



DIGITAL RIGHTS AND INCLUSION IN AFRICA

A PARADIGM INITIATIVE PUBLICATION

**Digital rights violations
continue across the
African continent**

**Health surveillance in
the midst of COVID-19,
a breach of privacy**

20

**Reports from
across the African
continent**

2020 REPORT



DIGITAL RIGHTS AND INCLUSION IN AFRICA

A PARADIGM INITIATIVE PUBLICATION

Published by Paradigm Initiative

374 Bomo Way, Yaba, Lagos, Nigeria

Email: media@paradigmhq.org

www.paradigmhq.org

Published in April 2021

Report produced by Paradigm Initiative

Design & Layout by Luce Concepts

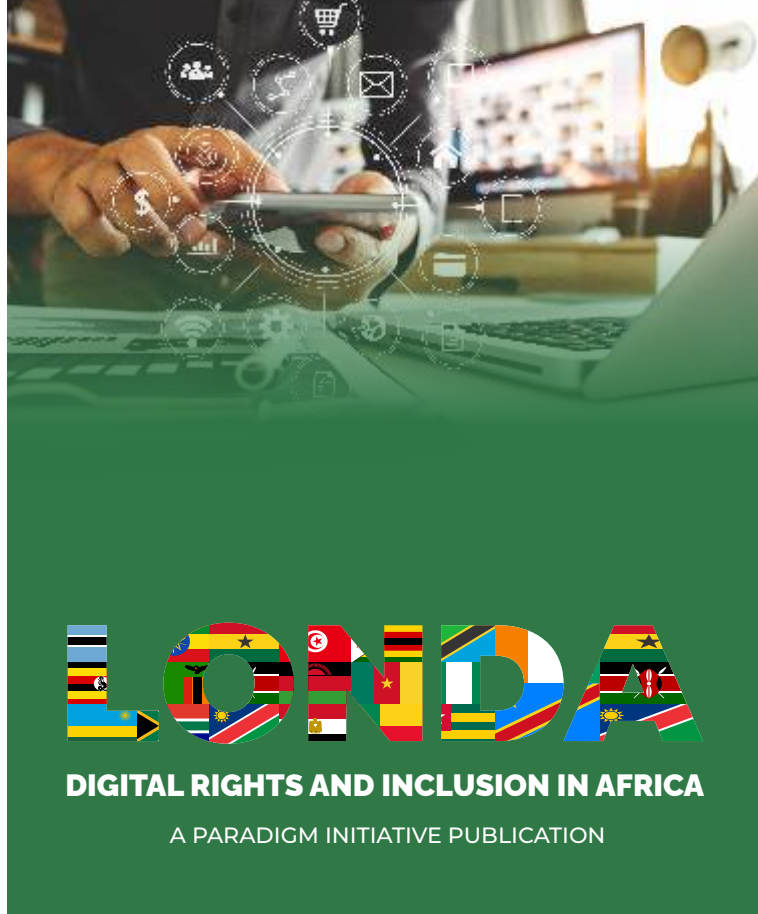
This publication maybe reproduced for non-commercial use in any form provided due credit is given to the publishers, and the work is presented without any distortion.

Copyright © 2021 Paradigm Initiative



Creative Commons Attribution 4.0 International (CC BY 4.0)

ISBN: 978-978-992-319-9



CONTENTS

ACKNOWLEDGEMENTS	i
INTRODUCTION	ii
BENIN	1
BOTSWANA	5
CAMEROON	14
COTE D'IVOIRE	23
DRC	27
EGYPT	31
ETHIOPIA	38
GHANA	44
KENYA	50
MALAWI	58
NAMIBIA	64
NIGERIA	72
RWANDA	86
SOUTH AFRICA	93
TANZANIA	103
TOGO	108
TUNISIA	115
UGANDA	120
ZAMBIA	126
ZIMBABWE	133
CONCLUSION	145

Civil society organizations continue to work to advance digital rights and inclusion in Africa, ensuring best practices are adopted into policy and legislation. This report analyses the state of digital rights and inclusion in Africa, examining violations and gaps, investigating the use and application of policy and legislation, highlighting milestones and proffering recommendations for the digital landscape in Africa. This edition captures among other issues, the digital divide worsened by the COVID-19 pandemic and unearths infractions on different thematic areas such as privacy, access to information, and freedom of expression with the legislative and policy background well enunciated.



ACKNOWLEDGEMENTS

This report features country reports authored by digital rights experts from various African countries. Paradigm Initiative is grateful for their contributions which are aimed at documenting and analysing digital rights and inclusion events and policies across Africa. The support received from our funding partners is greatly appreciated and ensures that we continue to advance digital rights and inclusion. We are truly grateful for the support of the editorial team who have ensured we deliver on this project through their review and advice.

Contributors:

Abdul Rahman Alfa Shaban - Ethiopia country report
Adeboye Adegoke and Judith Takon - Nigeria country report
Anonymous - Tanzania country report
Apolo Kakaire - Uganda country report
Bulanda Nkhowani - Zambia country report
Donald Flywell Malanga - Malawi country report
Ekai Nabenyo - Kenya country report
Jean-Pierre Afadhali - Rwanda country report
Konan Angan Maurice Constant - Cote d'Ivoire country report
Michael Gyan Nyarko - Ghana country report
Mohamad Farahat - Egypt country report
Nashilongo Gervasius - Namibia country report
Oarabile Mudongo - Botswana country report
Providence Baraka - DRC country report
Rigobert Kenmogne - Cameroon country report
Seyram Adiakpo - Togo country report
Sinatou Saka - Benin country report
Thobekile Matimbe - Zimbabwe country report
Tina Power - South Africa country report
Yosr Jouini - Tunisia country report

Editorial Team:

'Gbenga Sesan
Kathleen Ndongmo
Koliwe Majama
Margaret Nyambura Ndung'u
Mawaki Chango
Nnenna Paul-Ugochukwu
Thobekile Matimbe

Copy Editor:

Sabine Matsheka

Translators:

Paper Bag Africa (English/French)
Bonface Witaba (English to Swahili)

Design & Layout

Luce Concepts





LONDA DIGITAL AND INCLUSION IN AFRICA REPORT

INTRODUCTION

One of the defining events of 2020 was the global COVID-19 lockdowns. Although this was a time in which governments required heightened trust, in order to work with everyone to flatten the curve of the coronavirus, some African governments were criticised for using COVID-19 as an excuse to pursue various clampdown agendas.

In some cases, citizen pushback led to the improvement of policy proposals. For example, South Africa published regulations making it an offence to publish any disinformation, through any medium, about COVID-19 and contact tracing methods adopted by the government were debated before the regulations incorporated several important privacy safeguards, including user notification and an express provision that the interception of the content of communications is not permitted. In Botswana, there were concerns that the government's use of COVID-19 contact tracing technology lacked consistent, accountable and open oversight structures.

A letter from the Office of the President of Cameroon, in April 2020, instructed the Director of the National Agency for Information and Communication Technologies to monitor social media accounts in order to identify users disseminating fake news but this led to new mechanisms of intimidation, violations and restriction of freedoms. Zimbabwe enacted a statutory instrument that punishes any person who communicates falsehoods with up to 20 years' imprisonment, and there were concerns that the law had criminal defamation provisions that restrict freedom of expression. Alarmingly, the

Egyptian government dealt with the information that was circulating about the pandemic as fake news which led to many citizens, including journalists, lawyers, and civil society activists, being subjected to prosecution for allegedly spreading fake news.

During the year under review, several African countries made changes to existing laws, introduced new laws or concluded ongoing law making processes. In April 2020, the Parliament of Botswana passed emergency laws that gave the President full authority to govern for six months by decree, while in November 2020, a new telecommunications law replaced the 2002 law on Post and Telecommunications in the Democratic Republic of Congo. The parliament of Ghana passed the Right to Information Act in March 2020, which was assented by the President in May 2020, meanwhile Kenya appointed a Data Protection Commissioner in November 2020. Even though a proposal to regulate social media was said to have divided members of the Namibian parliament in 2019, the country's Ministry of ICT confirmed plans to regulate social media in February 2020. Nigeria's National Assembly hosted a public hearing, in March 2020, on the "Protection from Internet Falsehood and Manipulation Bill," which proposed

to give the Nigerian government the power to restrict access to internet services and determine the falsity or otherwise of information shared by citizens on digital platforms. In July 2020, South Africa's Draft Films and Publications Amendment Regulations caused an uproar, with concerns that the regulations were draconian and an attempt to censor the internet. The Parliament of Togo also passed a new digital identification law that defines the legal framework for biometric identification data collection, and in May 2020, Zimbabwe's Cyber Security and Data Protection Bill was gazetted, which was followed by the Freedom of Information Bill that was gazetted in July 2020.

Digital rights violations continue across the countries covered by this report, including Benin, Botswana, Democratic Republic of Congo, Egypt, Ethiopia, Ghana, Malawi, Namibia, Nigeria, Rwanda, Tanzania, Tunisia and Zambia. Apart from the indiscriminate arrest of journalists and other citizens, this report documents data privacy violations, internet shutdowns, lack of oversight for security agencies, mass surveillance, online gender-based violence, clampdown on peaceful protesters, invoking defamation laws to punish dissent and the use of ambiguous COVID-19 regulations as an opportunity to punish dissenting voices.

Since the COVID-19 pandemic began, digital technologies have become increasingly essential to everyday life across Africa. With day-to-day activities moving online, connectivity has become imperative to keep the world moving. This transition and for some, lack thereof, has further exposed the widening digital divide and growing vulnerability of under-served communities across the continent. Unsurprisingly, issues of affordability and access during the pandemic, impacted children, women, youth, people with disabilities, refugees and other vulnerable groups

the most. When schools and offices closed across most countries, many African citizens paid a huge price for the lack of reliable and affordable internet access.

Students were expected to learn online in places without adequate infrastructure or the economic means for such access. The need for remote work and schooling also revealed other worrying divides such as a growing gender divide across many African countries. For example, despite the number of women in Botswana's ICT industry, the sector remains male-dominated. However, countries, such as Ghana, made significant strides in closing the gender-digital gap, with one study suggesting that the gender-digital gap sits at 5.8%, far below the global average of 21%.

