DIGITAL RIGHTS AND ACCESS TO INFORMATION SERIES 1

DIGITAL RIGHTS ARE HUMAN RIGHTS

An introduction to the state of affairs and challenges in Africa

Hendrik Bussiek
April, 2022

In sub-Saharan Africa, 495 million people (46 percent of the population) subscribed to mobile phones in 2020, however, the cost of accessing the internet is very high and many African Governments are renowned for restricting access to the internet to limit critics and their opposition through internet shutdowns, especially ahead of elections.

There is widespread government surveillance in many countries in Africa without sufficient legal basis. In Zimbabwe, for example, the interception of private communications is permitted without a warrant issued by a court; instead, the Minister of Transport and Communication has the power to order such surveillance.

Many countries in Africa and around the world have passed cybercrime legislation in recent years or are about to do so. There is great concern that many of these laws over-reach their legitimate aim, lack clear definitions and are susceptible to being used for regulating online content and restricting freedom of expression.

FRIEDRICH EBERT STIFTUNG
fesmedia Africa

DIGITAL RIGHTS AND ACCESS TO INFORMATION SERIES

DIGITAL RIGHTS ARE HUMAN RIGHTS

An introduction to the state of affairs and challenges in Africa

Contents

1

INTRODUCTION

1 January 1983 is considered the official birthday of the internet. This is when a new technology (Transfer Control Protocol/Internetwork Protocol – TCP/IP) created a standard that enabled various computer networks to communicate with each other.[1] What started out as a tool of exchange among scientists and professionals gradually drew in more and more people and expanded in scope in the new millennium. The video/voice calling service Skype started in 2003, Facebook in 2004, Twitter in 2006, Instagram in 2010, Google in 2011, TikTok in 2017. Billions of people now have access to the internet at their fingertips wherever they go. In sub-Saharan Africa, 495 million people (46 percent of the population) subscribed to mobile phones in 2020[2]. All in all, 4.95 billion people around the world actively use internet.[3]

There has been no shortage of enthusiasm, hope and optimism along the way (not least on the part of the industry). The new digital technology turned the world into a global village. Humanity in all parts of the globe became connected. The speed of information increased exponentially. People now communicate with each other in real time over long distances. Questions are answered within seconds on Google. And the internet was about to democratise the entire world. The Arab Spring 2010, starting in Tunisia, was termed a 'Facebook revolution', the Sudan uprising 2019 would not have been possible without social media. People come together and organise for a common cause by digital means. Online media have sprung up and multiplied, bloggers started blogging, everyone is able to have her or his say.

Yes, sort of.

On the other hand, authoritarian governments have also discovered the potential of the new technology and learnt to use it for their purposes: to propagate their own version of "the truth" unchecked by professional media, to influence public opinion in their favour, to keep track of and clamp down on opposition voices, or shut down access altogether. General users also abuse the technology: there is a rising flood of hate speech and cyber-mobbing, of misinformation, disinformation and conspiracy myths. Of course, all of these are not new phenomena, but they are infinitely easier to set in motion at the click of a button or the touch on a screen in the faceless anonymity of the net.

As early as 2012 the United Nations' Human Rights Council established an important basic principle: Human rights apply equally online and offline, digital rights are human rights. All people have the right to access, use, create and publish information freely, to enjoy and exercise freedom of expression, information and communication as long as they do not violate the rights of others. Similarly, it is the right of everyone to access, use, create, share and publish information via digital media, blogs, websites and the like; again: as long as the rights of others are respected.

The challenge is how to realise these rights equally for all and how to protect them – against interference by the state as well as misuse. Any attempt to update declarations on freedom of expression, to develop new laws or amend existing ones to fashion specialised cyber-crime legislation needs to stand this basic test: does it serve to protect digital rights as human rights?

1. https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml
2. https://www.gsma.com/mobileeconomy/sub-saharan-africa/
3. https://datareportal.com/global-digital-overview

2

UNIVERSAL AND EQUAL ACCESS TO INTERNET

The Declaration of Principles on Freedom of Expression and Access to Information in Africa was adopted by the African Commission on Human and Peoples' Rights (AU Declaration) in 2002 and updated in 2019 to include digital rights. It states that the "universal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression, access to information and the exercise of other human rights".

