Human Rights Council. Special Procedures, the largest body of independent experts in the UN Human Rights system, is the general name of the Council's independent fact-finding and monitoring mechanisms that address either specific country situations or thematic issues in all parts of the world. Special Procedures' experts work on a voluntary basis; they are not UN staff and do not receive a salary for their work. They are independent from any government or organization and serve in their individual capacity.

⁸⁷ <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24057&LangID=E>

to communicate with its partners in the field, including with protection mechanisms. “I urge the authorities to restore internet services as a matter of urgency and to ensure the integrity of a fundamental democratic exercise such as this one,” the Special Rapporteur said. In 2016, the Human Rights Council passed a resolution which unequivocally condemned 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. This followed the 2015 Joint Declaration of UN and regional experts in the field of freedom of expression, which stated that network shutdowns or internet “kill switches” are measures which can “never be justified under human rights law”. The UN Special Rapporteur will continue to closely monitor developments in DRC and is at the disposal of the authorities to provide assistance as required. //END”

7.2 Zimbabwe Case Study – Internet Shutdown

In Zimbabwe, on 15 January 2019⁸⁸, following a directive by the State Security Minister, internet service providers shut down the internet. While the ban was lifted on Wednesday 16 January 2019⁸⁹, leaving only a ban on social media platforms, another full internet shutdown was ordered on Thursday 17 January 2019⁹⁰, effectively leaving a majority of Zimbabweans without access to the internet. Commendably Zimbabwe Lawyers for Human Rights and MISA Zimbabwe in their application⁹¹ challenged the directive in the High court leading to the High Court judge Justice Owen Tagu ruling⁹² on 21 January 2019 that the Minister of State in the President’s Office Responsible for National Security does not have the authority to issue any directives in terms of the Interception of Communications Act, leading to the setting aside of the shutdown directive.

| 8.0 |

Just in Time temporary service disconnections

Related to internet shutdowns is the disconnection of services in a particular area to facilitate by a Government. The trend is on the increase in the region, as seen in the two examples below:

8.1 Namibia and Swaziland Case Studies – Just in time disconnections

Namibia and Swaziland applied⁹³ ‘just in time’ temporary disconnections or event-based denial of selected content or services. These techniques⁹⁴ can be difficult⁹⁵ to verify, as they can be made to look like technical errors applied in ways that assure plausible, for example during important anniversaries. In the case of Namibia⁹⁶, internet has often been

temporarily disconnected in regions where the president is visiting. In Swaziland’s case⁹⁷, this has occurred during visits by foreign dignitaries and during the high court hearings of important human rights cases which potentially exposed the country’s bad human rights record.

88 See <https://www.techzim.co.zw/2019/01/law-society-of-south-africa-an-internet-shutdown-does-not-restore-order-it-does-the-contrary/>

89 See <https://www.accessnow.org/zimbabwe-orders-a-three-day-country-wide-internet-shutdown/>

90 See <https://www.zimbabwewatchdog.com/news/statement-on-the-internet-shutdown-in-zimbabwe/>

91 See <http://www.ventasim.net/node/3397>

92 See <http://zimbabwe.misa.org/2019/01/21/high-court-sets-aside-internet-shut-down-directives/>

93 See <https://globalsouthinitiative.com/wp-content/uploads/2018/10/Sub-Saharan-Africa-Internet-Freedom-Landscape-Final-version-edited.pdf>

94 Ronald Deibert and Rafal Rohozinski, “Control and Subversion in Russian Cyberspace,” in Ronald Deibert et al., eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*