Similar to other countries across Africa, in Kenya, three main bottlenecks to closing the gender-digital divide include affordability, relevance and lack of digital skills amongst women and girls. The country's digital infrastructure is less robust and there is a rural-urban divide and gender digital exclusion in some parts of the country. Only 31% of Namibian public schools have access to the internet but the country has launched a National Broadband Policy with a five year implementation action plan that seeks to achieve 95% broadband coverage by 2024 and also operationalise the Universal Access and Service Fund. In Egypt, one of the most vulnerable groups, the refugee community, faced further exclusion due to the pandemic, as many could not access the new distance learning system due to lack of internet access, absence of devices, cost of access and refugee identity documents not being recognised by Internet Service Providers. In Tunisia, students were granted free access to educational platforms but public schools did not provide online platforms. Most Zambian institutions of learning battled to cope with delivering online lessons due to

prohibitive costs, lack of access or ownership of gadgets, unavailability of adequate e-learning platforms in some institutions and limited digital literacy skills for both teachers and learners. Digital exclusion is also widening the inequality gap in Zimbabwe through the absence of adequate access to digital technology and connectivity to the internet.

In spite of this, 2020 also saw some African countries recording developments that could promote and protect digital rights. In addition to developments in Namibia and Ghana, telecommunications companies across many African countries worked with governments to create awareness about staying safe during, and after, the coronavirus lockdowns. Ghana launched its Digital Financial Services Policy in May 2020, to improve financial inclusion through the use of digital platforms.

Additionally, in November 2020, Kenya appointed a Data Protection Commissioner and Malawi's Access to Information Act of 2016 became operational on September 30, 2020.

Civil society organizations continue to work to advance digital rights and inclusion in Africa, ensuring best practices are adopted into policy and legislation. This report analyses the state of digital rights and inclusion on the continent, examining violations and gaps, investigating the use and application of policy and legislation, highlighting milestones and proffering recommendations for the digital landscape in Africa. With reports from 20 countries, this edition captures among other issues, the digital divide worsened by the COVID-19 pandemic and unearths infractions on different thematic areas such as privacy, access to information, and freedom of expression with the legislative and policy background well enunciated.



***This report analyses the state of
digital rights and inclusion on the continent,
examining violations and gaps, investigating the
use and application of policy and legislation,
highlighting milestones and proffering
recommendations for the digital
landscape in Africa.***





AFRICA REPORT






Bordered to the North by Niger, to the East by Nigeria, to the west by Togo and to the South by the Atlantic Ocean, Benin is situated at the center of Western Africa. The country is structured into 12 regions, with a land area of 114,764 km².

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN BENIN

Benin opened up to the world of the internet during the sixth summit of the Heads of States and Governments of the Francophone in November 1995.¹ Today, the mobile 3G internet covers an average of 60% of the population, (The Master Plan for ICT and telecommunications in Benin, June 2017). According to the statistics published by ARCEP, the internet penetration rate is 48,02%.

According to the Association of Developers and Coders in Benin, there are between 500 and 600 developers. In 2017, Benin's Internet Development Index (IDI) was 1.94, placing the country at number 161 globally, behind Togo, Mali, Senegal and the Ivory Coast. Benin's mobile connectivity rate for the year 2017 was 37.3. As for the Network Readiness Index, Benin is 128th globally out of 139 countries with an index of 2.9 in 2016.

 **60%**
of the population
is covered by the
mobile 3G internet

INTERNET INFRASTRUCTURE

After its adoption in 2016, the Sector Policy Statement (SPS)² became the digital roadmap in Benin. According to national authorities, on high and highest speed, a

1. <https://www.google.com/url?q=https://cursus.ebsi.umontreal.ca/vol6no1/bai.html%23~:text=3DL%27histoire%2520d%27Internet%2520a,couvrire%2520les%2520activit%25C3%A9s%2520du%2520Sommet&sa=D&source=editors&ust=1617863321683000&usg=AOvVaw0O3uL3QW8t4dFEZHmeaPv9>

2. Sector Policy statement – Strategic orientations 2021 in the digital economy sector: <https://numérique.gouv.bj/images/DPS.pdf>

network of more than 2000km of fiber optics has been put in place in 60 of the 77 municipalities.

According to official sources, the incumbent operator, Benin Telecom Infrastructures (BTO) has reduced its costs by 50% on average on capacity and 40 commune capitals have a capacity of 50 Mbps with the establishment of three services namely: Community digital points, free Wi-Fi terminals in certain public places with a capacity of 4 Mbps and a subscription service for individuals with a capacity of 36 Mbps.

INTERNET LEGAL FRAMEWORK

Law n° 2017-20 of April 20 2018 on the digital code in Benin is the only legal anchoring of the digital sector in Benin since 2018. The Digital Code deals with electronic communications, networks and services. It sets the rules applicable to operators and electronic communications activities. Electronic tools and documents, the rules applicable to trust service providers are also guided by this code, which also lists the provisions applicable to the protection of personal data and those relating to Cyber Crime and Cyber Security.

Compared to Law no° 2014 of July 9 2014, the scope of the current law on the Digital Code is broader. Not only does it contain the updated provisions concerning activities relating to electronic communications networks, services and personal data, but it also sets out the legal rules applicable to electronic commerce and communication, cybercrime and domains previously characterised by a legal vacuum. It regulates the criminal law applicable to crimes and offences committed online.

In its last report, the ARCEP (Regulatory Authority for Electronic Communication and the Post)

stipulates that network neutrality is a legal principle in the republic of Benin. “Operators providing internet access do not apply traffic management measures”. In essence, they must refrain from blocking, slowing down, modifying, restricting, degrading or discriminating against content, applications or specific content and application services.

The protection of privacy is also of great interest to the Beninese legislator. The Personal Data Protection Authority (APDP) exists to ensure the solicitation of legal provisions relating to the protection of personal data. Since its creation in 2009, it has only supplied 300 authorisations for the collection or deletion of personal data and registered around ten complaints.



FREEDOM OF EXPRESSION ON THE DIGITAL PLATFORMS

For the first time in the country's history, the internet was cut off all day during the legislative elections, on the April 28 2019.

“The decision to shut down access to the internet and social media on the day of elections is a direct violation of the right to freedom of expression”, affirms Francois Patuel, West Africa Researcher at Amnesty International.

Former journalist, Aziz Imorou was arrested on September 17 2020³ after posting an article on Facebook in which he denounced an alleged act of aggression against himself by a bodyguard of Armand Ganse, Director General of the Société de Gestion des Marchés Autonomes (SOGEMA), the state-owned company that manages public markets. He told the West Africa Media Foundation that he was assaulted by Mr. Ganse's bodyguard while taking pictures of a vehicle that hit a commercial motor cyclist. Whilst he was taking those photos, four people assaulted him and snatched his mobile.

A day after the publication on Facebook, Aziz Imorou was summoned to the Central Office for the Repression of Cyber Crime (OCRC) following the complaint filed by the Director of SOGEMA. After questioning him, Aziz Imorou was brought before a court of first instance in Cotonou. Without rendering a judgement, the judge returned the accused to Cotonou Civil Prison for defamation. The court released him for the benefit of the doubt on October 6 2020.

This is not the first case in the country. The Benin prosecutor, Mario Metonou, initiated the arrest, prosecution and imprisonment of Ignace Sossou, a journalist at Benin Web TV in December 2019.⁴

The prosecutor complained that a tweet, from the journalist claiming to quote words spoken at a conference, was incorrect. Imprisoned on December 24 2019, Ignace Sossou was released on June 24 2020 after a successful appeal against his 18-month prison sentence.

On July 8 2020, the High Authority of Audiovisual and Communication of Benin issued a statement, threatening websites to “put an end to all publications”. The latter would not have the publication authorization granted by the regulatory body.

This decision comes at a time when several press officials, having requested their publication authorization for several months, have never received a response from the HAAC. This move in particular would limit the spread of fake news on the internet.

According to Jeune Afrique, a spokesperson for the Beninese High Authority for Audiovisual and Communication (HAAC), evokes the imperative obtaining of a prior authorisation to claim the status of media support, notably via “inquiries of morality” the content of which is totally unknown and especially if these surveys are carried out by independent persons.

***The Personal Data Protection
Authority (APDP) exists to ensure the
solicitation of legal provisions relating
to the protection of personal data.***

3. https://www.google.com/url?q=https://www.24haubenin.info/?Le-journaliste-Aziz-Imorou-arrete&sa=D&source=editors&ust=1617864857954000&usg=AOvVawOnne_l1HsaFWp_2MPlyZtl

4. https://www.google.com/url?q=https://www.liberation.fr/planete/2020/01/23/journaliste-beninois-emprisonne-ce-qu-il-s-est-passe-est-une-aberration_1774894/&sa=D&source=editors&ust=1617863321688000&usg=AOvVawlwuzTJaLBwzblGVHcVXKN

HITIMISHO NA MAPENDEKEZO



The year 2020 was characterised by the arrest of two journalists for their online activity. The latest decision of the High Authority for Audiovisual and Communication, constitutes a regression of fundamental freedoms online.

From a technical standpoint, the recently launched standardized billing platform, the interfacing between mobile money and banks, the interoperability platform for government information systems and the launch of more than 250 e-services, are as many examples which testify to the progressive centrality of the Internet in the daily life in Benin. Digital Rights, linked to freedom of expression, to the quality and technical robustness of infrastructures, in terms of security, should be at the heart of Benin's digital transformation, as the expert Pierre Dandjinou reminds us.

Also, the 2016 activity report of the former CNIL Bénin (current APDP) indicates that: "for most cases, the illegalities observed here and there in the abusive appeals relating to the collection and manipulation of personal data personnel, derive their source from the ignorance of the texts which frame the matter and that is risky".

It would therefore be wise, as the lawyer Christine Tossavi recommends, to increase the protection of personal data in companies by updating the labor code to take into account the use of IT tools and updating the knowledge of labor inspectors and magistrates on the application of the Benin digital code. Collaboration between the APDP and the Directorate General of Labor would be a great asset in preserving the employee's right to privacy in the digital age.

The existing legal framework must not become more politicized to the detriment of citizens and Internet users. All citizens must be equal before the law, no one can use a legal provision for his own interests.

