digital rights SOUTHERN AFRICA

Issue No. 01

JULY 2022

Data and online privacy under attack

AFRICAN DECLARATION ON INTERNET RIGHTS AND FREEDOMS

African Declaration on Internet Rights and Freedoms

A fundamental challenge in need of urgent resolution in the digital age is how to protect human rights and freedoms on the Internet, and the African continent is no exception. The African Declaration on Internet Rights and Freedoms was developed in response to this challenge.

13 PRINCIPLES:

1. Openness

2. Internet Access and Affordability

3. Freedom of Expression

4. Right to Information

5. Freedom of Assembly and Association and the Internet

6. Cultural and Linguistic Diversity

7. Right to Development and Access to Knowledge

8. Privacy and Personal Data Protection

9. Security, Stability and Resilience of the Internet

10. Marginalised Groups and Groups at Risk

11. Right to Due Process

12. Democratic Multistakeholder Internet Governance

13. Gender Equality

Contents

digital rights

SOUTHERN AFRICA

ISSUE 01

JULY 2022

Southern Africa Digital Rights is produced under 'The African Declaration on Internet Rights and Freedoms: Fostering a human rights-centred approach to privacy, data protection and access to the internet in Southern Africa' project.

Editorial Board:
Jan Moolman (APC)
Zoe Titus (NMT)
Frederico Links

Editorial Coordinator:
Frederico Links

Layout & production:
Naua Web Trading

Contributors:
Thapelo Ndlovu (Botswana)
Ndimphiwe Shabangu (Eswatini)
Jimmy Kainja (Malawi)
Frederico Links (Namibia)
Susan Mwape (Zambia)
Otto Maki (Zimbabwe)
Nompilo Simanje (Zimbabwe)

Published and distributed by:
Association for Progressive Communications (APC)
133, 2nd Avenue, Melville 2092,
Johannesburg, South Africa

Namibia Media Trust (NMT),
13 Adler Street, Windhoek,
Namibia

Funded by:
Open Society Initiative for Southern Africa
1st Floor, President Place
1 Hood Ave. / 148 Jan Smuts Ave.
Rosebank, Johannesburg,
South Africa

Correspondence can be sent to:
Rosevitha Ndumbu
rosevitha@nmt.africa

Editorial

Showcasing the will and commitment of those fighting

FREDERICO LINKS

Digital rights are under threat everywhere across the African continent at the moment.

This is borne out and underscored by a string of influential reports over recent years from prominent regional and global civil society, multilateral and digital rights non-governmental organisations.

The constricting of digital civic spaces through lawfare, the use of sophisticated spyware by some governments to invasively and violatingly intrude into and monitor people's lives, pervasive social media mediated disinformation souring online experiences, rampant cyber criminal attacks and the dehumanising commercial surveillance economy all combine to degrade Africans' online lives.

This is happening at a time when cyberspace also still shows so much promise as an avenue for achieving broad-based social justice, as well as unlocking socio-political and economic freedoms.

African internet users remain resilient in the face of all manner of state-sponsored and private tech-enabled cyber threats and obstacles, and civil society actors across various countries continue to raise and amplify their voices and the hopes and aspirations of their constituencies even as their spaces for free expression, both online and offline, are being squeezed tighter and tighter by a range of malevolent actors and forces.

This project – an initiative of the African Declaration (AfDec) Coalition, supported by the Association for Progressive Communications (APC) and the Namibia Media Trust (NMT), and funded by the Open Society Initiative of Southern Africa (OSISA) – seeks to open up another avenue for elevating the voices of African civil society actors, specifically those scattered across six southern African countries in most of which democratic engagement spaces are increasingly, and in some severely, constrained.

The project brings together civil society and digital rights researchers, activists and advocates from about 10 organisations spread over Botswana, Eswatini, Malawi, Namibia, Zambia and Zimbabwe. These individuals and organisations are partnering and collaborating to shine a bright spotlight on the individual

As part of our collaboration we will be bringing you regular updates concerning access to the internet and the state of data and online privacy in our respective countries. We will be bringing you these updates through six regional digests, of which this is the first, that we will be producing until May 2023.

country-level digital rights and online civic spaces in which they operate.

This six-country digital rights collage captures and portrays broader regional narrative streams in the quest to democratise the sub-regional cyber space.

As part of our collaboration we will be bringing you regular updates concerning access to the internet and the state of data and online privacy in our respective countries. We will be bringing you these updates through six regional digests, of which this is the first, that we will be producing until May 2023.

In this first edition, we look at how civil society in Botswana, with regional support, managed to convince the government to make significant and meaningful changes to draft criminal procedures law that would have been a death-knell to digital privacy.

We also discuss how in the wake of uprising and unrest ordinary citizens in Eswatini have to navigate a new reality under a newly imposed cybercrime law.

Then there is the discussion of how the arrests of journalists and social media users are problematically characterising the digital rights space in Malawi.

In the same vein, Namibia is introducing mandatory SIM card registration and data retention regulations that could become a violation of the constitutionally enshrined right to privacy.

In Zambia, civil society actors are pushing for the review and repeal of a cybercrime law that was brought in to suppress legitimate political expression.

And from Zimbabwe, we bring you a discussion of how a complex range of issues are impacting the exercising of digital rights in the country.

While all this might not make for happy reading, it certainly is important reading, and it showcases the will and commitment of those in each of the countries who continue to fight for freedoms, both online and offline.

With all that said, we bring you *Digital Rights Southern Africa.*

Botswana CSOs **rebuff criminal procedures bill**

THAPELO NDLOVU

The draft bill would have enabled surveillance abuse and privacy violations.

State surveillance practices have been jolted into sharp focus in Botswana since public revelations in 2020 and 2021 implicated the Botswana government as a client of some of the most notorious spyware makers and distributors in the world.

The sensitive issue was reignited in early 2022 as the country's Minister of Defence, Justice and Security sought to push through a bill that would have further undermined online privacy and freedom of expression, in a disturbing trend which has concerned civil society in the country over recent years.

The emergence of the problematic provisions of the Criminal Procedures and Evidence (Controlled Investigations) Bill galvanised regional support for Botswana media and human rights civil society organisations to have the bill's human rights violating elements amended once it was tabled in the country's parliament.

New criminal procedures bill

On 24 January 2022 the Minister of Defence, Justice and Security, Kagiso Mmusi, indicated in the country's parliament that he would be tabling the Criminal Procedures and Evidence (Controlled Investigations) Bill through an urgent motion.

The fast-tracked bill was published on 12 January 2022.[1]

Even before the bill was table in the Botswana parliament, on 26 January 2022, a coalition of Botswana press freedom organisations, including the Media Institute of Southern Africa (MISA) Botswana chapter, issued a scathing statement of the bill, including stating that the proposed law would amount to "nothing short of criminalising journalism itself, and with that, the freedom of expression".[2]

Similarly, on 1 February 2022, the Universal Periodic Review (UPR) NGO Working Group – consisting of six organisations and led by the Botswana Centre for Human Rights (Ditshwanelo) – had issued a statement, saying the bill "gives the law enforcement agencies of Botswana power to intercept communication of journalists, human rights defenders and other citizens; power to force journalists and ordinary citizens to disclose information; allow intelligence agents to use assumed identities; and be immune from prosecution. Two other effects will be an increased shrinking of civil society space and vulnerability of Human Rights Defenders (HRDs)".[3]

On 4 February 2022 the bill was tabled in the National Assembly of Botswana following which it attracted almost immediate public outcry that it provided for invasion of privacy and that it would enable the infringement of freedoms of expression and the media.