Conditions on the ground show that this principle is still far from being realised. The precondition for access to the internet is access to a stable power supply. According to the World Bank[4] only 46.5 percent of the population in sub-Saharan Africa had access to electricity in 2019. The share of people using the internet in Africa as a whole is 39.3 percent of the population in 2020 compared to 62.9 percent in the rest of the world. Within the continent, regional and national differences are extreme, with 59.5 percent of people in Southern Africa having access to internet but only 24 percent in Eastern Africa.[5] And the correlation between power supply and internet access shows most starkly when comparing urban and rural areas continent-wide: While 77.9 percent of urban dwellers have electricity and 50 percent have internet access, in rural regions the figures stand at 28.1 and just 15 percent respectively.[6]

The costs of accessing the internet on mobile phones, as most people do, are high. The United Nations has defined ideal internet affordability as "1 for 2" – that is 1 gigabyte of data costing no more than 2 percent of the average monthly income. (1 gigabyte allows you to use Facebook for about 51 hours, browse websites for 44 or chat on skype for 4; a regular user of social media accounts will clock up 3 to 5 gigabytes per month[7].) In Africa users, on average, pay 4.3 percent of their monthly income for this amount of data (in the Americas the percentage is 2.5, in the Asia-Pacific region 1.4).[8] Again, there are vast differences in prices among countries: in Malawi, for example, one gigabyte costs the equivalent of US $ 25.46, in Namibia 22.37, in South Africa 2.67, in Zambia 1.13.[9]

The question is whether – and for how long – such a divide between the digital haves and the have-nots can be allowed to persist, even to widen. To do so will mean risking serious damage to the social fabric, to people's sense of common purpose as citizens of one country and thus, ultimately, to the very foundations of a democratic state.

CHALLENGES

In many countries huge investments are needed for the development of an improved electricity grid and communications infrastructure, particularly in underserved regions. The political will to embark on such endeavours may be there, but funds are often lacking.

- How can private – local and international – investors (or the donor community?) be encouraged to engage in this sector?
- How can competition between more service providers be stimulated to bring prices down?
- How can governments be sensitised/engaged to create a favourable environment for digital investments and development?
- What can governments or civil society do to provide affordable access to underprivileged and marginalised communities?

4. worldbank.org/indicator/EG.ELC.ACCS.ZS? locations=ZG
5. https://www.statista.com/statistics/1176668/internet-penetration-rate-in-africa-by-region/
6. https://www.itu.int/itu-d/reports/statistics/2021/11/15/internet-use-in-urban-and-rural-areas/
7. https://www.confused.com/mobile-phones/mobile-data-calculator
8. https://a4ai.org/affordability-report/report/2020/#what_is_the_state_of_internet_affordability_and_policy?
9. https://www.cable.co.uk/mobiles/worldwide-data-pricing/

3

GOVERNMENT INTERFERENCE WITH INTERNET ACCESS

The AU Declaration says that states "shall not interfere with the right of individuals to seek, receive and impart information … through removal, blocking or filtering of (internet) content". Nevertheless, authoritarian governments in a number of African countries have blocked or filtered citizens' access to the internet for various periods of time and for very similar reasons, usually the protection of 'national security', read: their own secure stay in power – as the only guarantors of 'national security', of course. Just for the record: a threat to national security is generally defined as the use or threat of force against a country's very existence or its territorial integrity, be it external or internal.[10]

The all-too-common misinterpretation of national security as being synonymous with state security or regime security presents problems for the unhindered practice of freedom of expression both online and offline. However, it seems to come in particularly handy as a ready excuse to cut off a whole array of information and communication channels at one go, swiftly and effectively.

Technically, this is relatively easy for governments to do: not by pushing their own 'stop' button but by ordering internet service providers (ISPs) to suspend internet connectivity as a whole or block certain websites or apps. ISPs are companies dependent on government licences and will mostly comply with such orders for fear of retribution or legal action. In 2019, for example, the Zimbabwean government ordered the largest telecommunications company in the country to shut down all internet services. The Chairman followed the directive because, as he wrote in a post, "non-compliance would result in immediate imprisonment of management on the ground".[11]

Governments (not just) in Africa block or restrict access to the internet during elections, demonstrations, ahead of planned protests, in the case of military coups - whenever the going for them gets rough and they seek to suppress criticism and opposition. As a simple rule-of-thumb: the less democratic a government is, the more likely it is to order an internet disruption. The official justification for restricting one of citizens' basic rights is ostensibly in line with the AU Declaration and other international standards which allow for limitations on the right to freedom of expression "to protect national security".