Digital Rights, linked to freedom of expression, to the quality and technical robustness of infrastructures, in terms of security, should be at the heart of Benin's digital transformation.

”

PIERRE DANDJINOU



Botswana is a landlocked country in Southern Africa.

According to the latest United Nations data, Botswana's population is estimated at 2.3 million.¹ It is one of the most sparsely populated country in the world.

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN BOTSWANA

As of March 2020, the country experienced an increase of 4 million mobile phone subscribers and a 1.3 million increase in mobile money subscriptions.² Mobile money is used by many consumers as a cheaper way to transfer money and to bridge existing financial gaps.³ Although the government has made considerable progress and investment in rolling out fiber optic cable, Botswana's broadband demand has seen a significant rise in the user market, with a high volume of mobile broadband traffic reported at 242 percent between 2017 and 2018.⁴

According to Internet World Stats, in September 2020 the number of internet users was over 1.1 million.⁵ Between 2019 and 2020, there was a slight increase of 23,000 users (+2.1 percent).⁶ Access to digital skills, affordable and quality internet connectivity remains unevenly distributed in Botswana. Due to a lack of statistical evidence, there seems to be no precise figures measuring the country's digital divide.



4 Million
mobile phone
subscribers

1. Worldmeter, Botswana Population, <https://www.worldometers.info/world-population/botswana-population/>

2. Botswana Communication Regulatory Authority statistics, <https://www.bocra.org.bw/telecoms-statistics>

3. Research ICT Africa, After Access Survey (2018), Comparative Report, https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

4. BOCRA (2020), "Broadband Facts and Figures",

<https://www.bocra.org.bw/sites/default/files/documents/Mar%2029%202020%20Final%20BB%20Facts%20and%20Figures.pdf>

5. <https://www.internetworldstats.com/stats1.htm>

6. Digital 2020: Botswana, <https://datareportal.com/reports/digital-2020-botswana>

The cost of 1GB is USD 5.84 (BWP64,34),⁷ considered too be high, which means that many people continue to be excluded from the internet space.⁸

ICT INFRASTRUCTURE AND POLICY LANDSCAPE

Botswana Communication Regulatory Authority (BOCRA) is the country's communications regulator, formerly known as the Botswana Telecommunication Authority (BTA). Botswana's communications sector consists of five divisions: telecommunications, Internet and ICTs, radio communications, broadcasting and postal services. The sector has four network operators, three of which operate under a Public Telecommunications Operator (PTO) license (BTC, Mascom, and Orange).⁹ BoFiNet, the fourth entrant, focuses primarily on the distribution of wholesale telecommunications services to customers. In contrast, the rest of the operators focus on converging network telephony services, such as mobile data. Launched in 2007, Botswana's first blueprint, the Maitlamo National Strategy for ICT Development, directs the country to use ICTs while driving national development efforts.¹⁰ It is expected that this policy will transform Botswana from a manufacturing economy to an innovation-driven and accelerated digital economy.¹¹



Although digital literacy and data protection were key concerns regarding internet use in Botswana that lacked a policy response, both were recognised in the ICT Policy (2007) and in the Broadband National Strategy (BNS) launched in 2018 as crucial issues needing policy guidance.¹² Section 5 of the BNS, for example, discussed the effect of these policies on digital rights and addressed concerns related to data privacy and internet security.¹³ Striving to reach its development agenda to become one of the leading regional ICT hubs in the Southern Africa region, Botswana has invested in its futuristic innovation centre (Botswana Innovation Hub).¹⁴ Such advances in ICT and internet technology have driven the government to implement policies for e-governance and led citizens in the digital transition of public service delivery.¹⁵

7. Research ICT Africa Mobile Pricing (RAMP), https://researchictafrica.net/ramp_indices_portal/

8. https://researchictafrica.net/polbrf/Research_ICT_Africa_Policy_Briefs/2017%20Policy%20Brief%201_Botswana%20.pdf

9. Botswana Communication Regulatory Authority, ICT Licensing Framework in Botswana, https://www.bocra.org.bw/sites/default/files/documents/ICT%20Licensing%20Framework_0.pdf

10. Republic of Botswana, Ministry of Communications, Science and Technology, Maitlamo: National Policy for ICT Development, https://publicadministration.un.org/unpsa/Portals/0/UNPSA_Submitted_Docs/2019/f912b59f-5963-4335-9dff-194a1a522c49/Maitlamo%20Policy_26112019_083359_d807e512-ea2e-4d56-8fba-60679904b985.pdf?ver=2019-11-26-083359-520

11. This policy builds into diversification of Botswana's economy. The policy aims at "diversifying Botswana's economy from heavy dependence on mining to other sectors."

12. Botswana National Broadband Strategy, <https://www.bocra.org.bw/sites/default/files/documents/National-Broadband-Strategy-FINAL%28June2018%29.pdf>

13. Communications Regulatory Authority Act of 2012 deals with some aspects of network security (See in this regard section 56 of the Act that seeks to protect networks by outlawing the damaging or obstruction of construction or maintenance of communications networks), it does not provide for a comprehensive framework for network security.

14. Bloomberg, Africa's Diamond Capital Invest in a Futuristic Innovation Hub, <https://www.bloomberg.com/news/articles/2020-09-18/in-africa-a-silicon-valley-style-tech-hub-emerge>

15. Republic of Botswana, Botswana national e-government strategy, http://staging.nationalplanningcycles.org/sites/default/files/country_docs/Botswana/egovstrategy.pdf

Botswana also notes the importance of ICT infrastructure development and technology as an essential factor in implementing its e-governance policy. Embracing projects driven through Public-Private Partnerships (PPP) have shown great success in achieving digital transformation government goals. For instance, Botswana Telecommunications Corporation (BTC) and Mascom Wireless' Ntelelsa flagship project targeted villages linked to telephony and internet networks.

Moreover, in 2010, Botswana Post also founded Kitsong Centres (rural telecommunications development programme).¹⁶ For economic acceleration, this PPP model and projects have transformed citizens' lives in rural areas and the government to carry out its e-governance mandate to this day.¹⁷ However, available data shows that the overall level of electrical connectivity in rural areas of Botswana is 12% making this one of Botswana's key challenges in improving its ICT infrastructure and connectivity.¹⁸

While new creative concepts for increased internet access continue to be embraced by the telecommunications industry, the market rivalry remains unchallenged and one-sided. Other competitors do not actively contest the status quo; telecom service providers such as Mascom appear to dominate the market share. Mascom's market ownership was 55 percent from 2014 to 2016, while Orange retained 28 percent and BeMobile had an overall percentage of 17 percent.

Botswana is ranked 21 in a total of 49 countries across Africa providing the cheapest prepaid mobile voice products (Voice/SMS basket) (30 Calls/100 SMS) at USD5.88 (BWP 64.90) in Q2 2020, according to Research ICT Africa Mobile Pricing (RAMP) index. Botswana ranks 7th compared with other countries in the Southern Africa region.¹⁹



ONLINE FREEDOM OF EXPRESSION

Freedom of speech is protected by section 12 (1) of the Constitution of Botswana.²⁰ The country has been described as having an outstanding record for its long-standing democracy and political tolerance in Africa.²¹ However in June 2020, Botswana security agents detained two Weekend Post journalists accusing them of “common nuisance” for photographing a building connected to the Directorate of Intelligence and Security Services (DISS), the country's domestic and international intelligence agency.²² Although these journalists have been released after spending a night in a police cell, this act reflects an increasing press freedom violation in Botswana and targets media freedom.²³

16. https://media.africaportal.org/documents/technology_and_nature_active_citizenship.pdf

17. Critical Success Factors For e-Governance Projects: The Case of Botswana, <https://ibimapublishing.com/articles/JEGSBP/2018/335906/335906.pdf>

18. https://inis.iaea.org/search/search.aspx?orig_q=RN:38031492

19. Research ICT Africa, Botswana Telecommunication limp a decade after policy change, <https://researchictafrica.net/2017/02/23/botswana-telecommunications-limp-a-decade-after-policy-changes/>

20. Charles Manga Fombad, “The Protection of Freedom of Expression in the Public Service Media in Southern Africa: A Botswana Perspective”, Vol. 65, No. 5 (Sep., 2002), pp. 649-675, <https://www.jstor.org/stable/1097611>

21. Philomena Apiko, “Botswana: One of Africa's most stable democracies, but where are the women?”, <https://ecdpm.org/talking-points/botswana-one-of-africas-most-stable-democracies-where-are-women/>

22. President Masisi and the illusion of change, <https://inkjournalism.org/2216/president-masisi-and-the-illusion-of-change/>

23. Committee to Protect Journalist (2020), “Journalists arrested, charged with 'nuisance' in Botswana”, <https://cpj.org/2020/06/journalists-arrested-charged-with-nuisance-in-botswana/>



Civil society has since expressed questions about the misuse of authority by state security and the use of diverse strategies and regulations that stifle press freedom.

Civil society has since expressed questions about the misuse of authority by state security and the use of diverse strategies and regulations that stifle press freedom. After de-campaigning against the Chief Justice for infringing their freedom of speech and demanding the independence of the judiciary, judges were dismissed in 2015.²⁴ There was also a case in 2015 in which, according to Section 16 (2) (a) of the Cybercrime and Associated Crimes Act,²⁵ journalist Daniel Kenosi was charged with “unlawful distribution of obscene material”. Since then, the Directorate of Public Prosecutions (DPP) indicated that they were hindered from investigating the matter and sought specialist support from abroad. This investigation was suspended thereafter.²⁶

To tackle misinformation and disinformation in Botswana, the publication of false information is punishable by law under Section 59 of the Penal Code, which specifies that: “Any person who publishes any false statement, rumour or report which is likely to cause fear and alarm to the public or to disturb the public peace is guilty of an offence”.²⁷ Latest media reports have accused the Botswana government of arresting opposition members and journalists for their online activities.²⁸ A British journalist was also convicted under the same statute even though the allegations were subsequently dismissed.²⁹ These cases illustrate how Section 59 can be used ruthlessly to threaten, but with little intention of equal trial and prosecution.