In an editorial following the tabling of the bill, Mmegi newspaper stated that "the public had issues with the provisions of the Bill that allowed the State to spy on them. This caused a furore amongst Batswana".[4]

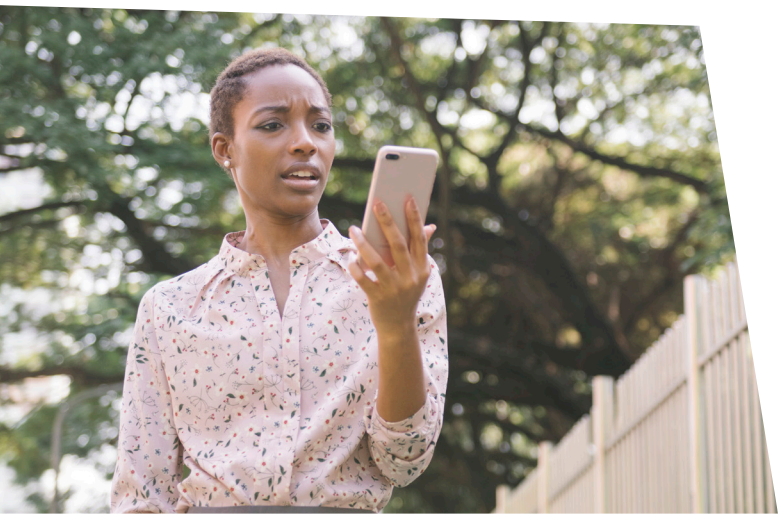
1 https://cpj.org/wp-content/uploads/2022/01/Botswana-Criminal-Procedure-and-Evidence-Bill.pdf

2 https://misa.org/blog/botswana-media-groups-fret-over-new-snooping-bill/

3 https://www.facebook.com/ditshwanelobotswana/

4 https://www.mmegi.bw/editorial/the-fruits-of-the-medias-watch-dog-role/news

In a statement, SAEF observed that the bill as it was then, "was dangerous as it forces the disclosure of information by citizens including journalists and allows intelligence officers to use fake identities while providing them immunity from prosecution".



The bill "provides for an interception of communications framework, which authorises the interception of communications by investigatory authorities and sets out the role of service providers in controlled investigations for the gathering of criminal evidence".

One of the more troubling provisions of the bill singled out for criticism was clause 16 (1), which enabled warrantless communications interception and surveillance, and stated: "Where a head of an investigatory authority believes on reasonable grounds that the delay in obtaining an interception warrant would defeat the object of the investigations, he or she may, in writing, authorise an investigating officer to intercept communications to detect, investigate or uncover the commission of an offence, or to prevent the commission of any offence."

It was this provision that the UPR NGO Working Group said would "have a chilling effect on the ability of the media to conduct its work as well as on the right of all persons to privacy".

The campaign against the bill attracted regional support as the Southern African Editors Forum (SAEF), the African Editors Forum, the Campaign for Freedom of Expression (CFE) and the Media Institute of Southern Africa (MISA) extended assistance to local organisations, notably to MISA Botswana chapter and the Botswana Editors Forum to openly challenge the bill.

In a statement, SAEF observed that the bill as it was then, "was dangerous as it forces the disclosure of information by citizens including journalists and allows intelligence officers to use fake identities while providing them immunity from prosecution".[5]

The African Editors Forum (TAEF) followed with its own statement amplifying the concern. The TAEF stated: "The bill will allow the government to spy on citizens without a warrant and supervision from the courts. This is a direct move to subvert democracy and violate the rights of the media to do its work freely and the rights of Batswana to freely receive information."[6]

In the end, the pressure that was brought to bear by various human and media rights organisations, and the international spotlight that it attracted, paid off and the bill was withdrawn and amended.

The new bill which was later passed through the committee stage to become law introduced new diluted clauses such as Clause 7, 'Protection of privacy in controlled investigations,' as well as replacing the offending ones such as Clause 16, which was replaced with one titled, 'Prohibition of interception of communications without a warrant.'

The amended bill contained the following provisions, among others, that:

- "Prohibit investigators from intercepting communications without a warrant, where previously the Bill provided for authorities to conduct warrantless interception of a person's communications for up to 14 days;
- Create a committee, to be headed by a judge, which will give oversight on interception operations and undercover investigations and receive complaints about any misuse of such powers;

5 https://sanef.org.za/saef-expresses-shock-at-the-criminal-procedure-and-evidence-bill-before-the-botswana-parliament/

6 https://cpj.org/wp-content/uploads/2022/01/TAEF-statement-on-Botswana.pdf

"In mid-2021 it emerged that Botswana was also a client of another spyware firm, Cellebrite, that is a vendor of phone-hacking technology."

- Require the committee to report annually on its work, which the Minister of Defence, Justice and Security must table in Botswana's National Assembly."[7]

Following this, the MISA Regional Governing Council visited Botswana at the end of February 2022 and met with Botswana government officials, including the Minister of Defence, Justice and Security, Kagiso Mmusi, as well as local media and CSOs.

In a statement issued on 7 March 2022, after the Botswana visit, the MISA Regional Governing Council stated: "It was MISA's position that Botswana has a good reputation in terms of being the oldest democracy on the continent. There was therefore a need to maintain this distinction by ensuring the Bill does not infringe on individual freedoms such as the rights to free expression, privacy and association. MISA acknowledged and noted that the government of Botswana had listened to civil society organisations by amending the contentious parts of the Bill."[8]

According to various reports on the bill, quoting the Minister of Defence, Justice and Security, the attempt to rush the bill through enactment in the Botswana parliament was ostensibly brought about by the country having to meet commitments in terms of cyber crime regulation under the auspices of the Financial Action Task Force (FATF). However, this justification has been disputed by Botswana's political opposition and CSOs, as there appeared to be nothing in the FATF recommendations to the country to justify the human rights violating provisions in the original bill.[9]

Historical violations

In 2020 Botswana was exposed as one of seven African countries that used spyware marketed by Isreali-owned, Cyprus-based, firm Circles, to spy on journalists.[10] The other African countries implicated as clients of Circles were Equatorial Guinea, Kenya, Morocco, Nigeria, Zambia, and Zimbabwe.

The Botswana government's Directorate of Intelligence and Security Services was identified as having used Circles' spyware to hack into people's communications devices. The spying was traced as far back as 2015, with the latest incident reportedly being recorded in 2020.

Circles is reportedly associated with the Isreali spyware maker NSO Group, vendor of the notorious Pegasus spyware system.[11]

In mid-2021 it emerged that Botswana was also a client of another spyware firm, Cellebrite, that is a vendor of phone-hacking technology. Reports revealed that the Botswana police "are making use of Cellebrite's flagship product the Universal Forensic Extraction Device to extract data from the phones of journalists as part of a wider crackdown on the media".[12]

It is against this backdrop – of the use of law and technology to enable the violation of data and online privacy – that the digital rights landscape in the country remains a cause for concern within local civil society. ■

Thapelo Ndlovu is a media consultant and compiled this report on behalf of the Media Institute of Southern Africa (MISA) Botswana chapter. Additional reporting by Frederico Links.