However, the AU Declaration (and democratic legislation worldwide) specifically points out that the right to freedom of expression can only be limited if such restrictions are clearly defined and "prescribed by law". In most countries there is no legislation which would authorize the suspension of access to the internet and the use of social media platforms. In Tanzania, for example, Twitter and WhatsApp were blocked during the 2020 elections without any legal basis. In Uganda, access to the internet was suspended ahead of the 2021 elections in spite of the Communications Act which says that a service provider shall not deny access to a customer "except for non-payment of dues or for any other just cause". The authorities simply used "any other just cause" as justification for the shutdown. In June 2021, the Nigerian Ministry of Information suspended Twitter till January 2022, after the platform had deleted the tweets and account of the President, Muhammadu Buhari, for "contents that threatens or incites violence". As justification the Ministry (on Twitter) cited "the persistent use of the platform for activities that are capable for undermining Nigeria's corporate existence"; without making reference to any legal basis.[12]

CHALLENGE

Government orders for blockages or suspensions of internet access need to be questioned and tested in courts of law for their compliance with legal and constitutional requirements. Judgements should be published widely (on the net, among others) to create a body of case decisions for reference in other cases, as a basis for the development of model legislation, and as a deterrent to similar government actions in the future.

10. https://www.article19.org/resources/foe-and-national-security-a-summary/
11. https://www.techzim.co.zw/2019/01/my-companies-in-zimbabwe-drc-and-sudan-were-complying-with-the-law-when-they-blocked-the-internet-but-i-am-praying-and-fasting-for-you-says-strive-masiyiwa/
12. https://twitter.com/FMICNigeria/status/1400843062641717249?ref_asrc=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1400843062641717249%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.nytimes.com%2F2021%2F06%2F05%2Fworld%2Fafrica%2Fnigeria-twitter-president.html

4

SURVEILLANCE

The surveillance of internet communications seems to be a considerable temptation for some African governments – again because it is such an easy and effective way to keep track on the mood and concerns of the people, especially those critical of government.

The AU Declaration says unequivocally that "states shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications". Targeted surveillance, on the other hand, must be "authorised by law" and has to be "premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim". At a minimum, says the UN Special Rapporteur on freedom of opinion and expression, such surveillance must be authorized by an independent, impartial and competent judicial authority, certifying that the request is necessary and proportionate.[13]

In reality there is widespread government surveillance in many countries in Africa without sufficient legal basis. In Zimbabwe, for example, the interception of private communications is permitted without a warrant issued by a court; instead, the Minister of Transport and Communication has the power to order such surveillance. The Tanzania Intelligence and Security Service is authorised to intercept communications without a warrant if it "has reasonable cause to consider a risk or a source of risk of a threat to the state security". In Uganda a court warrant is needed to intercept communications but there are no clear and objective criteria for courts to apply. A warrant has to be issued if such surveillance is needed for the protection of national security, national defence and public safety.

In South Africa, legislation provides for a "designated judge", appointed by the minister in charge of the administration of justice. In February 2021, the Constitutional Court declared this provision unconstitutional because "the designation by a member of the Executive … does not conduce to a reasonable perception of independence". Even more, the court demanded safeguards for special groups such as lawyers and journalists to ensure the confidentiality of communications between them and their clients or sources respectively. The court also required "post-surveillance functions", meaning that the person surveilled should be informed of the fact afterwards. This would enable the subject of surveillance to "seek an effective remedy for the unlawful violation of privacy". And, the court continued, "that will help … reduce violations of the privacy of individuals".[14]

CHALLENGES

- What are the best ways to organise and pursue strategic litigation to challenge existing laws and actions that violate constitutionally guaranteed rights (to freedom of expression as well as to privacy) and how can civil society, independent media and the courts be empowered to do so?
- What can be done to ensure that African states comply with minimum standards such as prior authorisation by an independent court, notification of the victim after surveillance and special protection for lawyers and journalists?
- Should such protection perhaps be granted also to other professionals such as medical doctors or priests?