24. Amnesty International, ‘Suspension of judges in Botswana potentially threatens freedom of expression and judicial independence’, 10 July 2017, accessible at <https://www.amnestyusa.org/press-releases/suspension-of-judges-in-botswana-potentially-threatens-freedom-of-expression-and-judicial-independence/>

25. Freedom House (2017) Freedom of the Press 2016/Botswana, <https://freedomhouse.org/report/freedom-press/2016/botswana>

26. DPP seeks external help on Daniel Kenosi case, <https://www.sundaystandard.info/dpp-seeks-external-help-on-daniel-kenosi-case/>

27. <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/61336/92021/F138317428/BWA61336.pdf>

28. Botswana government accused of arresting opposition members and journalists, <https://www.enca.com/news/botswanas-govt-accused-arresting-opposition-members-journalists>

29. Botswana drops case against british journalist, <https://www.independent.co.uk/news/botswana-drops-case-against-british-journalist-1157355.html>

The Botswana government should recognise the Declaration of Principles on Freedom of Speech in order to uphold the freedom of expression clause.³⁰ Principle 3 and 37 describe “freedom of expression and access to information on the Internet” as an individual human right, and pillar of democracy.

Botswana does not have existing regulations towards fake news, but strict liability provisions are imposed, it is the duty of the convicted party to show that what they have published is not false news.³¹

Any person who publishes any false statement, rumour or report which is likely to cause fear and alarm to the public or to disturb the public peace is guilty of an offence

SECTION 59 OF THE PENAL CODE

DATA PROTECTION AND DIGITAL IDENTITY

The 2014 African Convention on Cyber Security and Personal Data Protection imposes signatories’ commitments to developing legal, political and legislative mechanisms to facilitate cyber-security governance and cybercrime regulation.³² Botswana is one of 14 African Union (AU) member states that have signed the convention. However, the Data Protection Act (2018) which was passed by the Parliament of Botswana, has not applied yet to protect the data and privacy of people in Botswana.³³

Sections 48 (1) and 49 (1) of the Data Protection Act 2018 (DPA) on the transborder flow of personal data says: “the transfer of personal data to other countries is prohibited” and, without prejudice to Section 48, “the transfer of personal data that is undergoing processing or intended processing, to a third country may only take place if the third country to which the data is transferred ensures an adequate level of protection”.³⁴ Legislation and regulation are critical in ensuring the rights of citizens online are protected from cybercrime and the unauthorised use of personal data. Both the Botswana Electronic Communications and Transactions Act (2014) and the 2018 Data Protection Act (DPA) require a compromise to ensure that they are adequately enforced without violating citizens’ freedoms online and discouraging state apparatus from silencing dissent or spying on citizens.

30. <https://africaninternetrights.org/en/declaration>

31. Media Institute of Southern Africa, <https://zimbabwe.misa.org/2020/06/01/covid-19-fake-news-laws-being-used-to-stifle-free-speech/>

32. African Union convention on cyber security and personal data protection, <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

33. <https://www.endcode.org/post/does-botswana-have-a-data-privacy-law>

34. Data Protection Act 2018, <https://www.bocra.org.bw/sites/default/files/documents/32%20Act%2010-08-2018-Data%20Protection.pdf>

In 2017 the new multi-biometric ID platform in Botswana that operates all identification operations for various government ministries came into effect. The Government of Botswana signed a new agreement between the Botswana Police Service (BPS) and Safran Identity & Security, a giant leader in identity and security solutions, through its division Morpho South Africa. The system upgrade comes as the government's legacy system AFIS (Automated Fingerprint Identification System) was retired to a new one offering fingerprint and facial recognition features.³⁵

Botswana recently deployed smart CCTV cameras with facial recognition features and capabilities to alert the police and make it easy to identify those that commit crime.³⁶ Although it is arguably possible to classify this surveillance network as more advanced, both the technology sector and the government are the main drivers of its technological deployments in the country. In 2018, the Botswana Police Service signed a Memorandum of Understanding (MoU) with Huawei to deploy CCTV surveillance cameras through the Safe City projects.³⁷ Botswana has no general laws to regulate the use of data gathered from CCTV surveillance by state agencies and now with a tainted private-partnership contract with Huawei, a global technology company known for its questionable record towards privacy and human rights,³⁸ such advances can only have chilling implications on the future of Botswana's digital rights, online freedom and personal privacy.

Media sources reported that under the leadership of then-President Ian Khama, DISS and the Military Intelligence Unit (MIU) were alleged to have acquired state-of-the-art surveillance equipment, including spying capabilities from an Israeli based company on the internet and telephone in the run-up to the 2014 general election.³⁹



In February 2015, leaks disclosed that DISS had invested USD 64.7 million to a German corporation, classified documents revealed that DISS had installed FinSpy Mobile and FinSpy PC to track opposition political rivals, journalists and government critics.⁴⁰ Subsequently, due to a lack of oversight and responsibility, these actions have potential and daring consequences of violating human rights, personal privacy and freedom of information.

35. IDEMIA (2017), "Government of Botswana selects Morpho South Africa to provide a single multi-biometric platform for all the identification requirements of various government departments", <https://www.idemia.com/press-release/government-botswana-selects-morpho-south-africa-provide-single-multi-biometric-platform-all-identification-requirements-various-government-departments-2017-05-02>

36. The Patriot, "F/town gets crime-monitoring cameras", <http://www.thepatriot.co.bw/news/item/7315-f-town-gets-crime-monitoring-cameras.html>

37. Xinhuanet (2019), "Huawei project in Botswana to help reduce crime incidents: official", http://www.xinhuanet.com/english/2019-08/27/c_138340372.htm

38. Samuel Woodhams (2020), "Huawei says its surveillance tech will keep African cities safe but activists worry it'll be misused",

<https://qz.com/africa/1822312/huaweis-surveillance-tech-in-africa-worries-activists/>

39. Khama/Kgosi network of shady intelligence security big shots has DISS over a barrel, <https://www.sundaystandard.info/khama-kgosi-network-of-shady-intelligence-security-big-shots-has-diss-over-a-barrel/>

40. Botswana Guardian (2015), "DIS launches massive surveillance operation", <http://www.botswanaguardian.co.bw/news/item/1284-dis-launches-massive-surveillance-programme.html>

COVID-19, PRIVACY AND HUMAN RIGHTS

In several African nations, the spread of the COVID-19 pandemic has had a significant socio-economic effect. The Botswana government has adopted radical measures, including social distancing and strict lockdown regulations, to stop the transmission of COVID-19.⁴¹

In April 2020, the Parliament also passed emergency laws that gave the President full authority to govern for six months by decree.⁴² These policies pose an immense danger and empower the government to potentially misuse their authority, and this could erode respect for human rights and digital rights.⁴³

The United Nations High Commissioner for Human Rights (UNHCR) has called for human rights to be at the forefront of the state's response to the COVID-19 pandemic.⁴⁴ There is a need for the government to take adequate steps to protect human rights while fighting the pandemic.

In July, the government launched the first of its kind, BSafe mobile application, a QR code contact tracing tool donated by a local firm, Brastorne Enterprises,⁴⁵ the first of its kind in the region.⁴⁶ Without checks and balances on these measures and tools, there are concerns that these may potentially violate personal privacy and other human rights.

GENDER AND ACCESS TO THE INTERNET

The African Declaration on Internet Rights and Freedoms (African Declaration)⁴⁷ and the Feminist Principles of the Internet (FPI),⁴⁸ provides for the rights of all citizens and calls for affordable and equal access to the internet, free from the oppression of any sort. Despite the number of women in the ICT industry increasing in Botswana, this sector remains male-dominated.⁴⁹ The full extent of the gender digital divide in Botswana is difficult to ascertain, especially given the lack of gender-disaggregated ICT data.⁵⁰ However, the gender digital divide in Botswana is, as the majority of other African countries, a cause for concern.



41. Democracy Works Foundation, "Assessing COVID-19 Response Measures - Botswana", <https://democracyworks.org.za/assessing-the-measures-at-country-level-case-of-botswana/>

42. Censorship, the unexpected side-effect of COVID-19, <https://mg.co.za/africa/2020-05-11-censorship-the-unexpected-side-effect-of-covid-19/>

43. Extraordinary powers need extraordinary protections, <https://privacyinternational.org/news-analysis/3461/extraordinary-powers-need-extraordinary-protections>

44. Office of the High Commissioner for Human Rights. (2020, 6 March). Coronavirus: Human rights need to be front and centre in response, says Bachelet. <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25668&LangID=E>

45. African Countries Growing App-etite for Coronavirus Apps get Mixed Results, <https://thecorrespondent.com/598/african-countries-growing-app-etite-for-coronavirus-apps-gets-mixed-results/78359490924-b6a9fec3>

46. Morgan Meaker, "African Countries Growing Appetite for Coronavirus gets mixed results", The Correspondent, 20 July 2020, <https://thecorrespondent.com/598/african-countries-growing-app-etite-for-coronavirus-apps-gets-mixed-results/78359490924-b6a9fec3>

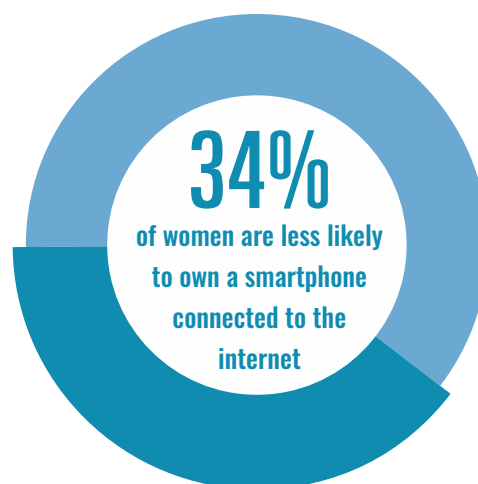
47. <https://africaninternetrights.org/declaration>

48. <https://feministinternet.org/en/principles>

49. Botswana Daily News, <http://www.dailynews.gov.bw/news-details.php?nid=19997>

50. Sey, A., & Hafkin, N. (2019). Op. cit.; see also APC. (2017). Op. cit., where it is noted that "representative and gender-disaggregated data should be gathered in a consistent and rigorous manner to reach a better understanding of the factors shaping women's access to and ability to benefit from meaningful internet access in diverse contexts."