7 https://altadvisory.africa/2022/02/11/botswana-media-groups-note-changes-to-controversial-interceptions-bill/
8 https://misa.org/blog/misa-meets-government-officials-in-botswana-over-the-criminal-evidence-procedure-controlled-investigations-bill/
9 https://freeexpression.org.za/a-threat-averted/
10 https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/
11 https://africanarguments.org/2021/02/the-seven-african-governments-using-israeli-cyberespionage-tools/
12 https://www.haaretz.com/israel-news/tech-news/2021-07-14/ty-article/.premium/cellebrite-tech-used-against-journalists-in-botswana-investigation-reveals/0000017f-db5a-d3a5-af7f-fbfe72930000

Eswatini passes **cyber laws under dark clouds**

NDIMPHIWE SHABANGU

Kingdom enacts cyber crime and data protection laws in a climate of suspicion and unrest.

Since early 2021 the Kingdom of Eswatini has been gripped by waves of civil unrest, with reports having emerged of human rights violations perpetrated by the country's security services and internet shutdowns implemented by the government in response to protests.

In June-July 2021, Eswatini experienced civil unrest which stemmed from governance related issues. The unrest resulted in violence which led to the death of citizens and damage to property. This resulted in the government directing telecommunications service providers – state-owned Eswatini Post and Telecommunications Corporation, MTN Eswatini and Eswatini Mobile – to shut down the internet[1]. This had never been witnessed before in the Kingdom. There were more protests in October 2021, and the government again shut down the internet and resorted to restricting social media platforms[2]. It should be noted that Internet shutdowns and restrictions negatively affect businesses, and disrupted citizens' ability to communicate.

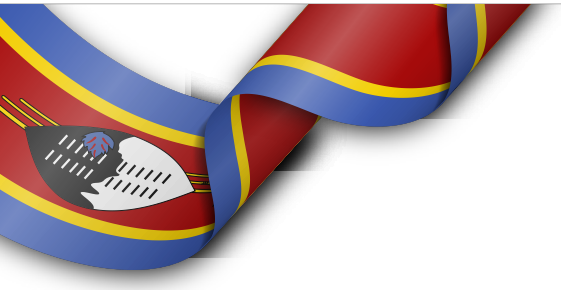
The political situation has remained volatile throughout the first half of 2022, as the general mood of unrest has continued to threaten to spill into public again.

It was in this climate of heightened political sensitivity and instability that the Kingdom, in early 2022, gazetted various cyber laws that will regulate how citizens conduct themselves on the internet.

Digital legislation

The Swaziland Communications Commission Act of 2013 established what is now called the Eswatini Communications Commission, which is a regulatory body

1 https://qz.com/africa/2029884/eswatini-turns-off-internet-to-silence-pro-democracy-protestors/



Among the concerns expressed is that the law has the potential to be interpreted in a way that targets vocal human rights defenders, media practitioners and activists.

that regulates all communications services, including the internet, in the country. This commission is under the Ministry of Information, Communication and Technology (MICT).

The creation of the Eswatini Communications Commission has been the catalyst for and instrumental in the enactment of the latest batch of cyber laws[3]. These new laws are the Computer Crime and Cyber Crime Act, 2022, the Data Protection Act, 2022, and the Electronic Communications and Transactions Act, 2022.

The Computer Crime and Cyber Crime Act, 2022, and the Data Protection Act, 2022, were gazetted and came into force on 4 March 2022, while the Electronic Communications and Transactions Act, 2022, which was also gazetted on the same date, had yet to be brought into force by the end of May 2022.

The Computer Crime and Cyber Crime Act, 2022[4], criminalises offences committed against and through the use of computer systems and electronic communications networks. Whilst mechanisms to protect citizens against criminal and terrorist elements that emanate from the use of the internet are necessary, there is a danger and risk that this can be misused by governments to curtail freedom of expression on the internet, which has implications such as the shrinking of online civil society spaces. Among the concerns expressed is that the law has the potential to be interpreted in a way that targets vocal human rights defenders, media practitioners and activists. The regulations of the law are yet to be developed.

The Data Protection Act, 2022[5], is a law that provides for the collection, processing, disclosure and protection of personal data and other matters. Data protection is imperative as internet usage increases. There are entities that collect and store people's personal data for commercial and other purposes, such as monitoring internet user's online habits and preferences. The law also includes provisions for third parties who collect data with consent. Furthermore, the law covers the protection and confidentiality of particular categories of personal data, such as health information.

The Electronic Communications and Transactions Act, 2022[6], is for the purpose of regulating electronic transactions, electronic communications and the use of e-government services, amongst others. This law is considered important in enabling the country's fourth industrial revolution, which coincides with rising levels of internet use. Furthermore, with increasing roll-out and penetration of e-commerce and other digital platforms, it has become imperative for countries to implement laws to regulate such platforms and technologies to protect users.

Cybercrime law flagged

Long before it became law, when it was first mooted in August 2020, the then Computer Crime and Cyber Crime Bill stirred controversy when it was announced that it would also "include an item to criminalise the posting of so-called "fake news" on the internet, potentially covering any story that is considered by the royal authorities as damaging to the kingdom's image"[7].

2 https://allafrica.com/stories/202110160242.html

3 https://www.esccom.org.sz/legislation/

4 https://www.gov.sz/images/ICT/COMPUTER-CRIME--CYBER-CRIME-ACT.pdf

5 https://www.gov.sz/images/ICT/DATA-PROTECTION-ACT.pdf

6 https://www.gov.sz/images/ICT/ELECTRONIC-COMMUNICATIOACT.pdf

7 http://country.eiu.com/article.aspx?articleid=1800140563&Country=Eswatini&topic=Politics&subtopic=Forecast&subsubtopic=Political+stability

In early September 2020 it was reported that the bill would carry heavy fines and jail sentences for "Facebook abusers" and "fake news perpetrators"[8]. At the same time it was reported that the secretary general of the opposition People's United Democratic Movement (PUDEMO), Wandile Dludlu, labelled the bill as "draconian" and that "it was intended to silence people expressing their views" online. Also at that time, the president of the Eswatini National Association of Journalists (SNAJ), Welcome Siyabonga Dlamini, expressed the hope that the proposed law "was not intended to muzzle the media or victimise individuals considered holding dissenting views or beliefs from those of the government".

A year later, in November 2021, as the bill passed the final stages of enactment in the Eswatini parliament, the country's Deputy Prime Minister, Themba Masuku, was reported to have come out in defence of the bill, stating that the intent behind it was not "nefarious" and that it was "not meant to target some Emaswati" at a time of political and social unrest[9].

How this law interacts with and impacts the Data Protection Act, 2022, will be discussed in a forthcoming article. ■

Ndimphiwe Shabangu is a development practitioner working for the Coordinating Assembly of NGOS (CANGO) in Eswatini. Additional reporting was done by Frederico Links.

8 http://www.times.co.sz/news/129721-e10m-fine-for-facebook-abusers-fake-news-perpetrators.html

9 http://new.observer.org.sz/details.php?id=17271

Arrests mar Malawi's **digital rights landscape**

JIMMY KAINJA

Two recent cases point to concerning state surveillance practices and the undermining of free expression online.

There are multiple issues affecting digital rights in Malawi. Recent instances of the use of state surveillance apparatus for repressive purposes and prosecutions, compounded by a lack of data and online privacy protections and low internet penetration and usage have heightened fears that the country is regressing in terms of safeguarding online rights. The environment is impacting both ordinary citizens and online journalists.