13. https://www.ohchr.org/en/issues/freedomopinion/pages/sr2017reporttohrc.aspx
14. https://privacyinternational.org/sites/default/files/2021-02/%5BJudgment%5D%20CCT%20278%20of%2019%20and%20279%20of%2019%20AmaBhungane%20Centre%20for%20Investigative%20Journalism%20v%20Minister%20of%20Justice%20and%20Others.pdf

5

CYBERCRIME LEGISLATION

"Cybercrime" is defined as actions taken against the confidentiality, integrity and availability of computer data or systems as well as traditional offences committed through the internet. According to international standards cybercrime legislation is meant to penalise illegal access to computer systems, illegal interception of digital communication, interference with data, computer-related forgery and fraud and infringements of copyright.

Many countries in Africa and around the world have passed cybercrime legislation in recent years or are about to do so. There is great concern that many of these laws over-reach their legitimate aim, lack clear definitions and are susceptible to being used for regulating online content and restricting freedom of expression.

Just as in the analogue world, there are, of course, legitimate restrictions to freedom of expression on the internet. As long as these restrictions are clearly specified, proportionate and justified in a democratic society in order to protect the rights and dignity of others, they will apply equally online and offline and there is no need to spell them out again in cybercrime legislation.

In some 'borderline' cases there may be good reason to do so nevertheless – because of the sheer magnitude of the internet as a medium of communication and its vast and immediate impact. A Model Law developed by SADC in 2013 prohibits the distribution of racist or xenophobic material or insults on the internet or the denial of genocide and crimes against humanity. The South African Cybercrimes Act 2021 criminalises posting "intimate images of a person" without the consent of that person. Similarly, the dissemination of child pornography, generally illegal, is possible by traditional media, but will have much more wide-reaching and devastating effects on internet platforms and thus should be expressly covered in cybercrime law.

In some countries governments are reviving shaky old concepts like the prohibition of 'false news' under the guise of new cyber law. Zimbabwe amended its Criminal Law to include internet-related offences such as 'false news'. The law criminalises the use of a computer or information system to make "available, broadcast or distribute data … knowing it to be false" to anyone "with intent to cause psychological or economic harm". In Kenya the Computer Misuse and Cybercrime Act makes it an offence to publish "information that is false in print, broadcast, data or over a computer system, that is calculated or results in panic, chaos, or violence among citizens of the Republic".

Given the ever-rising flood of dis- and misinformation on the net such provisions may seem to make sense. But who is to decide whether a piece of information was distributed with the intent to cause harm, let alone what is true or 'false'? Users of social media are receiving all sorts of messages and will seldom be able to determine their origin or authenticity. Are they all to be held liable for distributing 'false' data when they forward a message deemed 'false' by whoever? The Supreme Court in Uganda ruled in 2004 that "a person's expression or statement" is not precluded from the right to freedom of expression "simply because it is thought by another or others to be false, erroneous, controversial or unpleasant".

This seems to be a very apt description of a large chunk of internet content today, especially on social media. There is cyber-mobbing, spewing of hatred against public figures, denigration of minorities or 'others', offensive language of the kind no one in their right mind would use face-to-face with another person; there are conspiracy tales and deliberate disinformation campaigns. 'Unpleasant' indeed, all of it. But criminal?

If so, the nature of the offence must be clearly specified in law and perpetrators prosecuted and penalised accordingly. In the case of serious offences like hate speech (in the words of the South African constitution: "propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm") or the violation of a person's dignity and reputation, the requisite provisions will often already be in place in other pieces of legislation and thus not need any additional coverage by cyberlaw.

CHALLENGES

- If the right to "communicate anonymously or use pseudonyms on the internet" as stipulated by the AU Declaration is to be maintained, how does one identify perpetrators of serious cases of hate speech and disinformation? How can victims of cyber bullying get access to the names of account holders in order to claim damages?
- Is the definition of hate speech provided by the above cited South African constitution still sufficient? When does a sustained disinformation campaign become a serious threat to the foundations of a democratic society? Who is to determine the fine line between communications that a free society will need to tolerate and those that it must not?

Such decisions cannot be left to governments or to service providers who may or may not decide to pull the plug on individual accounts according to their own criteria. These questions need to be widely and publicly debated by civil society, the user community, legal and digital experts and governments to come up with solutions that will be backed by all.