For example, studies suggest that Africa has seen an increase in the gender disparity amongst internet users.⁵¹ With over 300 million off-line women in the Sub-Saharan region, Botswana appears to be part of this continental pattern.⁵² More recent research shows that 14 percent of women in the region are less likely to own a simple mobile phone, and 34 percent are less likely to own a smartphone connected to the internet.⁵³ In this sense, attempts to widen access and counter-current gender inequality, including the under-representation of women in leadership roles, must also be understood specifically in the field of internet governance.



CONCLUSION AND RECOMMENDATIONS



This study has revealed that the number of policies that regulate the use of digital communications, including the Internet, has been broadened by successive governments in Botswana since 1999. The state has sought to use legislation to legitimise activities that are otherwise unconstitutional to place limits and restraints on digital rights. Although laws in place are touted as important in order to curb cybercrime or enhance cybersecurity in the country, they have also been used to clamp down on opposition as well as quenching dissent.

While there are some indicators to increased access and use of ICTs in Botswana, the recent outbreak of COVID-19 pandemic could deepen the country's digital divide. The government's activities have largely undermined rather than facilitated, greater access to and affordability of digital technologies. In the absence of consistent, accountable and open oversight structures, new technological developments assessed in this study, including the use of COVID-19 contact tracing technology, lack in design data privacy consciousness, the reality that is likely to erode privacy rights, weaken the rule of law, strengthen impunity, and reduce the transparency of the state use of these tools. It may also suggest that these policies' consequences could continue for years to come unless all relevant stakeholders assess their long term impact.

In particular, this study also notes the deployment of CCTV surveillance networks by Botswana's government, which lacks transparency and legislation to regulate surveillance activities. Indeed, there is a need to continue pressing for transparency in this regard, including how CCTV surveillance networks operate and manage data.

51. Sey, A., & Hafkin, N. (2019). Op cit.

52. Mlambo-Ngcuka, P. & Albrechtsen, A. (2020, 6 May). Op-ed: We cannot allow COVID-19 to reinforce the digital gender divide. UN Women. <https://www.unwomen.org/en/news/stories/2020/5/op-ed-ed-phumzile-covid-19-and-the-digital-gender-divide>

53. OECD. (2018). Op. cit.



Data protection laws and regulatory standards for accountability and transparency, such as those outlined in this case study, may be able to mitigate some of the worst known privacy violations today, but as surveillance technology becomes more advanced and spreads into other fields, more work is required to protect human rights.

Civil society organisations need to collaborate by promoting internet freedom by lobbying, and public interest litigations that foster internet privacy for a desirable atmosphere that promotes the awareness and enjoyment of internet freedoms. Ensure that the legislation and regulations geared towards defending the right to privacy and personal data are considered when deploying CCTV surveillance systems for monitoring the movement of citizens which provide adequate protections and values, like ‘privacy by design’.

The Botswana government should establish regulatory and legislative measures to ensure accuracy and integrity in the gathering, storing, and analysing data gathered through the BSafe contact tracing app. Governments should have set in place mechanisms in this respect to ensure that sensitive data is safeguarded and not misused by unscrupulous people during COVID-19 crisis in order to breach human rights or to enforce programs for mass surveillance.

***The state has sought to use
legislation to legitimise activities
that are otherwise unconstitutional
to place limits and restraints
on digital rights.***



Cameroon, a bilingual country in Central Africa, has an estimated population of 27 million inhabitants.¹ The country has an estimated gross domestic product (GDP) of 479 billion FCFA over three years, including 180 billion in 2020.²

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN CAMEROON

ICT SECTOR AND POLICY

Over the past 20 years, Cameroon has adopted various laws and actions in the ICT sector. In 2016, the government adopted a strategy document for digital growth called the Cameroon Digital Strategic Plan 2020.³ The document identified the following eight strategic axes on which the government would base itself on in order to develop internet coverage in Cameroon:

- develop broadband infrastructure;
- increase the production and supply of digital content;
- ensure the digital transformation of administration and businesses;
- promote digital culture through the widespread use of ICT in society;
- strengthen digital confidence;
- develop a local digital industry and encourage research and innovation;
- ensure the development of human capital and digital leadership;
- and ensure the improvement of governance and institutional support.



**CAMEROON DIGITAL
STRATEGIC PLAN 2020**

1. https://fr.wikipedia.org/wiki/D%C3%A9mographie_au_Cameroun

2. <https://www.tresor.economie.gouv.fr/Pays/CM/ind%C3%A9t%C3%A9r%C3%A9s-et-conjoncture#:~:text=Le%20Gouvernement%20a%20pr%C3%A9sent%C3%A9%20un,interm%C3%A9diaire%20de%20la%20tranche%20inf%C3%A9rieure>

3. <https://localhostmmer.xyz/2020/08/18/plan-strategique-numerique-du-cameroun-2020/>

Several objectives were not achieved for cyclical and structural reasons. One of the priorities of the Ministry of Posts and Telecommunications set out in the 2020 Finance law⁴ is to increase qualitative and quantitative access and at a lower cost throughout the country. The indicator for this objective is the development of ICTs in Cameroon.

In Cameroon, 3G mobile coverage is estimated at a satisfactory rate of 69% with individual internet usage at 23% since 2018.⁵ Operators provide different network coverage including 5G. 5G coverage, the most popular one, covers less than a million users nationwide.⁶ According to a report published by Hootsuite and We Are Social as of January 2020, Cameroon had 7.8 million people connected to the internet. Cameroon's internet penetration rate reached 30% in January 2020,⁷ with an increase of 7.8%, estimated as 570,000 new internet users.

The country has four mobile operators, therefore three in the Global System for Mobile Communications (GSM), namely

- MTN,
- Orange,
- Nexttel
- and Cameroon Telecommunications (Camtel), the public mobile operator and the main intermediary provider of telephone and internet services.

MTN and Orange are the market leaders in terms of mobile subscribers, internet services, mobile transfer service and revenue. According to its latest report, MTN has more than 10 million subscribers in Cameroon, with a turnover of 5.6 billion in 2020.⁸

As part of the development of technological infrastructure, Cameroon has two internet exchange points, called CAMIX. The sale of internet services is carried out by around 20 internet access providers. In October 2020, the Minister of Posts and Telecommunications appointed CAMIX,⁹ an association therefore the members are operators and Internet Services providers as manager of exchange points in Cameroon, under the supervision of the Telecommunications Regulatory Agency (ART) and the National Agency for Information and Communication Technologies (ANTIC), two regulatory bodies for the ICT sector in Cameroon. Internet connectivity is provided by telephone operators and internet service providers of which 20 are privately owned.

Regulatory actors are at the centre of digital policy in Cameroon. The Ministry of Posts and Telecommunications coordinates all activities in the sector and is the main government institution responsible for ICT in the country. The Telecommunications Regulatory Agency (ART) is the regulator of the mobile telephony sector and internet connections. It has the power to sanction operations in case of violation of regulations. The National Agency for Information and Communication Technologies (NAICT) is also responsible for the promotion of ICT, the management of domain names (.cm) and fighting cybercrime. Digital legislation specific to the sector is described in the 2010 law on Electronic Communications.



7.8 Million
People connected
to the internet

4. <https://www.dgb.cm/news/consulter-loi-de-finances-cameroun-lexercice-2020/#>

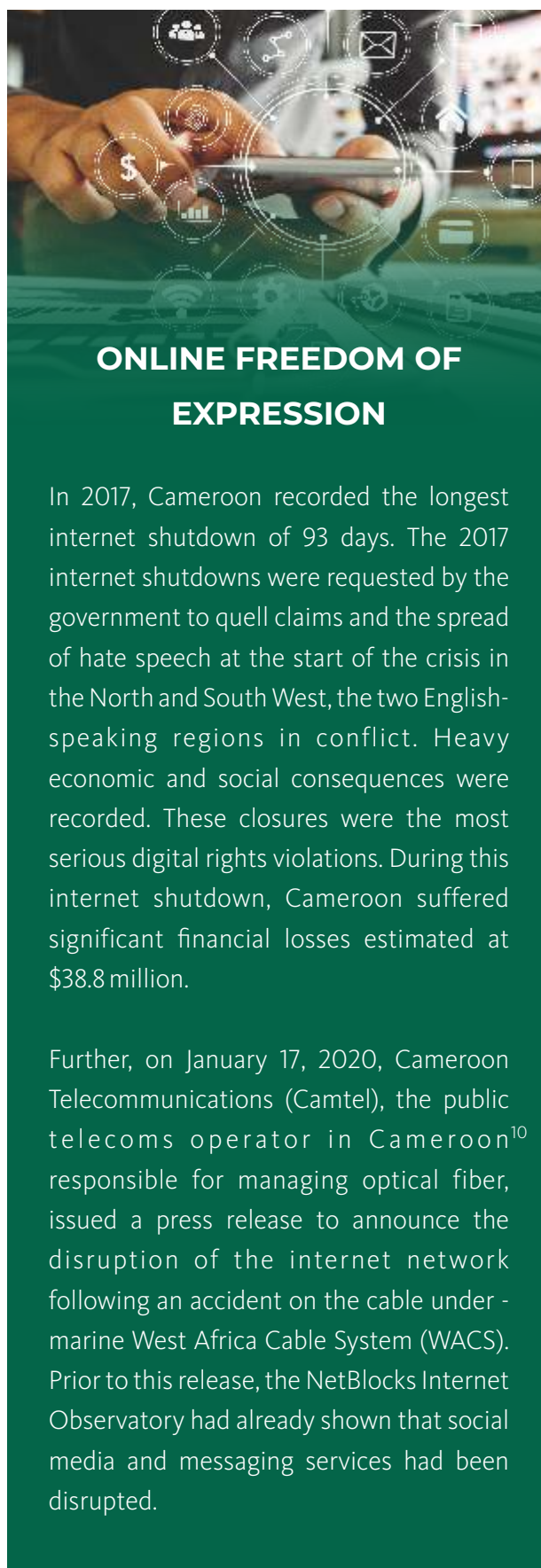
5. <https://www.nperf.com/fr/map/CM/-/-/signal/>

6. <https://www.nperf.com/fr/map/CM/-/449.MTN/signal/?ll=4.718777551249867&lg=9.953613281250002&zoom=6>

7. <https://www.investiraucameroun.com/economie/2402-14084-le-taux-de-penetration-de-l-internet-au-cameroun-atteint-30-en-2020-grace-al-arrivee-de-570-000-new-internet-users>

8. https://docs.google.com/document/d/1uJG-ZRCY6MsyXOB_NidENHjSfV8s4jh3jld_JvTo/edit

9. <http://www.camix.cm/>



ONLINE FREEDOM OF EXPRESSION

In 2017, Cameroon recorded the longest internet shutdown of 93 days. The 2017 internet shutdowns were requested by the government to quell claims and the spread of hate speech at the start of the crisis in the North and South West, the two English-speaking regions in conflict. Heavy economic and social consequences were recorded. These closures were the most serious digital rights violations. During this internet shutdown, Cameroon suffered significant financial losses estimated at \$38.8 million.