95 *ibid*

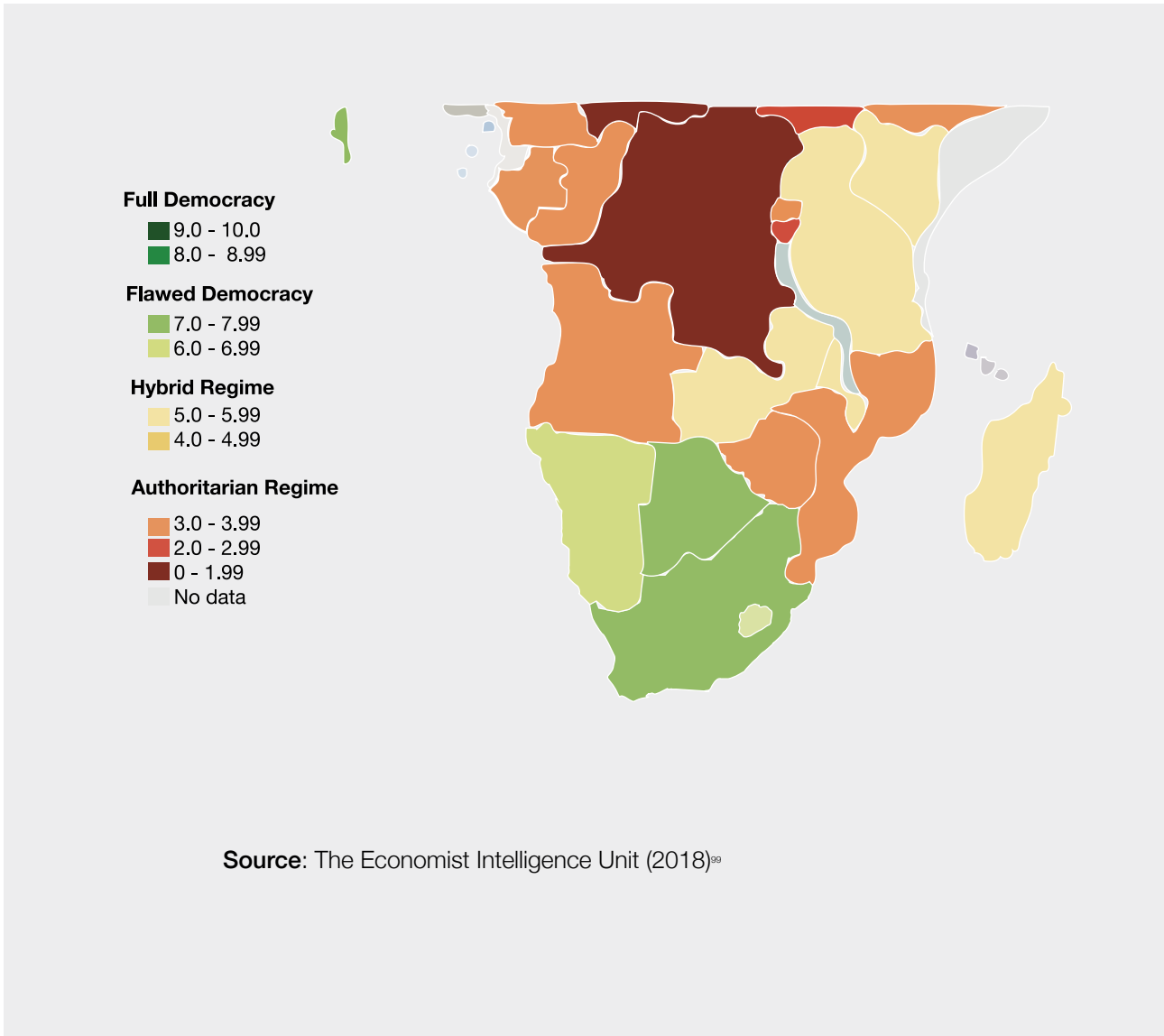
96 <https://globalsouthinitiative.com/wp-content/uploads/2018/10/Sub-Saharan-Africa-Internet-Freedom-Landscape-Final-version-edited.pdf>

97 *ibid*

Potential of more shut downs in Southern Africa

The state of democracy in Sub-Saharan Africa (SSA) and Southern Africa in particular has remained poor over the years⁹⁸. A concentration of authoritarian regimes and upcoming election in 2019 may pose a risk for more shutdowns in the region in 2019 due to the state of democracy and upcoming elections as shown in figure 12 and 13 respectively:

Figure 12: Southern Africa Democracy Status

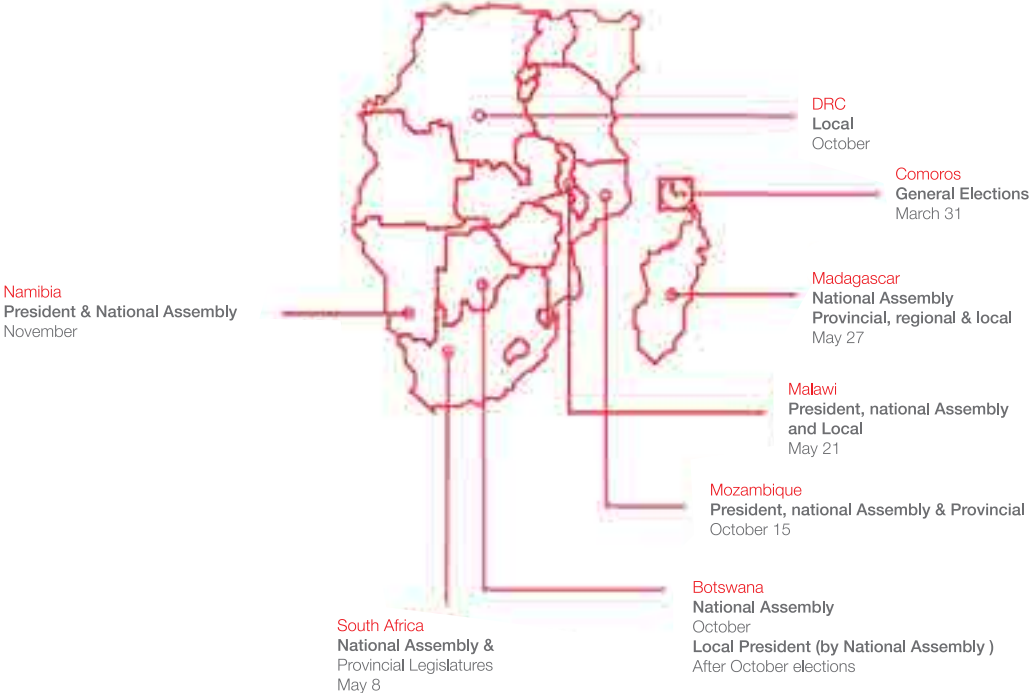


⁹⁸ See <http://www.eiu.com/topic/democracy-index>

⁹⁹ See <http://www.eiu.com/topic/democracy-index>

Southern Africa countries are performing relatively poorly as shown in terms of democracy as shown in figure 12 above. Recent research¹⁰⁰ has shown that the more authoritarian a country is the more the abuse of digital rights and the higher the chances for internet shut downs. Upcoming elections have a potential to increase number of internet shutdowns, figure 13 shows the countries in the region that are having election in 2019:

Figure 13: 2019 Election in Southern Africa



Source: Own Map: Data from Countries Election Bodies Websites

Close to half of SADC member states (Eight (8) countries) are going to hold elections in 2019. Research^{101 102 103 104} has shown that there is a correlation between elections and internet shut downs in authoritarian states. Elections are generally regarded as procedural instrument by which political authority and legitimation is periodically and formally granted to elected representative(s)¹⁰⁵. Yet holding elections does not mean that a country is democratic. In consequence, authoritarian rulers often, but

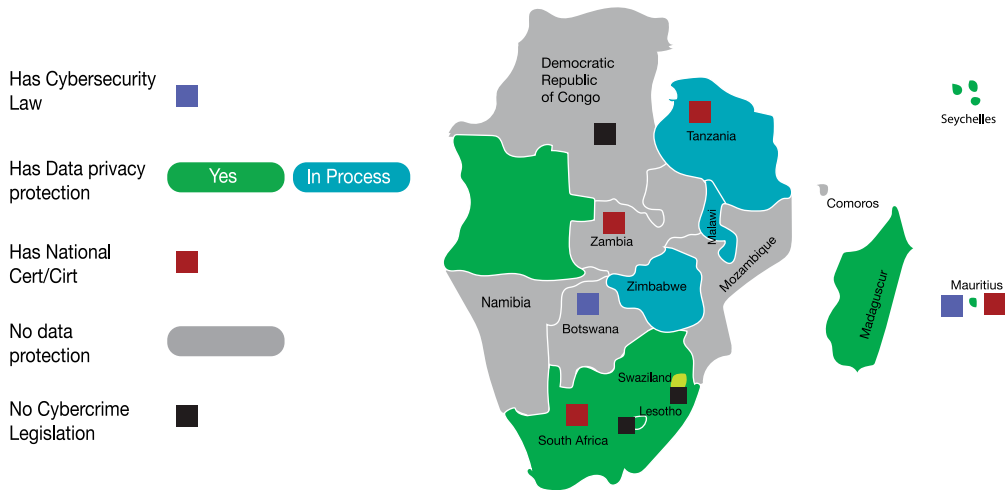
not always, manipulate elections to ensure their prolonged rule. They seek to incarcerate key opposition leaders and their supporters, ban their parties, repress the media and violate digital rights¹⁰⁶. In short, election violence and fraud often trigger protest against the handling or outcome of the election by opposition forces; such protests can, in turn, provoke the use of more state violence in an effort to dissolve public dissent and stay in power, a key tool to quell the protest is internet shutdown.^{107, 108}

100 https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf
 101 https://www.chctr.org/Documents/Issues/Expression/Telecommunications/AccessPart_I.docx
 102 See <https://ipoc.org/index.php/ipoc/article/download/8546/2464>
 103 See also <http://hartworkshop2018.com/Ewan%20Sutherland.pdf>
 104 See also <https://africaupclose.wilsoncenter.org/internet-shutdowns-during-elections/>
 105 <https://ipoc.org/index.php/ipoc/article/download/8546/2464>
 106 See https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf
 107 See <https://ipoc.org/index.php/ipoc/article/download/8545/2465>
 108 See also : https://www.accessnow.org/cms/assets/uploads/2017/11/Somaliand_RE-Internet-Shutdown.pdf

Privacy, Data protection and Cybersecurity¹⁰⁹

The current posture regarding cybersecurity, crime and data protection in SADC region is shown in figure 14 below:

Figure 14: Status of privacy, data protection and cybersecurity of SADC member states



Sources: Own Map, illustrated from data from ITU^{110, 111}

The above status does not adequately protect and promote digital rights in the SADC region. The posture is significantly limited in terms of institutional, technical and legal measures and capacity to effectively protect data, ensure cyber-security, mitigate cyber-crimes and protect citizen’s privacy. There is an urgent need of a region and statewide political will to cover gaps as frameworks are already there.

This must include the establishment of a national and regional CIRT (Computer Incident Response Team), enactment of human rights centered cyber-security and data protection legislation(s) which provides the capabilities to identify, defend, respond and manage cyber threats and enhance cyberspace security in the states and region.