This report will expand and provide detailed discussions on these issues, starting with internet access and affordability, the lack of data protection and, finally, surveillance.

Surveillance

Data centralization paves the way for state surveillance, and in Malawi, evidence of state surveillance is emerging. Between 2021 and 2022, over eight people have been arrested, and two of them have been convicted for their various online activities. However, one thing that stands out from these arrests is that those detained had allegedly offended influential people in the country, including the State President, a Member of Parliament and one of the big banks.

The most recent case concerns Chidawawa Mainje who was arrested on 1 May 2022 over a WhatsApp political conversation[1]. Mainje was charged under section 86 of the Electronic Transactions and Cyber Security Act of 2016 for allegedly insulting Malawi's President. WhatsApp has end to-end-encryption, which means this discussion was not open to the public, yet the police moved in to arrest an individual over a private conversation.

One exceptional case of this is the arrest of investigative journalist Gregory Gondwe for his journalistic work[2] (please see image 1). It is clear from Gondwe's own account of events surrounding his detention[3] that the police had been tracking his conversations, most likely aided by the fact that mandatory SIM Card registration in the country is linked to the national ID. Additionally, the confiscation of his mobile phone by the police suggests a clear case of surveillance, although not through covert means. A few weeks later, the Platform for Investigative Journalism website, where Gondwe's work is published, was hacked by State operatives[4], according to Gondwe and his colleagues.

These arrests could have a chilling effect on citizens who could become scared to participate in online conversations. The environment is particularly problematic for a country with low internet usage, where authorities should rather encourage wider internet access and use.

---

1 Voice of America, Malawi Police Arrest Nurse for Harassing President Online: https://www.voanews.com/a/malawi-police-arrest-nurse-for-harassing-president-online-/6554047.html

2 MISA Malawi, Hacking of Platform for Investigative Journalism Website not a Mere Coincidence: https://malawi.misa.org/2022/04/15/hacking-of-platform-for-investigative-journalism-website-not-a-mere-coincidence/

3 See Gregory Gondwe's Facebook post in this issue: https://web.facebook.com/GREGORY.GONDWE?_rdc=1&_rdr

4 Constitution of the Republic of Malawi: http://www.sdnp.org.mw/constitut/dtlindx.html

Journalist Gregory Gondwe (left) leaving the police station where he was detained for hours – photo credit, Jonathan Pansungwi.

Privacy and data protection

The Constitution of the Republic of Malawi protects privacy under Section 21. It says, "every person shall have the right to personal privacy, which shall include the right to be subjected to - (a) searches of their person, home or property; (b) the seizure of private possessions (c) interference with private communications, including mail and all forms of telecommunications.[5]"

In the absence of a data protection law, the Government of Malawi has, in the last five years, embarked on a mass data collection through the national biometric ID for those 16 years and older.

Yet, it is worth noting that Malawi also lacks a data protection law, particularly for the digital age, which is critical in ensuring safety and protection online. The right to privacy intersects with other fundamental rights, such as freedoms of expression, assembly and association. In the absence of data protection, the safety of people's data and the right to privacy is not guaranteed. In the absence of a data protection law, the Government of Malawi has, in the last five years, embarked on a mass data collection through the national biometric ID for those 16 years and older.

Since its implementation in 2018, the national ID has become the only form of identification for all public transactions, including voter registration, mandatory SIM Card registration, banking, MRA, farming subsidies, cash transfers, and Covid-19 vaccinations. Implementing the national ID means people's data is centralised through the ID system.

Access and affordability

Internet access is increasing in Malawi, although access remains very low. According to a 2019 national survey on access and use of ICTs by households and individuals in Malawi, only 14.6% of Malawians have access to the internet[6]. The 14.6% does not include the quality and level of access, given that among this, some can only afford specific social media bundles. The country's telecommunications regulator, the Malawi

5 The Constitution of the Republic of Malawi

6 The National Household Survey on Access and Usage of ICT Services in Malawi: http://www.nsomalawi.mw/index.php?option=com_content&view=article&id=232:national-household-survey-on-access-and-usage-of-ict-services-in-malawi-2019&catid=3:reports

Communications Regulatory Authority (MACRA), is mandated[7] to ensure that "... so far as it is practicable, every citizen in Malawi must have access to sufficient, reliable and affordable communication services."

The low level of internet access cited above[8] shows that the MACRA has fallen short of fulfilling this mandate. In addition to the low internet access, only 9.3% of internet users are in rural areas, where most of the population lives. Of those with access to the internet, 12.4% are female, and 15.4% are male. A significant number of Malawians (46%) say they don't use the internet because they don't know what it is – 2.4% say they don't use it because it is too expensive.

It is recognized internationally that people must access secure, stable, reliable, and trustworthy internet to enjoy their digital rights. Achieving this requires infrastructure, including reliable electricity and reliable mobile network connectivity. A 2019 GSMA report found that 72.6% of Malawi has mobile network coverage, and according to Freedom on the Net 2021, mobile connectivity in Malawi is usually "slow, sluggish and unreliable.[9]"

Jimmy Kainja is a lecturer in media, communication and cultural studies at Chancellor College, University of Malawi. His main areas of interest are new media and new technologies, journalism and freedom of expression in relation to governance and civil liberties.

7 Communications Act, 1998: https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/mw/mw019en.html

8 Ibid

9 Freedom House, Freedom on the Net, 2021: https://freedomhouse.org/country/malawi/freedom-net/2021

New surveillance regulations lurk **threateningly in Namibia**

The measures attack anonymity online and undermine the constitutional right to privacy.

FREDERICO LINKS

Two recent cases point to concerning state surveillance practices and the undermining of free expression online.

Namibia has become the latest African country to introduce mandatory SIM card registration and data retention regulations that will have a far-reaching impact on online privacy and data protection in the country.

On 28 April 2022, barely days before World Press Freedom Day 2022 was marked under the theme 'Journalism Under Digital Siege', conditions to be imposed on internet and telecommunications service providers were gazetted.

The newly gazetted regulatory conditions[1] followed from the gazetting of regulations under Part 6[2] of the Communications Act of 2009 on 15 March 2021.

Part 6 of Namibia's Communications Act[3] provides the enabling framework for wide-ranging telecommunications surveillance by the state, but has never been officially operationalised since the law was passed almost 13 years ago, because regulations for implementation had not been finalised in all that time.

The Part 6 regulations and conditions come at a time when Namibia is still busy formulating and drafting a data protection bill, a process that has also been ongoing for more than a decade.