Further, on January 17, 2020, Cameroon Telecommunications (Camtel), the public telecoms operator in Cameroon¹⁰ responsible for managing optical fiber, issued a press release to announce the disruption of the internet network following an accident on the cable under - marine West Africa Cable System (WACS). Prior to this release, the NetBlocks Internet Observatory had already shown that social media and messaging services had been disrupted.

IMPACT OF COVID-19 ON DIGITAL RIGHTS AND INCLUSION

As part of collective actions to fight the coronavirus pandemic, the opposition party, Mouvement pour la Renaissance du Cameroun (MRC), initiated fundraising actions to support those in need. On May 4 2020, the Minister of Territorial Administration considered this action as illegal and sent letters to the CEOs of MTN and Orange, demanding the closure¹¹ of the accounts Mobile Money and Orange Money for fundraising.

Additionally, during the crisis, the use of social media rose. In April 2020, a letter from the office of the President of the Republic instructed the Director of the National Agency for Information and Communication Technologies (NAICT), to monitor all accounts by technological means and users disseminating fake news as well as the presence of fake news on platforms like Facebook.

On June 23, 2020, the Facebook page and the Cameroon election website (ELECAM), the organ for the organization and control of elections in Cameroon, was hacked for a period of 24 hours. This attack targeted the databases of registrants.

On September 17, 2020 Facebook announced a VAT of 19.25% will be paid on any advertising in Cameroon from October 1, 2020. According to the provisions of the 2020 Finance law, the educated tax is expanding to other platforms like Google and Amazon for online shopping.

10. <http://www.camix.cm/>

11. In Cameroon, the government wants to stop a fundraiser against the virus launched by the opponent Kamto, Le Monde, April 30, 2020, https://www.lemonde.fr/afrique/article/2020/04/30/in-cameroon-the-government-wants-to-stop-a-fundraiser-against-the-virus-launched-by-the-opponent-kamto_6038237_3212.htm/

Article 127, paragraph 15 of the 2020 finance law stipulates that:



“

The sales of goods and the provision of services carried out on Cameroonian territory or through foreign or local electronic commerce platforms; commissions received by operators of online commerce platforms.

Further, on September 22 2020, the country recorded the presence of low internet disruptions. At the announcement of the elections of regional advisers for December 6, 2020 in Cameroon, the opposition party, MRC invited its activists to demonstrate throughout the country. It is likely that the internet was disrupted to stifle the mobilizations.

Cameroon has various legal instruments on digital use. One in particular is the law on electronic commerce adopted in 2000, the law on consumer protection, law n° 2010/012 of 21 December 2010 on cybersecurity and cybercrime is the law no longer used to regulate cyberspace.

In general, this law “governs the security framework of electronic communication networks and information systems, defines and punishes offenses related to the use of information and communication technologies in Cameroon”.

On March 13, 2020, the Ministers of Finance and Posts and Telecommunications signed a joint decision setting out the modalities for the electronic collection of customs duties and taxes on phones, tablets, terminals and software. This widely criticized joint decision on the possibility of digital rights violations was overturned by a letter from the President of the Republic.

CONCLUSION AND RECOMMENDATIONS



The year 2020 in Cameroon has recorded several news stories on digital rights. Slight cases of digital rights violations have been recorded. In the context of the Coronavirus crisis, the rights of users have been influenced by the barrier measures to combat the pandemic.

New mechanisms of intimidation and violations have developed in the context of Covid-19. Although the government and sometimes telephone operators and internet providers use these new mechanisms to violate digital rights and restrict freedoms, the role of local and international organizations has remained dynamic in addressing non-compliance through various advocacy actions and campaigns.

In view of the digital rights situation in 2020 in Cameroon, the following recommendations should be made to improve digital rights and digital inclusion in the country for the coming year;

- An audit of Cameroon's 2020 digital strategic plan before setting up new strategies plan;
- Adopt a law on the protection of personal data;
- Adopt a law on social media platforms with the definition of government responsibilities;
- Initiate decisions on the ICT sector by involving all the key stakeholders in the internet ecosystem;
- Request an annual transparency report for data privacy from all telephone operators and ISPs in Cameroon on digital inclusion and digital rights.

One of the priorities of the Ministry of Posts and Telecommunications set out in the 2020 Finance law is to increase qualitative and quantitative access and at a lower cost throughout the country.



Case Study: COVID-19: What turned my life upside down

Compiled by Rigobert Kenmogne

In April 2020, when my aunt, Suzanne, went to the Djoungolo Health Center, in the city of Yaoundé, she did not know that she was going to experience some moving moments in her life. 50 years old, she went to the Health Center for a COVID-19 test. Four days, Suzanne had been reluctant to go to a Health Center for the test. Reassured to have made the right choice, under the advice of her cousin, she finally decides to go there one morning. Once in the Health Center, she is shy, because she has already started developing seizures after a few days of her onset of cough, external signs of a potential COVID-19 contamination.

Once at the Health Center, those in charge of the service will make arrangements to take the necessary samples. But the service is slow, due to many patients who want to know their health situation. In addition, the test kits are not in great numbers; the service is saturated; the cousin comforts Suzanne and they wait. Around the middle of the day, Suzanne gets her results, as the signs indicate her status is positive. She is visibly in shock and fears losing her life. Suzanne becomes blade, bruised and lives into silence for a few minutes. She was probably wondering if she could live with this contamination that is so scary. Suzanne must begin quarantine immediately. "Madam, your result is positive, you must go into quarantine, everything will be better with care" indicates a person in charge of the Center. She holds her breath and listens to the doctors' instructions. To avoid any outbreak of the disease, Suzanne's cousin must also be tested. She does not refuse. Fortunately, her status is negative, she has not contracted the disease, but the barrier measures, distancing and quarantine are necessary for her.

A week after the start of treatment in quarantine, Suzanne discovers that her COVID-19 status with her photos and those of other infected people in the Health Center are published on social media, in particular the Facebook and WhatsApp platforms. She was deeply disappointed, upset and lost a lot of weight in a few days. This situation caused other illnesses in her life context. Fortunately, she survived these difficult situations.

According to a young influencer who worked with Plan International-Cameroon, "Suzanne went into a rage when she saw her information online,



which in fact made her situation worse". Suzanne confided that she was back in her forties thanks to the support of Plan International and the work of young influencers of the organization and partners. As in similar cases, as part of its activities, Plan International, sensitized populations on the dangers of COVID-19 by distributing protection kits. Advice was given to Suzanne to help her health balance her moral. Campaigns on the ethical responsibility of physicians have also been initiated directly in targeted health centres or on social media.

Since March 2020, at the start of the crisis, more than 10 cases of personal data breaches have been reported to Plan International through the activities of young influencers. More women than men have complained about posting their health status on social media.

On the prospects of protecting personal data and limiting violations as it has been for Suzanne and many others, the young influencer recommends: " we must adopt a law on the protection of personal data, make Internet users aware of the notion of personal data, encourage Internet users to read the confidentiality policies of social network companies, and draft and make available to the public a personal data protection charter for better impregnation".

Plan International works in 4 areas: health, education, protection and defense of the rights of vulnerable people. The actions of the organization in raising awareness against the spread of COVID-19 and its impact on populations have been significant. For more information on Plan International, please visit <https://plan-international.org/>



Case Study: COVID-19: Between personal data breaches and disinformation in Cameroon

Compiled by Rigobert Kenmogne

At the beginning of 2020, Bernard (name changed), 60 years old, went to Europe as usual. But this visit would not be like the others. His stay in April 2020 coincides with the start of the Coronavirus lockdowns. Originally from the western region of Cameroon, Bernard plans his return to Cameroon to avoid the worst. Once in the country, via Douala International Airport, Bernard must undergo tests as indicated in the health protocol in times of crisis.

Several other passengers like Bernard are waiting for their tests to be carried out with long waits as health services are saturated and are still adapting. Bernard is a well-known personality in the country. Given his age, he must be attended to as a high risk patient as is the case with other elderly passengers.

Bernard tested positive for COVID-19 and went into quarantine. During quarantine, he did not survive and his death left his friends and colleagues in shock. He was an emblematic figure of his community. Despite receiving assistance from healthcare workers, as well as friends and family, Bernard died from COVID-19. During his quarantine, several family members and friends came into contact with him, most of whom did not have a real knowledge of the dangers of the virus yet.

Bernard's funeral was organized in strict compliance with barrier measures away from his native village. A few days later, after Bernard's funeral, friends and relatives became aware of a publication on social media brandishing his COVID-19-related personal data. The news is received with doubt given the denial amongst many Cameroonians of the virus' existence. The announcement with the photo of Bernard a few days after his funeral created a panic in the community. There are mixed sentiments from some refusing to be tested to others seeking home remedies to treat the virus. There is also anger following the publishing of the deceased's personal information.

Other COVID-19 cases that have been disclosed on social media have also created shock in the community as noted through the work carried out by Merveilles du Monde through the International Foundation for Development, Education, Entrepreneurship and Environmental Protection (FIDEPE) in



Cameroon. A team member says: “The second case for me was even more stigmatizing. After Bernard's death, a false announcement spread about the contamination of his private secretary. This situation plunged the whole community into turmoil a second time, with the fear for everyone to approach a member of the different families. It was later that the private secretary of the deceased arrived in the village a few weeks later and in good health, very angry, after having published a post in advance on Facebook to express his dissatisfaction to all those who disseminated this false information of a positive test for COVID-19 with his photo.”