¹⁰⁹ Everyone has the right to benefit from security, stability and resilience of the Internet. As a universal global public resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. Different stakeholders should continue to cooperate in order to ensure effectiveness in addressing risks and threats to security and stability of the Internet. Unlawful surveillance, monitoring and interception of users’ online communications by state or non-state actors fundamentally undermine the security and trustworthiness of the Internet.

¹¹⁰ https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci-01-2017-pdf-e.pdf

¹¹¹ <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2016.aspx>

Constitutional Provisions of Digital Rights

All the states in the region have some provisions on digital rights. While it is a significant success that all the constitutions in the region have to an extent have explicit or implied digital rights provisions, it is critical that all the governments and stakeholders move ensure, promote the enjoyment of these rights, enact human rights centered operational and administrative legislation to operationalize these constitutional rights and above all, ensure and protect constitutionalism¹¹². Some examples of digital rights provisions in the constitutions:

11.1 Case of Zimbabwe¹¹³ -Constitutional Provision

Every person has the right to privacy, which includes the right not to have-- (a) their home, premises or property entered without their permission; (b) their person, home, premises or property searched; (c) their possessions seized; (d) the privacy of their communications infringed; or (e) their health condition disclosed.

11.2 Case of Tanzania¹¹⁴ - Constitutional Provision

Every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications. (2) For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his person, his property and residence may be encroached upon without prejudice to the provisions of this Article.

11.3 Case of Democratic Republic of Congo¹¹⁵ - Constitutional Provision

All persons have the right to the respect of their private life and to the secrecy of their correspondence, of telecommunications and of any other form of communication. This right may only be infringed in the cases specified by the law

11.4 Case of Malawi¹¹⁶ - Constitutional Provision

Every person shall have the right to personal privacy, which shall include the right not to be subject to - (a) searches of his or her person, home or property; (b) the seizure of private possessions; or (c) interference with private communications, including mail and all forms of telecommunications.

112 The concepts of constitution and constitutionalism refer to the legal framework of a country. While constitution is often defined as the "supreme law of a country," constitutionalism is a system of governance under which the power of the government is limited by the rule of law. Read more: Difference Between Constitution and Constitutionalism: <http://www.differencebetween.net/miscellaneous/politics/difference-between-constitution-and-constitutionalism/#kzz5j1HQTVv>

113 Constitution of Zimbabwe,

https://www.constituteproject.org/constitution/Zimbabwe_2013.pdf

114 Constitution of Tanzania,

<http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan040857.pdf>

115 Constitution of the DRC 2005 (rev. 2011) https://www.constituteproject.org/constitution/Democratic_Republic_of_the_Congo_2011?lang=en

116 Constitution of Malawi,

<http://www.wipo.int/edocs/lexdocs/laws/en/mw/mw002en.pdf>

Impact of HIPSSA¹¹⁷ SADC Model Law¹¹⁸ on Digital Rights

From a brief non analytic look at the SADC Model law(s) they appear to follow the Commonwealth Model law (based on the Budapest Convention) and thus, appear to coincide in structure with many of the provisions of the Convention. However, on a closer examination it becomes clear that the seemingly deliberate ‘tampering’ with language has diluted the efficacy and limited the application of the offences and powers with edits that make the provisions technically and legally unsound. The changes made to the model law in an effort to make it better or seem different from the common wealth model law, significantly reduced conformance and consistence with Human rights mainly UNDHR and Budapest Convention. They deviate from the Convention both in terms of the definitions, ingredients of offences established as best practice as well as redefining the scope of cybercrime to include criminalizing defamation of religion, blasphemy, insults, and any form of pornography, SPAM and a unique concept of “Illegal Remaining” without any carve outs, exceptions or safeguards.

Key issues that need review and changes for countries domesticating the model law:

1. Improve Article 1 Definitions
e.g. Definitions of access and authorization
2. Impact on business/ rights holders
3. Compatibility of definitions for International Cooperation
4. Overall legal and technical adequacy –
5. Section 1- Substantive law : Absence of offences, inappropriate, technically incorrect or unsafe offences
6. Ensure Consistency with Human Rights (Contains regressive offences)
7. Compatibility of offences for International Cooperation

¹¹⁷ Harmonisation of the ICT Policies in Sub-Saharan Africa

¹¹⁸ At the direction of the Assembly of Heads of State, the African Union has been working to support the development of various ICT and internet enabling policy and regulatory frameworks in member states. The ITU, with financial support from the European Union, has been helping to shape national cyber security laws with human capacity building in sub-Saharan Africa.

“

However, on a closer examination it becomes clear that the seemingly deliberate ‘tampering’ with language has diluted the efficacy and limited the application of the offences and powers with edits that make the provisions technically and legally unsound.