6

HOW TO PRESERVE A FREE INTERNET

For a start, every user can at least try to check the facts: verify information, seek proof from additional sources, sort facts from fiction. It may be a little more time-consuming but is fairly easy to do (thanks to the net) and certainly more rewarding than just mindlessly hitting the button to share or like a post. There is a basic old principle that has served generations of journalists well: When in doubt, leave it out. And it's up to each individual user to either feed a shitstorm or help to stop it.

Fortunately, there are now a number of projects in Africa that engage in fact-checking. Africa Check, for example, is a non-for-profit organisation that works continent-wide and has correspondents in several countries who investigate major pieces of misinformation and publish corrections. The goal is to break the cycle of false information by having a critical mass of people with appropriate skills to slow down the wave. A national example is Namibia Fact Checks which aims to verify public statements and media reports. Over the past few years it focussed in particular on the spread of misinformation on COVID 19.

The key word is 'media and information literacy' (MIL). MIL education should start at school level. However, a 2020 study on the curricula of state schools in seven African countries shows that none of them included any meaningful media education. Only one province in South Africa – Western Cape – has introduced a structured plan for MIL, starting in grade 8 with establishing a mindset of 'click restraint'. In grade 9 students are taught to identify misinformation and 'fake' websites, in grade 10 the potential social and political impact of online misinformation is addressed, and in grade 11 students discuss how social media become a tool for exerting political influence. [15]

With the education system in Africa showing little or no interest in the subject, it is up to civil society organisations to fill the gap. UNESCO, for example, calls upon youth organisations to become active and encourage young people to acquire literacy skills. The hope is that they will then spread the MIL message among their peers online.

The internet is and remains an invaluable tool of information, communication and empowerment. And, contrary to common perception, it is not a parallel world or universe or metaverse (or whatever next). It is populated by the same fellow human beings we may meet any day on a train or in the streets, in an office or a pub anywhere in the world, all of us able to use our brains, to act responsibly and treat others with the respect we expect to be given in return. There is no reason why this shouldn't work online. And we should do everything in our power to make it work, for our benefit.

14. file:///C:/Users/Bussiek/AppData/Local/Temp/misinformation-policy-in-sub-saharan-africa-1-the-state-of-media-literacy-in-sub-saharan-african.pdf

ABOUT THE AUTHOR

Hendrik Bussiek is a journalist and international media consultant. He is an expert in the areas of media policy and legislation with a special focus on Africa, author/editor of several publications on freedom of expression and public broadcasting, and co-founder of the African Media Barometer.

Editor:
Friedrich-Ebert-Stiftung fesmedia Africa
95 John Meinert Street
E-mail: **info@fesmedia.org**

Responsible Person
Freya Gruenhagen, Director *fesmedia* Africa

Design and layout
Bryony van der Merwe

Contact/Order: **dickson@fesmedia.org**

ABOUT THIS PROJECT

fesmedia Africa is the regional media project of the Friedrich Ebert-Stiftung (FES) in Africa. Its work promotes a free, open, liberal and democratic media landscape that enables ordinary citizens to actively influence and improve their lives, as well as those of the communities and societies they live in. *fesmedia* Africa believes that in order to participate in public life and decision-making, people need to have the means, skills and opportunities to access, exchange and use information and knowledge. They need to be able to communicate and exchange ideas, opinions, data, facts and figures about issues that affect them and their communities.

For more information, visit:
https://fesmedia-africa.fes.de/

ISBN
978-99945-77-95-8

DIGITAL RIGHTS ARE HUMAN RIGHTS

An introduction to the state of affairs and challenges in Africa

In sub-Saharan Africa, 495 million people (46 percent of the population) subscribed to mobile phones in 2020, however, the cost of accessing the internet is very high and many African Governments are renowned for restricting access to the internet to limit critics and their opposition through internet shutdowns, especially ahead of elections.

There is widespread government surveillance in many countries in Africa without sufficient legal basis. In Zimbabwe, for example, the interception of private communications is permitted without a warrant issued by a court; instead, the Minister of Transport and Communication has the power to order such surveillance.

Many countries in Africa and around the world have passed cybercrime legislation in recent years or are about to do so. There is great concern that many of these laws over-reach their legitimate aim, lack clear definitions and are susceptible to being used for regulating online content and restricting freedom of expression.

More information on the subject is available here:
https://fesmedia-africa.fes.de/

FRIEDRICH EBERT STIFTUNG
fesmedia Africa