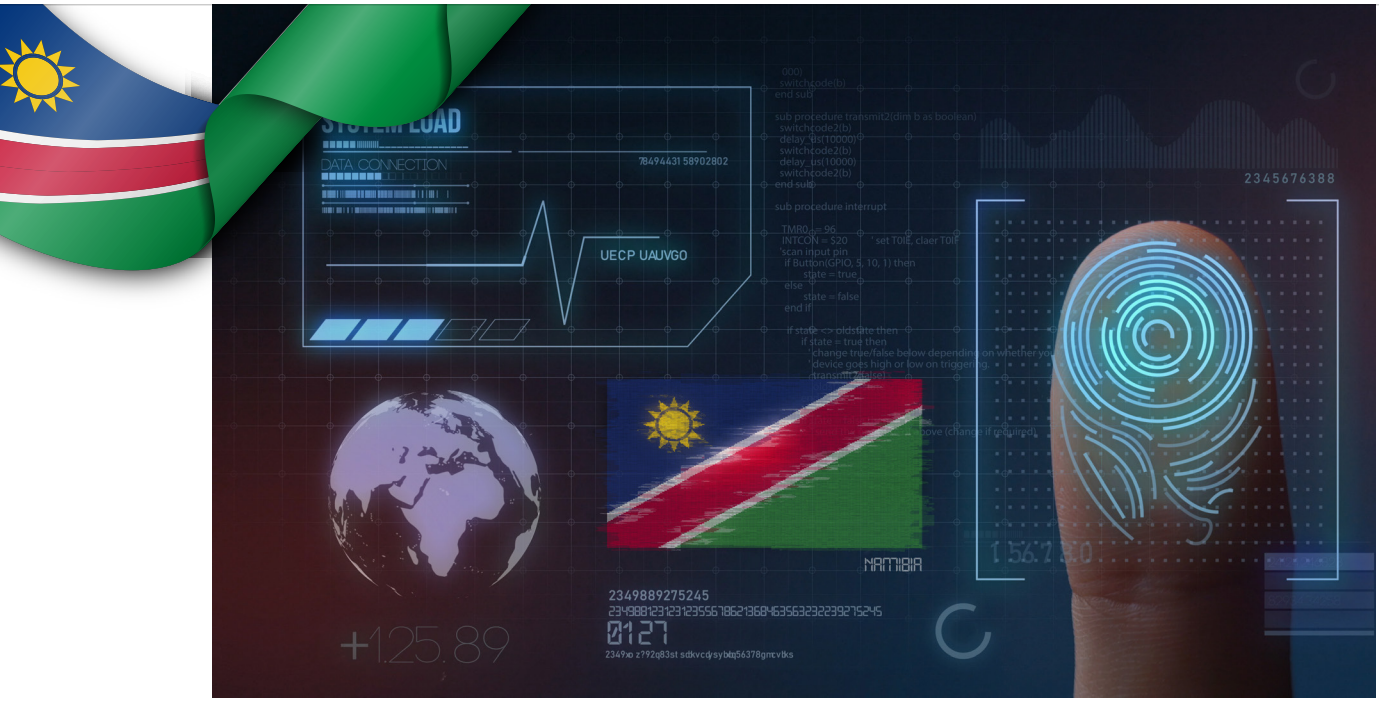
However, while the Part 6 regulations and conditions have been gazetted, they have not been implemented as the directives, issued by the Minister of Information and Communication Technology (MICT) and the Communications Regulatory Authority of Namibia (CRAN), that set the operationalising date had not been issued yet by end May 2022.

The regulatory conditions and their potential threat to data and online privacy first came to light in October

1 https://drive.google.com/file/d/1jAQyI7eiuuRAjhxY0k4EE-A-FFGnOnwe/view

2 http://www.lac.org.na/laws/2021/7481.pdf

3 https://www.lac.org.na/laws/annoSTAT/Communications%20Act%208%20of%202009.pdf



2021, following reports of discussions[4] of the then draft conditions between the Communications Regulatory Authority of Namibia (CRAN) and telecommunications and internet service providers.

The regulations and conditions have come as Namibians appear to be highly suspicious of state communications surveillance practices.

The eighth round of the Afrobarometer survey[5], from 2019, found that almost exactly 60% of respondents "agree with" or "very strongly agree with" the statement that people "should have the right to communicate in private without a government agency reading or listening to what they are saying".

The threats

The danger that the Part 6 regulations and conditions pose to online and data privacy was articulated by the executive director of the Ministry of Information and Communication Technology (MICT), Mbeuta Ua-Ndjarakana in an official communique[6] issued on 26 October 2021, in which he stated: "The benefits of SIM card registration is that it eradicates anonymity of communications, which aids in legal surveillance and interception."

The eradication of anonymity of communications is to be achieved through two ways that are extensively prescribed in the Part 6 regulations and conditions – through mandatory SIM card registration and data retention by telecommunications and internet service providers.

When selling and registering a SIM card or registering a customer for an internet connection, telecommunications service providers would be required to collect all sorts of identifying information or data from the customer.

The customer information to be collected is: the full name of the customer, the residential address of the customer; and the Namibian identity or passport or driving licence number of the customer.

In terms of data retention, telecommunication and internet service providers would also be required to store all telecommunications and internet traffic of all users for a period of five years.

The regulations and conditions mean that mobile phone and internet users in Namibia will all be instantly and permanently identifiable and trackable – the definition of continuous bulk or mass surveillance.

This sort of surveillance environment will probably have the effect of stifling critical media reporting[7], as it enables the easy identification of journalistic sources and whistleblowers, as well as undermining lawyer-client or doctor-patient confidentiality, to point out just some of the obvious threats to sectors where privacy, anonymity and confidentiality are highly prized.

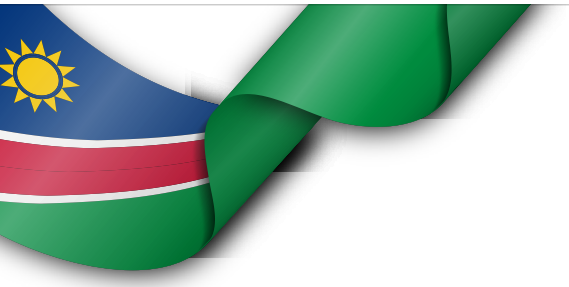
---

4 https://www.namibian.com.na/6214602/archive-read/Civil-society-warns-against-Govt-phone-spying

5 https://www.afrobarometer.org/wp-content/uploads/2022/02/afrobarometer_sor_nam_r8_en_2019-12-03.pdf

6 https://drive.google.com/file/d/1bn9NaAgSyJoQgzm_kp4gNNrRobxw95QU/view

7 https://ispeak.africa/fearless-journalism-under-threat/



The eradication of anonymity of communications is to be achieved through two ways that are extensively prescribed in the Part 6 regulations and conditions – through mandatory SIM card registration and data retention by telecommunications and internet service providers.

A legal response

For Namibian public interest law firm, the Legal Assistance Centre (LAC), there's one important question swirling around the Part 6 regulations and conditions, and that is "whether Namibia's requirements for telecommunications data collection and retention might be unconstitutional"?

In a policy brief[8] published around the time the conditions were being discussed and finalised, the LAC answered this question by stating "the scheme needs to comply with basic data protection principles – including measures pertaining to the security of the data and protections for confidentiality and the prevention of unauthorised access, as well as provision for the erasure or destruction of data after the requisite time period for its retention has expired".

The legal assessment concludes that "it seems likely that Namibia's telecommunications data retention scheme might be found to be an unconstitutional infringement of the right to privacy overall, given the intrusion into the privacy of large segments of the population in a manner that has a questionable ability to serve the intended objectives".

The LAC assessment of the emerging Namibian surveillance environment echoes sentiments and concerns expressed by former UN special rapporteur on freedom of expression, David Kaye, in a report submitted to the UN Human Rights Council[9] in May 2015.

Kaye states of broad data retention regulations, such as those now on the verge of being rolled out in Namibia, that they "limit an individual's ability to remain anonymous. A State's ability to require internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint."

He adds that a "State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information".

The special rapporteur's report concludes, among others, that "Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity".