The messages of support enabled Bernard's private secretary to organize awareness-raising campaigns alongside Merveilles du Monde. “He organized an anti-COVID-19 awareness and response campaign in his community,” indicates a member of Merveilles du Monde. For the third case, the member adds that, “This was a man who had health problems for a long time before the COVID-19 crisis. After his death, images were broadcast on social networks announcing a subsequent death from COVID-19 when his test was negative.”

In each case, Merveilles du Monde provided psychological and social assistance as part of the campaign. To limit such violations, in similar crises, Merveilles du Monde recommends “setting up wider platforms for discussion and awareness of the risks of personal data exposure in times of crisis”. In general, awareness training on the consequences of these violations during the crisis is necessary.



Cote D'Ivoire is situated in the western part of Africa. The population made up predominantly of young people is estimated at 26,453,542 in 2020.¹ The internet penetration rate is 26,3%. In 2018, the number of people connected to the internet in Cote d'Ivoire was estimated at around 6.53 million, out of a population of 24.9 million.

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN COTE D'IVOIRE

The mobile penetration rate is also estimated at 131.6%.² In general, 60% of the Ivorian population is connected to the internet through a smartphone, 38% from a computer and 2% from a tablet.³ Cote D'Ivoire is number 9 in Africa and is 131st at the global level on the information and Communication Technologies (ICT) Development Index by the International Telecommunications Union (ITU).⁴

INTERNET INFRASTRUCTURE AND POLICIES

The Ministry of Digital Economy and Post is responsible for the telecommunications sector. It is supplemented by the Telecommunications/ICT Regulatory Authority of Côte d'Ivoire (ARTCI), and by the Commission for Access to Information of Public Interest and Public Documents, (CAIDP). In terms of legislation, Côte d'Ivoire has legal instruments including Law No. 2012-293 of March 21 2012 relating to Telecommunications and Information and Communication Technologies, to govern the telecommunications sector. There is also Law No. 2013-867 of December 23 2013 relating to access to information of public interest, Law No. 2013-451 of 19 June 2013 relating to the fight against cybercrime and Law No. 2017-803 of December 7 2017 on the orientation of the information society.



60%
of Ivorian population
is connected to the
internet through a
smartphone

1. Internet user Statistics for Africa

2. Authority of the Telecommunication Regulation of Côte d'Ivoire

3. Digital report 2018 in Western Africa "we are social"

4. ICT development index 2017 "ITU"

IMPACT OF COVID-19 ON DIGITAL RIGHTS AND INCLUSION

The first cases of COVID-19 were identified and confirmed on March 11 2020. Since then, Côte d'Ivoire has recorded 21,513 confirmed cases.⁵ In an announcement on April 15, Doctor Aka Aouele, Minister of Health and Public Hygiene indicated that “the average age of patients is 40 years with extremes of 18 months to 82 years.”⁶ The government has deployed a crisis management plan mainly focused on economic, social and humanitarian aspects.

The National Security Council proceeded to contain the city of Abidjan on March 29. In fact, the economic capital represents the epicenter of the pandemic and this measure was intended to contain it by reducing mass movement of people. Companies were exempted from tax audits for a period of three months. The penalties for delays in the execution of public contracts and orders with the State and its branches during the crisis period were also canceled.⁷ These measures were aimed at maintaining economic activities, relieving businesses' cash flow and preserving jobs. On the public health front, websites were put into service with all the information in real time relating to the pandemic, its news, and preventive and safety measures.⁸ The official Facebook page of the Ministry of Health and Public Hygiene also supported communication on social networks with daily updates on the development of the health situation.

Mobile phone operators and internet service providers (ISP) have also contributed to curb the impacts of the crisis. Main operators such as Orange, Moov and MTN have launched awareness campaigns through their various channels. In collaboration with the government, an SMS system regularly informs and sensitizes the citizens on protective measures against the coronavirus.⁹ Special internet packages have been made available for each social layer, so that everyone can communicate and access different internet services.¹⁰ The measures taken by the telephone operators were crucial as to ensure the social welfare of the populations, given the imposed social distancing measures.



5. Ministry of Health and Public Hygiene

6. <http://apanews.net/news/lage-moyen-des-personnes-atteintes-du-covid-19-en-cote-divoire-est-de-40-ans-ministre>

7. Retrouvez l'intégralité des mesures prises par le gouvernement su, <https://www.ccifici.org/actualites/mesures-gouvernementale-en-ci-face-au-covid-19.html>

8. <http://info-covid19.gouv.ci> et <http://sante.gouv.ci>

9. <https://www.orange.ci/fr/tous-engages-contre-le-coronavirus.html>

10. <https://www.orange-business.com/fr/covid-19-solutions-voix-et-data-temporaires-pour-collaborateurs>

Faced with the health crisis, the actions of the government resulted in less than 200 deaths per day. However, this commendable government response was in many ways somewhat delayed and punctuated by a crisis in access to information about the disease in light of the changing world situation. In general, COVID-19 has prompted the government to take a series of barrier measures against the pandemic which impacts on human rights. The government's lack of proactivity was noticeable in particular in the management of communication on social networks.¹¹ This has manifested itself in the rise of fake news and cases of human rights violations.

According to Doctor Eddy Gnapi, the difficulties of access to accurate information in the early days of the health crisis in Côte d'Ivoire pushed citizens not only to flock to social networks, but also to produce and relay information without verifying the sources.¹² Social networks have thus become the main channel for disseminating information both for citizens and for certain press houses.

According to the report issued by the Network of Online Press Professionals of Côte d'Ivoire (REPPRELICI), "Some 30% of fake news (false information) on COVID-19 in Côte d'Ivoire has been disseminated in traditional media against 70% on social networks during the period from May 3 to July 31 2020."¹³ Citizens, crystallized by fear and hungry for information about the pandemic were sharing the information at their fingertips without verification. Some press houses also took advantage of this, often publishing fake news in order to generate traffic on their platforms.

According to Anderson Diédri, "The fake news broadcasts mislead citizens and lead them to behave unreasonably. We saw people destroy the screening center that was under construction in Yopougon,¹⁴ believing that this center was going to receive patients who were going to contaminate them, when in reality it was a screening center that was to help improve management within the framework of the fight against the pandemic."¹⁵

The mismanagement of the crisis on social media has also given rise to numerous cases of degradation and violation of human dignity. Indeed, photos and videos of people, victims of corporal punishment and humiliation of all kinds, during the curfew period were widely shared on social networks.¹⁶ The police forces, in their desire to enforce the curfew established by the President of the Republic, exceeded their sovereign mission which is to ensure the safety of citizens. The security forces "therefore took to the field with confidence. No mercy for those still outside after 9 p.m." Some human rights organizations widely denounced the abuses committed against citizens. These waves of condemnation forced the National Police to release a statement to reassure the populations and public that measures will be taken to respect the rights of citizens in the exercise of their mission.

The government's lack of proactivity was noticeable in particular in the management of communication on social networks

11. Les réseaux sociaux, ennemis ou alliés de la lutte contre le COVID 19 – in, https://www.facebook.com/watch/live/?v=259755478483571&ref=watch_permalink

12. Les réseaux sociaux, ennemis ou alliés de la lutte contre le COVID 19 – in, https://www.facebook.com/watch/live/?v=259755478483571&ref=watch_permalink

13. <http://www.atoo.ci/2020/08/15/70-des-fake-news-sur-la-covid-19-ont-ete-diffusees-sur-les-reseaux-sociaux-rapport/>

14. Commune de la ville d'Abidjan

15. <https://www.lemediacitoyen.com/epidemie-de-coronavirus-retour-sur-une-crise-de-linformation/>

16. Couvre-feu à la matraque : l'Afrique de l'Ouest se rebelle in, https://www.lemonde.fr/afrique/article/2020/03/30/couvre-feu-a-la-matraque-l-afrique-de-l-ouest-se-rebelle_6034953_3212.html

CONCLUSION AND RECOMMENDATIONS



The coronavirus pandemic was not far from a simple health crisis in Côte d'Ivoire. It has indeed served as a test of the entire state system at the political, educational, social, economic and health levels. What should be noted is that the challenges to be met are still significant, especially in terms of digital rights and access to information which, in all likelihood, were not perceived as priorities at the start of the crisis. This situation has caused the rise of fake news with very often the disclosure of false information or personal data of citizens on social networks.

The coronavirus disease has also enabled the Ivorian government to better deal with technological tools, particularly teleworking and the gradual digitization of certain sectors of activity. The challenge of education in the proper use of social networks and in knowledge of the legal measures which govern this new virtual space of expression must also be taken up by the Ivorian State because, poorly trained and poorly informed citizens constitute a danger above all in times of crisis such as COVID-19.

***This situation has caused the rise of
fake news with very often the disclosure of
false information or personal data of
citizens on social networks.***

”



The Democratic Republic of Congo¹ is the largest country in Central Africa with over 88 million inhabitants, making it the fourth most populous country in Africa behind Nigeria, Ethiopia and Egypt.²

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN DEMOCRATIC REPUBLIC OF CONGO

The country is ranked 49th out of 54 African countries in global governance with a score of 31.7 out of 100.0³ and a GDP of 47.22 billion (USD) in 2018⁴ compared to 38.01 billion (USD) in 2017.⁵ The whole country is covered by four telephone networks which are: Airtel, Orange, Africel and Vodacom and numerous internet service providers. As of today, the country has around 16.35 million internet users on different devices, with a penetration rate of 19%.⁶

The Democratic Republic of the Congo has nine neighbouring countries. The country is headed by President Antoine-Félix Tshisekedi, following the December 2018 elections in which the Constitutional Court proclaimed him winner and successor of Joseph Kabila who led the country for 18 years.⁷



16.35 Million
Internet users

1. Banque Mondiale, <https://www.worldbank.org/en/country/drc/overview#1>

2. Wikipedia: https://fr.wikipedia.org/wiki/R%C3%A9publique_d%C3%A9mocratique_du_Congo

3. Mo Ibrahim FOUNDATION Rapport - 2019: <http://iiag.online/app.html?loc=CD&meas=PRI&view=overview>

4. Banque Mondiale - 2020:

https://www.google.com/publicdata/explore?ds=d5bncppjof8f9_&met_y=ny_gdp_mkt_p_cd&idim=country:COD:RWA:UGA&hl=fr&dl=fr

5. Banque Mondiale - 2020:

https://www.google.com/publicdata/explore?ds=d5bncppjof8f9_&met_y=ny_gdp_mkt_p_cd&idim=country:COD:RWA:UGA&hl=fr&dl=fr#!ctype=c&strail=false&bc=s&d&nselm=s&met_y=ny_gdp_mkt_p_cd&scale_y=lin&ind_y=false&idim=country:COD&ifdim=country:region:SSF&pit=1511647200000&hl=fr&dl=fr&ind=false

6. Datareportal - Janvier 2020: <https://datareportal.com/reports/digital-2020-democratic-republic-of-the-congo>

7. Wikipedia: https://fr.wikipedia.org/wiki/Joseph_Kabila

Over the past 10 years, the country has drawn the attention of several actors on issues of human rights violations in Africa. The authorities have strategically put in place means to stifle public demonstrations and speeches against those in power by shutting down the internet, including messaging services, and by also performing filtering.⁸

Under Article 46 of the Framework Act which governs the postal sector and telecommunications, the authorities had the power to interrupt “partially or completely and for a period that they determine the use of telecoms installations” for public safety and national defense reasons.⁹ Under the same Act, the government also had the power to requisition telecommunications facilities.