Section 2

Procedural law

Article 15

Conditions and safeguards ; Impact on Private Sector Non-compliant to UNDHR/ ICCPR ; Proportionality; Adequacy of grounds justifying application of powers

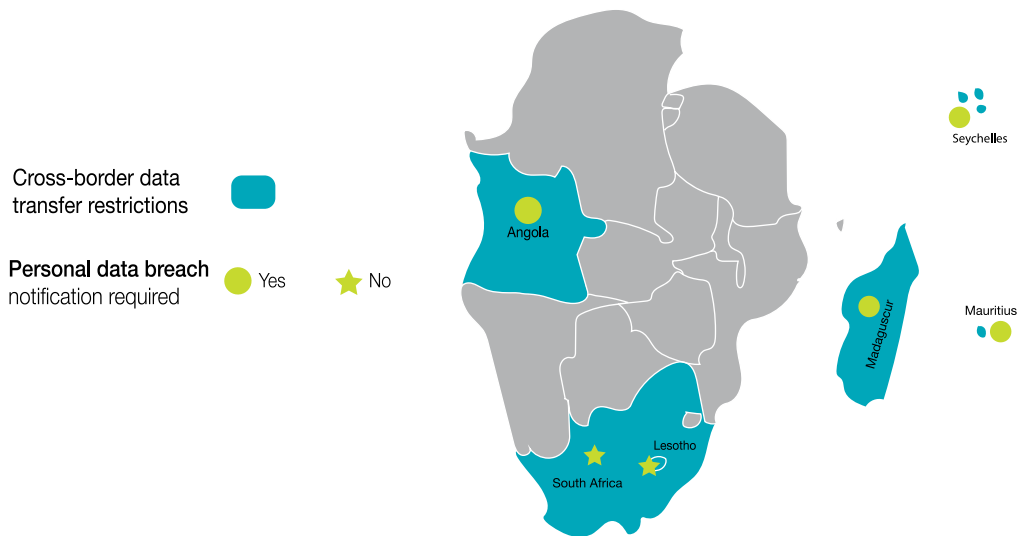
The Model Law should attempt to bridge the best practice principles of substantive offences, powers, and mutual legal assistance, such as those enunciated by the Convention and modeled by the Commonwealth model law, which may work as a sound technical and legal starting point with specific examples of language that elaborate the various elements that need to be included in a law when implementing these principles.



Data protection

All the Southern Africa governments are collecting and processing data yet the majority lack comprehensive and harmonised legal framework for data protection. The common areas which by law require mandatory collection of personal information by government, and which are regulated by law, include registration of SIM cards, voters, births, marriages, deaths, driving licenses, national identity cards, passports, tax payers, health insurance, social security, and national census. Under the circumstances, the lack of sufficient judicial or independent oversight puts the protection of privacy and personal data in danger, as there is no sure way of assessing compliance with legal requirements. The status of data protection is shown in **Figure 15**.

Figure 15: Status of data protection in Southern Africa region.



Source: Deloitte¹¹⁹

13.1 The AU Data Protection Convention

Before the adoption of the AU Convention, some efforts on data protection had been made by the AU. The first of such efforts was in 2011 with the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, got a name change¹²⁰ in 2013 after review, then a second draft was done.¹²¹ These drafts were heavily criticised by the private sector, civil society organisations and privacy advocates because they had little involvement in the process.¹²²

The AU Convention has two broad objectives, which are: Firstly, it commits state parties to ‘establishing a legal framework aimed at strengthening fundamental

rights and public freedoms, particularly the protection of physical data and to punish any violation of privacy without prejudice to the principle of free flow of data.’ Secondly, the framework so established by member states shall ensure that any form of data processing respects fundamental freedoms and human rights while recognising the right of the state, local communities and the purposes for which businesses were established. The objectives of the Convention show an unequivocal human rights protection agenda. Furthermore, the Convention recognises the interests of other entities in individuals’ information like states, local communities and the purpose for which businesses are established.

119 https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

120 The reason for the slight change in name is still unclear. However, it is submitted that the present Convention is largely similar to the previous drafts. The Convention has a broad scope to cover three important areas of cyber law viz: electronic transactions, data protection and cybersecurity and cybercrime. This paper focuses on only the data protection provisions of the Convention.

121 See <http://au.int/en/cyberlegislation> (accessed 10 March 2019)

122 See <https://www.accessnow.org/africa-moves-towards-a-common-cyber-security-legal-framework>

Privacy and Personal Data Protection¹²³ Cases of Concern

With proliferation of ICT, digital rights violations are now becoming prevalent in Southern Africa, especially in areas such national identity cards schemes, election registration, SIM card registration exercise and surveillance technologies. These will be briefly explained below:

14.1 SIM card registration

An avenue for the harvesting of personal information which is increasingly becoming prevalent in Africa is the subscriber identity module (SIM) card registration schemes. All Southern Africa countries have mandatory requirement for SIM card registration. This has serious data protection implications for the security of accumulated personal information as the information can be abused by states if there is no subsequent provision(s) on data protection. With sensitive personal information in the hands of the state, mobile surveillance is made easy with negative consequences for human rights.