The report goes on to state that because "of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective".

It is these principles that civil society organisations, such as the LAC and the Institute for Public Policy Research (IPPR), an independent Namibian think-tank which has for years been sounding the warnings on the looming threats of increased state surveillance powers through law and regulation, have been citing to advocate for transparency and accountability around state surveillance measures and mechanisms in order to minimise the avenues for surveillance abuse and overreach.

As the Namibian state moves to implement the Part 6 regulations and conditions, these CSOs and others are looking to increase their advocacy engagements around the emerging state surveillance environment. ■

Frederico Links is a freelance journalist and a governance researcher with the Institute for Public Policy Research (IPPR) in Namibia and the Namibia Media Trust (NMT).

8 http://www.lac.org.na/projects/grap/Pdf/constitutionality_of_telecommunications_data_retention_schemes.pdf

9 https://www.ohchr.org/en/calls-for-input/reports/2015/report-encryption-anonymity-and-human-rights-framework

Lungu law looms dangerously **over Zambian digital rights**

SUSAN MWAPE

The previous administration brought in a cyber crime law that weaponised the internet.

With elections looming in August 2021, earlier in the year, then Zambian president Edgar Lungu signed into law a batch of cyber or online laws, one of which has remained especially problematic into 2022[1].

The three laws that Lungu signed in March 2021 were the Cyber Security and Cyber Crimes Act of 2021[2], the Data Protection Act of 2021[3] and the Electronic Communication and Transactions Act of 2021[4].

The most contentious of the three new laws, the Cyber Security and Cyber Crimes Act, attracted criticism from politicians and civil society actors even before it was enacted and after it was signed into law. To many observers the quick enactment of the law appeared to be a thinly veiled attempt at orchestrating social media regulation and clamping down on Zambians' online political expression under the guise of ostensibly fighting cyber crime. This was because president Lungu, in the run-up to the passing of the law and his signing it, had been vocal about dealing with "people who abuse social media"[5].

A week after the Cyber Security and Cyber Crimes Act was signed, then leading opposition presidential candidate and now Zambian president, Hakainde Hichilema, indicated that he would prioritise the repeal of the law once elected[6].

Around the same time, five Zambian civil society organisations (CSOs) approached the Zambian High Court to have the law declared unconstitutional, and in early April 2021, the Media Institute of Southern Africa (MISA) Zimbabwe chapter – that serves as the MISA Regional secretariat – issued a statement in support of the Zambian CSOs[7]. The legal challenge ultimately proved unsuccessful.

In its statement in support of the court action brought by the Zambian CSOs against the Cyber Security and Cyber Crimes Act, MISA Zimbabwe stated: "The enactment of the Cyber Security and Cyber Crimes Act has a chilling effect on freedom of expression, media freedom and Zambians' right to privacy. The Act falls far short of regional and international standards and instruments on human rights such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo

1 https://www.znbc.co.zm/news/president-lungu-signs-cyber-security-bill/

2 https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%202%20of%202021The%20Cyber%20Security%20and%20Cyber%20Crimes.pdf

3 https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%203%20The%20Data%20Protection%20Act%202021_0.pdf

4 https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%204%20of%202021%2C%20The%20Electronic%20Communications%20and%20Transactions_0.pdf

5 https://www.znbc.co.zm/news/social-media-abusers-irk-lungu/

6 https://www.lusakatimes.com/2021/03/29/hh-sets-repealing-cyber-security-and-cyber-crime-bill-as-number-one-priority-once-elected/

7 https://misa.org/blog/misa-meets-government-officials-in-botswana-over-the-criminal-evidence-procedure-controlled-investigations-bill/

Among some of the other major issues of contention around the three new laws at the time was that many stakeholders felt excluded from the consultative processes.

Convention), which sets the standards for cybersecurity and personal data protection laws as well as capacity building, knowledge exchanges and experience sharing among signatories."

Among some of the other major issues of contention around the three new laws at the time was that many stakeholders felt excluded from the consultative processes. Furthermore, the hasty manner in which the laws were passed raised a lot of suspicion, and CSOs accused the Lungu government of planning to use the laws to stifle dissenting views, while opposition political parties said the cyber laws were the most controversial pieces of legislation passed since the country's independence[8].

Since early 2022 there has been a push from within Zambian civil society, led by Bloggers of Zambia, to re-ignite efforts to repeal the Cyber Security and Cyber Crimes Act[9].

In March 2022, the Bloggers of Zambia, in collaboration with Nigeria-based Paradigm Initiative, held talks with Zambian CSOs and parliamentarians about the state of digital rights in the country and especially the potential impacts of the Cyber Security and Cyber Crimes Act on such rights. Following these engagements the chairperson of the Zambian parliament's standing committee on media and ICT, Raphael Mabenga, indicated that the committee was open to receiving amendment proposals for the Cyber Security and Cyber Crimes Act from CSOs[10].

In a report from March this year, Mabenga was quoted saying that "there were some clauses in the Cyber Security and Cybercrimes Act, which was enacted in a fast paced and secretive manner in 2021, [that] need to be corrected to make the law responsive to people's needs".

In a meeting in March 2022 with Zambian president, Hakainde Hichilema, Amnesty International secretary general, Agnes Callamard, also called for the repeal of the Cyber Security and Cyber Crimes Act[11], and in mid-May 2022, Hichilema announced that his government would review the law with a view to either revising or repealing it[12].

The political context

In the past, under the Lungu government, the state had censored online content by blocking websites, which could only be accessed using virtual private networks (VPNs)[13]. On occasions, journalists, politicians and private citizens found themselves in trouble after having their private conversations recorded and publicly exposed.

The widespread state surveillance appeared a real threat when in 2019 the government announced the establishment of a cyber security squad to tackle cyber crimes and digital platform abuse. Following this, the Zambian government acquired CCTV camera systems that were mounted around the capital city, Lusaka, to support the state surveillance efforts.

At the time the Cyber Security and Cyber Crimes Act (2021), the Data Protection Act (2021) and the Electronic Communication and Transactions Act (2021) were enacted and signed into law, Zambian civic space had been shrinking and become severely restricted. Media houses that were critically reporting on the Lungu government were being shut down, and civil society activists were being threatened with arrest.

---

8 https://itweb.africa/content/6GxRKqYJKNlvb3Wj

9 https://www.aa.com.tr/en/africa/ahead-of-parliament-debate-rights-groups-stress-need-for-review-of-zambias-cyber-laws/2502489

10 https://www.znbc.co.zm/news/parliamentary-committee-ready-to-take-submissions-on-cyber-laws/

11 https://www.amnesty.org/en/latest/news/2022/03/zambia-amnesty-international-secretary-general-urges-president-hichilema-to-move-with-speed/

12 https://itweb.africa/content/GxwQD71DVkYvlPVo

13 https://cpj.org/2013/06/critical-website-blocked-for-four-days-in-zambia/

The Lungu government also used the COVID-19 pandemic as a pretext to limit gatherings by political opponents.

In June 2020, youths unhappy with the poor state of political governance under the Lungu government were prevented from holding a peaceful protest[14]. They were threatened with arrest and scores of police officers roamed the streets, as the youth activists defiantly declared that they would go ahead with the protest as planned. As the police combed the streets, the youth took their protest online, where they broadcast their grievances to the world. The online protest attracted over half a million engagements, which was considerably more support than what had been expected for the physical street protest event.