14.2 Surveillance

Surveillance technologies are now a commonplace in the region. Surveillance, in this context, is a systematic means of personal information collection, especially by governments or private entities. States now have laws mandating telecommunication providers to integrate surveillance systems capable of interception of communications. Some case of legislated surveillance:

14.2.1 Case of South Africa - Surveillance

South Africa's Regulation of Interception of Communications and Provision of Communication-related Information Act (2002)¹²⁴ require service providers to incorporate surveillance machinery before they can offer services to the public.

The act legislates the following among others:

1. The act provides for interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information;
2. Authorises the interception of communications and the provision of communication-related information under certain circumstances;
3. Telecommunication service providers and decryption key holders in the execution of such directions and entry warrants;

¹²³ Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication.

¹²⁴ See https://www.gov.za/sites/default/files/gcis_document/201409/a70-02.pdf

4. Prohibit the provision of telecommunication services which do not have the capability to be intercepted;
5. Provides for the establishment of interception centres,
6. prohibit the manufacturing, assembling, possessing, selling, purchasing or advertising of certain equipment;
7. Associated legislation for interception in South Africa¹²⁵
8. General Intelligence Laws Amendment Act 11 of 2013 from 29 Jul 2013
9. Regulation of Interception of Communications and Provision of Communication-related Information Act 48 of 2008
10. Electronic Communications Act 36 of 2005 from 19 Jul 2006
11. Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004 from 11 Feb 2005
12. Prevention and Combating of Corrupt Activities Act 12 of 2004 from 28 Apr 2004
13. Criminal Procedure Act 51 of 1977 from 30 September 2005
14. Drugs and Drug Trafficking Act 140 of 1992 from 30 September 2005
15. Intelligence Services Oversight Act

14.2.2 Case of Tanzania – Surveillance

Tanzania’s Electronic and Postal Communications (Online Content) Regulations, 2018¹²⁶, legislated based on the Electronic and Postal communications act, (2010)¹²⁷

Section 9 (c) of the 2018 regulation states ‘ to put in place mechanism to filter access to prohibited content; (d) to install surveillance camera to record and archive activities inside the cafe. (e) To keep a proper service user register and ensure every person using internet service is registered upon showing a recognized identity card. (2) The images recorded by surveillance camera and the register of users recorded pursuant to sub regulation 1 shall be kept for a period of twelve months.’

While section 14.-(1) ‘states Any person who wishes to provide online content services shall fill in an application form as prescribed in the First Schedule and pay fees as set out in the Second Schedule to these Regulations.’

¹²⁵ See <https://www.gov.za/documents/regulation-interception-communications-an>

¹²⁶

¹²⁷ <https://www.tkra.go.tz/images/documents/policies/epoca.pdf>

14.2.3 Case of Zimbabwe - Surveillance

Interception of Communications Act [Chapter 11:20] (2007)¹²⁸

Provide for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Zimbabwe; to provide for the establishment of a monitoring centre;

The legislation ensures that, a service provider

1. Postal or telecommunications systems are technically capable of supporting lawful interceptions at all times
2. Installs hardware and software facilities and devices to enable interception of communications at all times or when so required, as the case may be;
3. Services are capable of rendering real time and full time monitoring facilities for the interception of communications;
4. All call-related information is provided in real-time or as soon as possible upon call termination;
5. Provides one or more interfaces from which the intercepted communication shall be transmitted to the monitoring centre;
6. Intercepted communications are transmitted to the monitoring centre via fixed or switched connections, as may be specified by the agency;
7. Provides access to all interception subjects operating temporarily or permanently within their communications systems, and, where the interception subject may be using features to divert calls to other service providers or terminal equipment, access to such other providers or equipment;
8. Provides, where necessary, the capacity to implement a number of simultaneous interceptions in order—
9. Allow monitoring by more than one authorised person;

14.3 Dataveillance

The concept of “Dataveillance” brings about a critical shift and advance form of surveillance, it describes practices of sorting and aggregating vast datasets to track and regulate populations: “Dataveillance in the present moment is not simply descriptive (monitoring) but also predictive (conjecture) and prescriptive (enactment).”¹²⁹ It arguably differs from targeted surveillance: “Whereas surveillance presumes monitoring for specific purposes, Dataveillance entails the continuous tracking of (meta) data for unstated preset purposes.”¹³⁰

¹²⁸ See <http://www.veritasim.net/node/252>

¹²⁹ Riley, R. (2013). Dataveillance and Countervallance. In L. Giteiman (Ed.), *Raw Data is an Oxymoron*. Cambridge, MA: The MIT Press

¹³⁰ van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197-208.

Big data¹³¹, metadata¹³² and the technologies used to collect, store and analyse them are by no means neutral, but come with their own exclusions and biases. Big data is generated in many places – social media, global positioning system (GPS) data, radio frequency identification (RFID) data, the internet of things, health data, and financial data or phone records are just a few examples of data sources. Some of these data are knowingly created, for example by updating a status, posting an image or writing a tweet. Others are the side product of using services and their features, for example swiping a card or using/carrying a phone.

Targeted surveillance thus requires a suspect to monitor for a purpose, while Dataveillance generalises suspicion and algorithmically produces suspects, thus turning the assumption of innocence until proven guilty on its head. Most pertinently to a discussion of surveillance in the region are the following:

1. New surveillance often lacks consent, with higher proportions of involuntary production/collection of data.
2. The location of data and its collectors/analysts is often remote and less visible.
3. After collection the data is stored remotely and migrated often.
4. The temporality of new surveillance is continuous, omnipresent, and covers past, present and future occurrences of data; it is also acontextual.
5. Whole populations rather than individuals are surveilled. An understanding that data never emerge in isolation, are always contingent on context, technologies, humans and their algorithms that collect, sort, and analyse them, as well as on the power relations that all of the above are¹³³
6. Mass or indiscriminate surveillance of individuals or the monitoring of their communications, constitutes a disproportionate interference, and thus a violation, of the right to privacy, freedom of expression and other human rights. Mass surveillance shall be prohibited by law.
7. The collection, interception and retention of communications data amounts to an interference with the right to privacy and freedom of expression whether or not the data is subsequently examined or used.

131 See https://www.sas.com/en_us/insights/big-data/what-is-big-data.html

132 See <https://www.opendatasoft.com/2016/08/25/what-is-metadata-and-why-is-it-important-data/>

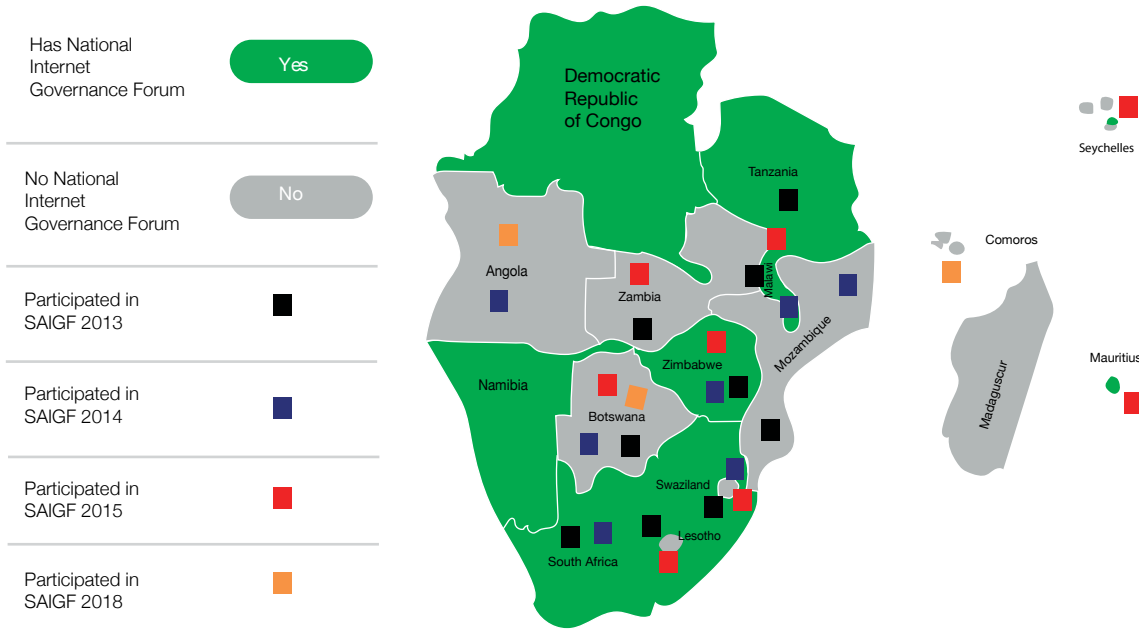
133 Manovich, L. (2011). Trending: The Promises and the Challenges of Big Social Data. In M. K. Gold (Ed.), *Debates in the Digital Humanities* (pp. 1–17). Minneapolis: University of Minnesota Press.

Internet Governance¹³⁴

The search for an Internet governance model began in 2003 at the World Summit on the Information Society (WSIS) in Geneva¹³⁵. It continued with the work of the Working Group on Internet Governance, which submitted its report in 2005¹³⁶. Finally, during the second phase of the WSIS in Tunis, that same year, it was decided to create the Internet Governance Forum (IGF). The IGF is a multi-stakeholder forum (this concept goes beyond the notion of multi-sectorial, as it

implies more commitments of the parties, the absence of barriers to access to discussions and equal participation) that provides a space for dialogue between different stakeholders on the Internet's public policy issues. That also led to the launching of the African Internet Governance Forum and The Southern Africa Internet Governance forum in 2011¹³⁷. The status of internet governance in the region is shown in figure 16 below:

Figure 16: Status of internet governance in Southern Africa



Source: Own map from data taken SAIGF reports (2013 -2018)

¹³⁴ Everyone has the right to participate in the governance of the Internet. The Internet should be governed in such a way as to uphold and expand human rights to the fullest extent possible. The Internet governance framework must be open, inclusive, accountable, transparent and collaborative.