The Lungu government also used the COVID-19 pandemic as a pretext to limit gatherings by political opponents.

In view of the health crisis, the Electoral Commission of Zambia (ECZ) instituted a number of health measures in collaboration with the Ministry of Health to ensure that the spread of COVID-19 was minimized[15]. Key among the measures announced by the commission was a ban on traditional campaign rallies, a key feature of Zambian electoral processes.

In response, instead of holding large rallies in the run-up to the August 2021 general election, opposition political parties conducted mobile roadshows at which smaller groups of people could be hosted. However, the roadshows became mobile rallies that drew crowds that could not be contained and were eventually banned too by the ECZ. They were cited as potential major spreaders of COVID-19.

Opposition political parties criticized the decision by ECZ, pointing out that they were only banning opposition roadshows because they were attracting more supporters than the ruling party.

This was happening against the backdrop of incumbent president Edgar Lungu, who was also running as a presidential candidate, holding campaign events that drew large crowds, and looked to not be compliant with the COVID-19 health protocols.

As the general election drew near, it was observed that the internet became increasingly slow. This largely affected live streaming of online political campaign activities. Additionally, increasing electricity disruptions became a problematic feature to accessing the internet during this period. At the same time, the expiry period of data bundles meant that the costs of data bundles became significantly higher. Whenever there was no internet access or poor connection, or no electricity, citizens would incur huge data losses without any form of compensation.

In response to this situation, Common Cause Zambia, in collaboration with AccessNow's #KeepItOn campaign, wrote an open letter to then president Lungu urging him to ensure that the internet stayed on before, during and after the general election. Following the release of the letter, the permanent secretary in the Ministry of Information accused those suggesting there would be an internet shutdown of being alarmist and said that the government had no intention to shut down the internet.

A few days before the election, though, the same

14 https://diggers.news/local/2020/06/23/youths-dribble-police-as-they-take-protest-to-the-bush/

15 https://zambianews365.com/ecz-bans-campaign-rallies/

permanent secretary in the Ministry of Information issued a statement saying the government would shut down the internet if citizens did not behave themselves online.

Around noon on election day, the internet was partially shut down and social media platforms, such as Facebook, WhatsApp, Instagram, Twitter and some VPNs and other platforms were blocked[16].

A local CSO challenged the Zambia Information Communication Authority (ZICTA) in court for ordering mobile service providers to stop providing internet services and to block social media.

A local CSO challenged the Zambia Information Communication Authority (ZICTA) in court for ordering mobile service providers to stop providing internet services and to block social media. The court ordered the restoration of full services and the unblocking of platforms, and ZICTA agreed to not act outside its legal authority going forward[17].

At the time of writing, despite committing to review and revise or repeal the Cyber Security and Cyber Crimes Act, the Hichilema administration still had to make substantive moves in that direction. The existing limitations contained in the cyber laws passed in early 2021 remain a threat, especially in the absence of adequate checks and balances.

With the internet being a critical tool for many, not just civil society and the media, it can only be hoped that the new government will follow through on its stated intention of revising the Lungu laws of 2021.

Future digest contributions from Zambia will spotlight in greater detail the issues raised in this introductory article. ■

Susan Mwape is the founder and executive director of Common Cause Zambia (CCZ). She contributed to this article on behalf of MISA Zambia. Additional reporting was done by Frederico Links.

16 https://www.accessnow.org/shutdown-in-zambia-on-election-day-how-it-affected-peoples-lives-and-wellbeing/

17 https://allafrica.com/stories/202108150063.html

Affordable connectivity and privacy violations **plague Zimbabwe**

OTTO SAKI

NOMPILO SIMANJE

A complex range of issues are impacting the exercising of digital rights in the country.

Zimbabwe remains one of the countries in Southern Africa with expensive internet access and various factors contribute to this including the macro-economic policies, unstable currency and political interests. Due to the hyperinflationary environment, limited access to foreign currency and also the taxation of the telecommunications industry, it is therefore difficult for citizens to enjoy affordable internet.[1] This has therefore continued to widen the digital divide in Zimbabwe particularly between people with low income levels and those with higher income levels and also between those in rural areas vis-a-vis those in urban areas.

The internet infrastructure is controlled by the private sector, though the government dictates and influences the pricing systems for telecommunications from voice, short messages services, to internet costs.2 The regulator of the telecommunications industry, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), is responsible for setting the prices of mobile data using its pricing index. Following public outcry in December 2021 over the high cost of data, POTRAZ highlighted that, "Our principle for tariff reviews have always been cost-based, hence as cost of service changes we always try to ensure that service provision is aligned to the costs incurred by the service providers."[3]

According to NewsDay, from 10 March 2021, the cost of 8GB of data was pegged at US$18, with 50GB of private internet data from Econet Wireless rising to US$47. In July of 2021, increases were recorded bringing the cost of 8GB to US$23, and 50GB rising to US$73.[4] The internet service providers bemoaned the "imposition of an additional 10% excise duty across all internet and VoIP packages effective 1 March 2022", which caused a substantial increase in the costs of data in March 2022.[5] Media groups raised concerns about this decision, which impacts on citizens' access to information and online participation.[6]

Following a petition submitted to Zimbabwe's parliament by MISA Zimbabwe, calling for internet

1 Enacy Mapakame, "Telcos record 247BN revenue in Q2", The Herald, October 12, 2021 https://www.herald.co.zw/telcos-record-247bn-revenue-in-q2/

2 https://www.newsday.co.zw/2021/09/the-internet-costs-in-zimbabwe-compared-to-southeast-african-countries/

3 https://www.zimbabwesituation.com/news/potraz-defends-data-tariff-hikes/

4 https://www.newsday.co.zw/2021/07/exorbitant-internet-costs-choke-zimbos/

5 https://itweb.africa/content/rW1xL759kpO7Rk6m

6 https://zimbabwe.misa.org/2021/10/28/increase-in-data-tariffs-impediment-to-access-to-information/

The monitoring of social media and the use of social media brigades has historically increased during sensitive political periods, such as in the run up to elections. Lawyers, human rights defenders, journalists, and opposition political activists are subjected to online harassment to silence legitimate criticism of the ruling party or government.

affordability in Zimbabwe, and a directive to POTRAZ by the Parliamentary Portfolio Committee, POTRAZ convened a multi-stakeholder meeting on 9-10 May 2022 under the theme, 'Ensuring operator viability and service affordability-the balancing act and challenges.' The meeting underscored that several stakeholders had a role to play to facilitate universal access to the internet, including the Reserve Bank of Zimbabwe, the Ministry of Finance, the Zimbabwe Electricity Supply Authority (ZESA) and the Ministry of Local Government.[7]

Most Zimbabweans access the internet through mobile data and what are called bundled packages specifically for social media platforms like WhatsApp, Twitter and Facebook, while others use private Wi-Fi bundles. According to POTRAZ director, Gift Machengete, data in Zimbabwe is pegged at 0.010 cents per megabyte which translates to US$10.00 per gigabyte.