¹³⁵ See <https://www.itu.int/net/wsis/>

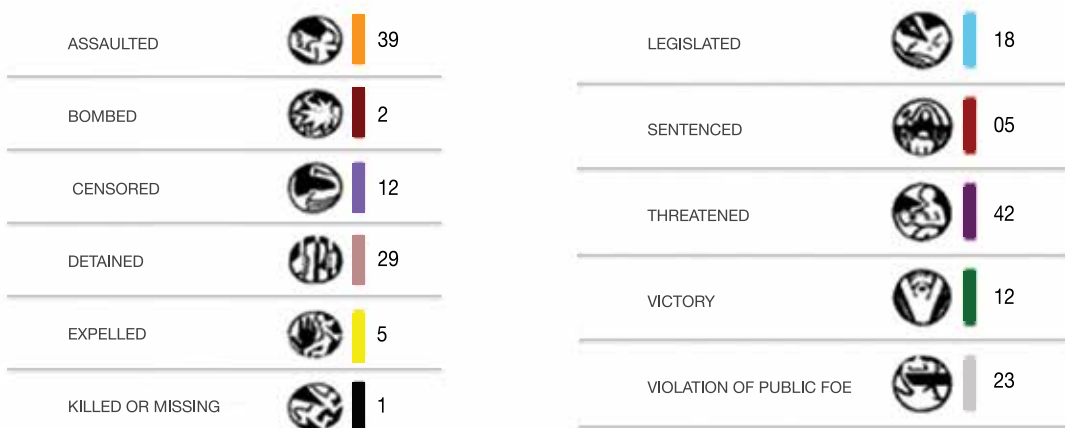
¹³⁶ Ibid

¹³⁷ See https://au.int/web/sites/default/files/documents/30938-doc-african_internet_governance_forum_rev1_0.pdf

Attacks on Journalist

Journalists, media workers and other communicators who contribute to shaping public debate and public opinion on the Internet should be recognised as actors who enable the formation of opinions, ideas, decision-making and democracy. Attacks on all who engage in journalistic activities as a result of their work constitute attacks on the right to freedom of expression.

Figure 17: Attacks on journalist¹³⁸



Source: MISA¹³⁹

Assaulting and threatening of journalist are the top threats to freedom of expression¹⁴⁰. There is need of protecting Journalist and ensure there rights are given and enjoyed as way to protect digital rights.

¹³⁸ See <http://misa.org/>

¹³⁹ *ibid*

¹⁴⁰ *ibid*

Overall Recommendations

SADC states to sign, accede, ratify and localize to regional, continental and international articles, charters, conventions; and other instruments (a list shown in section 3 of this paper) on digital rights.

1. States to refrain from internet shut down
2. Establish independent and well-resourced NIGFs; Strengthen NIGFs and the regional IGF, such that multi-stakeholder decisions and policy formulations are improved.
3. Enactment of clear cyber-security, privacy, surveillance and/or interception and access to information legislation that is human rights centered.
4. Ensure and promote digital rights, democracy and constitutionalism.
5. Develop strong institutions that may perform their duties as per international standards and local laws, mainly the judiciary and legislature.
6. Need of advocacy and political will to promote and ensure digital rights, reduce digital divide; with special focus on gender and location based digital divide.
7. Enhance regional cooperation among stakeholders.
8. SADC to have an independent mechanism to monitor digital rights like the UN and AU Special Rapporteur on Freedom of Expression and Access to Information.
9. Increase awareness and advocacy for digital rights in the region.
10. Promote research, information sharing and entrepreneurship in the area of digital rights.
11. Protect and ensure rights of journalist.

Conclusion

The spread and access of digital instruments has been rapid due to increasing ICT innovations and relatively decreasing costs in mobile technology, thus allowing remote and rural parts of the world to connect, and in some cases sidestep landlines altogether. The importance of communication is recognised internationally as having a profoundly positive effect on the enjoyment of civil, cultural, political, physiological, economic, physiological, and social rights both online and offline. The key digital rights under threats and that need continuous monitoring, respect and protection as shown in the paper are freedom of expression, right to privacy, right to receive and disseminate information, freedom and right of association and assembly and rule of law.

The concerning rise in incidents of Internet shutdowns, ban on

mobile services, internet throttling, social media and content taxation, surveillance, criminalisation of free expression and abuse of journalist, among others, completely violate an individual's freedom of expression, right to access online and freedom of assembly and association online. The practice of restricting or blocking Internet and mobile services also contradicts human right instruments, as shown in this paper. Thus, human rights implications of restricting and blocking the Internet or mobile services; and surveillance intentional creation of communication or media dark zones by not providing enough infrastructure for Internet services or by imposing laws and policies that violate right to access online, freedom of expression online and freedom of assembly and association online, need to be analysed and investigated critically.



Finally, we reiterate that digital rights are human rights, promote, protect and enjoy them.



Media Institute of Southern Africa Zimbabwe Chapter
Harare, Zimbabwe
Telephone: +263242776165/ +263242746838
www.zimbabwe.misa.org

ISBN
9781779065353