Recently, on 19 May 2022, one of the mobile operators, Econet Wireless increased its data tariffs by 20 percent. The new prices of data are as follows:

GIGABYTES	PRICE ZWL	PRICE USD[8]
8GB	5184	17.87
15GB	7920	27.00
25GB	9432	32.52
50GB	14 400	49.66

While the above costs might seem cheaper in US dollar terms as compared to the previous months, what should be noted is that Zimbabwe is yet to dollarize and what has increased is the official exchange rate between the local currency and the US dollar. On the other hand, the income levels of the majority of citizens remain the same despite an increase in the cost of living and access to the internet. [9]

Residents of border towns are now relying on neighbouring countries' mobile internet services, which are cheaper and more reliable. A market for foreign SIM cards is therefore thriving in those areas.[10] As the country's economic situation deteriorates, the cost to connect to the internet will increase.

Online surveillance

Social media has become a site for political and social debates and has also been used for organising and mobilising politically.[11] Irked by rising online activism and internet-based organising, the government announced in November 2021, through the Ministry of Information, Publicity and Broadcasting Services, that it set up a social media monitoring unit.[12] The Minister of Information, Monica Mutsvangwa, was quoted saying: "We have actually come up with a cyber-team that is constantly on social media to monitor what people send and receive since we cannot wish social media away."

While no further information was provided about the unit and the monitoring tools they use, what is clear is that

---

7 http://easterntimeszim.org/2022/05/11/ict-parliamentary-portfolio-slams-finance-ministry-rbz/

8 At official rate of 1:290 as at 30 May 2022

9 Zimbabwean teachers strike amid pandemic and high inflation, AP News , https://apnews.com/article/coronavirus-pandemic-business-health-africa-pandemics-0d70cfa5d5b6c23c3826498e331d3378

10 https://restofworld.org/2022/black-market-sim-cards-zimbabwe-border-work-hub/

11 Many social movements groups used hashtags to organise such as #This Flag or #ShutdownZim (2022)

12 https://www.newsday.co.zw/2021/11/govt-sets-up-team-to-monitor-social-media/

there is some form of mass surveillance of social media and social media users in Zimbabwe, which appears to be a violation of the right to privacy online.

The monitoring of social media and the use of social media brigades has historically increased during sensitive political periods, such as in the run up to elections (Zimbabwe has general elections in 2023).[13] Lawyers, human rights defenders, journalists, and opposition political activists are subjected to online harassment to silence legitimate criticism of the ruling party or government.[14]

The Cyber and Data Protection Act

In December 2021, Zimbabwe enacted the Cyber and Data Protection Act, which also amended the Criminal Law Codification and Reform Act, the Criminal Procedure and Evidence Act and the Interception of Communications Act. The law provides a comprehensive framework on data protection and privacy, by including the rights of data subjects, regulating the processing of sensitive data and also providing for notification in the event of a security breach.[15] The law therefore codifies the right to privacy as provided for in Section 57 of the Zimbabwe Constitution.

The law also establishes the Data Protection Authority, by mandating POTRAZ to establish conditions for the lawful processing of data. Since February 2022, POTRAZ has started implementing the provisions of the law,[16] by requesting all data controllers and processors, that hold or process the data of more than 30 people, to provide information on the following:

- What data was collected and processed and for what purpose;
- Whether a data protection officer was appointed and the professional credentials of the appointed officer;
- The address of the data controller and proof of residence.

The protection of personal data and information remains contested, as the Zimbabwean government has several data centres in the country, since before adopting the data protection law, raising concerns of unauthorised access to personal data.[17]

Arrests for online conduct

The Cyber and Data Protection Act has already been used to prosecute individuals for online conduct with two people having been arrested for cyberbullying. Cyberbullying is defined as "unlawfully and intentionally by means of a computer or information system, generating and sending any data message to another person or posting any material whatsoever on any

13 Charles Moyo 'Social media, civil resistance, the Varakashi factor and the shifting polemics of Zimbabwe's social media "war" Global Media Journal 2019

14 https://www.aa.com.tr/en/africa/zimbabwean-regime-shifts-oppression-to-social-media/2146273

15 https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/

16 https://businesstimes.co.zw/potraz-enforces-data-protection-act/

17 https://www.herald.co.zw/new-dawn-for-zim-as-president-launches-data-centre-to-anchor-govt-operations/

electronic medium accessible by any person, with the intent to coerce, intimidate, harass, threaten, bully or cause substantial emotional distress or to degrade, humiliate or demean the person of another.....”

On 19 May 2022, a Nyanga resident was charged with cyberbullying for allegedly using foul language to describe the Zimbabwean ambassador to Tanzania and his wife in a WhatsApp group.[18]

On 24 May 2022, television actor David Kanduna was reported to have been arrested and fined for cyberbullying after recording a police officer being jeered at one of the local universities and posting the video to WhatsApp and Tik Tok.[19]

Concerning these cases and the definition of cyberbullying, the danger is that the Cyber and Data Protection Act may have resuscitated criminal defamation, which was outlawed by the Constitutional Court in 2014.

A 23-year-old woman, known for marketing sex toys on TikTok, Twitter and Facebook, was also arrested on 16 May 2022 for allegedly exposing children to pornographic material and violating the Customs and Excise Act.[20]

Internet slow down

On 20 February 2022, the Citizens Coalition for Change political party was officially launched in the Highfields area of Harare, in the run up to by-elections scheduled for 26 March 2022.

Netblocks recorded a significant slow-down of the internet on the day, which limited access to online coverage of the launch and the sharing of videos and images on social media platforms.[21]

POTRAZ indicated that the government had not throttled the internet in any way on the day and instead said that a technical issue had been caused by the large number of people at the launch attempting to access the internet at once.[22]

MISA Zimbabwe criticised the internet slow-down and highlighted that internet connectivity should not be unjustifiably restricted so that people can exercise their right to access information and also exercise political rights, especially during election periods.[23]

The issues spotlighted clearly indicate that there is a need for further advocacy to promote digital rights. There are several factors, some legal, some political and some economic, that continue to impact the exercising of rights online, particularly free expression, the right to privacy and access to information. At the same time, with the enactment of the Cyber and Data Protection Act, Zimbabwe is one of only nine countries in southern Africa with such a framework. ■

Otto Saki is a human rights lawyer with an interest in digital rights, technology, political economy and health rights. Nompilo Simanje is the Legal and ICT Policy Officer at the Media Institute of Southern Africa, Zimbabwe Chapter.

---

18 https://www.zimbabwesituation.com/news/former-army-chief-cyber-bullied/

19 https://www.hmetro.co.zw/television-actor-kanduna-fined-for-cyber-bullying/?fbclid=IwAR3iGx_Ddgs39xl-BjvGrt73S6gad-4ifKhsH8amYDDISOer86T8BPNt8ro

20 https://www.herald.co.zw/dildo-vendor-in-trouble/?fbclid=IwAR16o52aY5z6RH6H7RlTuH2Sv71d0TG917D-Q8FH_7O4Et3NsDKJvTt4LQo

21 https://netblocks.org/reports/internet-slowdown-limits-coverage-of-zimbabwe-opposition-rally-oy9Ykoy3

22 https://bulawayo24.com/index-id-news-sc-national-byo-215629.html

23 https://www.newsday.co.zw/2022/02/misa-blasts-yellow-sunday-internet-slowdown/

digital rights SOUTHERN AFRICA

MISA BOTSWANA · CANGO Change · Growth · Empowerment · MISA MALAWI · nmit FREE SPEECH FOR AFRICA · MISA ZAMBIA · MISA ZIMBABWE

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS · OSISA Open Society Initiative for Southern Africa · AFRICAN DECLARATION ON INTERNET RIGHTS AND FREEDOMS