INTERNET POLICIES AND REGULATIONS

The country introduced a bill in April 2017, initiated by the government, which was adopted by the National Assembly on May 7 2018 and adopted November 22 2018 at the Senate level. On November 25 2020, the new Telecoms Law (Law No. 20/17 of November 25 2020) replaced¹⁰ the Framework Law No. 013-2002 of October 16 2002¹¹ on post and telecommunications in the Democratic Republic of the Congo. In his first year as the Head of the country, President Félix Tshisekedi adopted an ambitious plan called the “National Digital Plan” in order to “prepare the country for the advent of the fourth industrial

revolution”.¹² On 7 February 2020, a Member of the National Assembly introduced a bill on cyber security and cybercrime in the hope of filling the legal gap in this sector.¹³ On 24 September 2020, the DRC launched, via the Ministry of Post, Telecommunications and New Information and Communication Technologies (PTNTIC), the automatic identification of all telephones in service in the country, with the introduction of the Mobile Device Registry (MDR).¹⁴

HUMAN RIGHTS AND DIGITAL EXCLUSION

Although internet penetration rates rose from 17% in 2019 to 19% in 2020, there still remains a digital divide in terms of access, accessibility and inclusion of communities in the Democratic Republic of Congo.¹⁵

According to a 2018 report released by Global System for Mobile Applications (GSMA) titled, “Reforming the taxation of mobile telephone in the Democratic Republic of the Congo to support economic growth through a more favourable fiscal framework”, it is stated that taxation is an “impediment” to digital inclusion in DRC, as the price of mobile communications weighs heavily on the household budget.¹⁶

With the introduction of the mobile device tax in the Democratic Republic of Congo, telecommunication service users will have to pay between USD 0.17 for a 2G device and USD 1.17 for

8. QUARTZ AFRICA : <https://qz.com/africa/1187727/the-dr-congo-is-using-a-decades-old-law-to-shut-down-the-internet/>

9. LEGANET.CD – Lois cadre Telecoms RDC: <http://www.leganet.cd/Legislation/JO/2003/JO.25.01.2003.PT.pdf>

10. SCOOPRDC.NET : <https://scooprdc.net/2020/12/16/nouvelle-loi-sur-les-telecoms-et-tic-voici-quelques-innovations/#:~:text=La%20loi%20sur%20les%20t%C3%A9l%C3%A9communications,par%20le%20pr%C3%A9sident%20F%C3%A9lix%20Tshisekedi>

11. LEGANET.CD – lois cadre telecomms RDC: <http://www.leganet.cd/Legislation/Droit%20economie/telecommunication/LC.013.2002.16.10.2002.htm>

12. Zoom-Eco – Plan national du Numerique: <https://zoom-eco.net/a-la-une/rdc-enfin-le-plan-national-du-numerique-valide/>

13. Proposition de lois sur la Cyber-securite et Cyber-Criminalite: <https://www.radiookapi.net/2020/02/19/emissions/parole-aux-auditeurs/la-proposition-de-loi-sur-la-cybersecurite-et>

14. Lancement RAM: <https://econews.cd/g?post=1037>

15. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/01/gsma-inclusion-num%C3%A9rique-et-fiscalit%C3%A9-dans-le-secteur-de-la-t%C3%A9l%C3%A9phonie-mobile-en-r%C3%A9publique-d%C3%A9mocratique-du-congo-summary.pdf>

16. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/01/gsma-inclusion-num%C3%A9rique-et-fiscalit%C3%A9-dans-le-secteur-de-la-t%C3%A9l%C3%A9phonie-mobile-en-r%C3%A9publique-d%C3%A9mocratique-du-congo-summary.pdf>

3G/4G/+ devices once a month over a six-month period.¹⁷ The poor quality of digital services has raised waves of indignation from individuals, consumer groups and citizen movements across the country.

Since March 2019, LUCHA, a youth citizen movement, organized peaceful demonstrations in front of the premises of telecommunication companies to demand better quality services and more cooperation with the security forces to address the problems of kidnappers who use telecommunications services to intimidate victims' families and receive ransoms.¹⁸ On 18 August 2020, a citizen filed a complaint with the Commercial Court of Kisangani (Tshopo province) accusing Orange DRC, a subsidiary of the French multinational telecommunications group Orange, of "breach of trust".¹⁹

POSITIVE DEVELOPMENTS FOR THE PROMOTION OF INCLUSION AND HUMAN RIGHTS

On November 25 2020, the Democratic Republic of the Congo adopted a new law that would govern telecoms in place of the Framework law of October 16 2020 that governed this sector for almost 18 years and in which some provisions were already viewed to be problematic with the reality in relation to the evolution of new Information and Communication Technologies.

But also, in the third quarter of his first year in power, President Félix Tshisekedi adopted a digital plan while being convinced that ICTs will undoubtedly contribute to the performance of the Congolese economy, at the same time strengthening sociability, improvement of knowledge, the effectiveness of institutions and the fight against poverty.²⁰

On 7 February 2020, a bill on cybersecurity and cybercrime was submitted by the Deputy in the Office of the National Assembly of the Democratic Republic of the Congo.



17. Site web du Service RAM: <https://www.ram.cd/FAQ.aspx>

18. La Lucha en Revendication devant les telecoms: <https://www.rfi.fr/fr/afrique/20190511-rdc-lucha-manifestations-airtel-telecommunications-geolocalisation-kidnapping>

19. Orange RDC assignee en justice: <https://zoom-eco.net/a-la-une/rdc-la-societe-orange-assignee-en-justice-par-un-de-ses-abonnes-pour-abus-de-confiance/>

20. Validation du plan national du Numerique: <https://zoom-eco.net/a-la-une/rdc-le-chef-de-letat-lance-les-travaux-de-validation-du-plan-national-du-numerique/>

In his speech, he expressed his frustration that none of the laws passed in this country dealt with the protection of individuals in cyberspace.

This makes it difficult, at the current stage, to block cybercriminals in order to control their behaviour while simultaneously “normalizing the virtual space, so that it is a digital place where it is good to live.”

CONCLUSION AND RECOMMENDATIONS

Over the past two years, the Democratic Republic of Congo has experienced major turning points directly affecting the issue of digital inclusion and human rights.

Among other things, there are violations of users’ rights by - on the one hand, the powers in place and on the other hand by the providers of digital services under a vague and obsolete law.²¹ Some policies and regulations could be implemented in the perspectives: to mitigate the digital divide, to enhance the human rights of Congolese citizens and to ensure national security etc.

In relation to factors that limit digital inclusion and human rights in the Democratic Republic of Congo, we note:

- 87.5% of our key informants cited digital illiteracy as a key element limiting digital inclusion in general;
- 37.5% said that the lack of cooperation between digital stakeholders undermines the promotion of human rights and the inclusion of communities.
- 37.5% of our key informants mentioned that inadequate legislation also constitutes a limit to the promotion of digital rights in the DRC

Various stakeholders in the digital ecosystem in the DRC from civil society, the media, the private sector, and the public sector have issued various recommendations to promote digital inclusion as well as human rights. These include:

- Strengthen cooperation between stakeholders involved in the digital sector in the Democratic Republic of Congo.
- To promote education on new information and communication technologies within communities.
- Raise citizens’ awareness of their online rights.
- Increase lobbying to review digital policies and regulations in the Democratic Republic of Congo.
- Making NTICs tools, including the Internet, accessible to all citizens;
- Develop the digital legal framework and infrastructures.

21. Quartz Africa: <https://qz.com/africa/1187727/the-dr-congo-is-using-a-decades-old-law-to-shut-down-the-internet/>



Egypt is one of the largest and most diversified economies in the Middle East, which is projected to become one of the largest in the world in the 21st century. Egypt has the second-largest economy in Africa, the world's 33rd-largest economy by nominal GDP and the 19-largest by PPP.

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN EGYPT

The digital revolution and the use of technology as well as different social media applications in Egypt played a significant role in the political revolution that led to political changes in 2011 and 2013 and influenced Egyptian present day politics.

Post 2011, The regimes paid special attention to digital rights and social media by taking all possible measures to control access to the Internet and target activists. To achieve that, the different regimes used the technical means to censor and servile activists and content as well as using legislation tools to legalize internet shutdowns, ban websites, collect personal data, abuse rights to privacy and criminalize the right to freedom of expression under the accusation of fake news which is considered a national security crime. Such actions increased in 2020, in the time of COVID-19, where circulating information about the pandemic was considered as a national security issue.



***The digital revolution and use of technology
Role in the political revolution***

ACCESS TO THE INTERNET IN EGYPT

Egypt witnessed a revolution in the ICT sector during the past two decades. For example, by the end of 2000, there were only 450,000 users with access to the Internet. This number rose to 20 million users¹ before 2011 which was made up mostly by youth² then rose to 29 million in 2011. According to ITU, by 2019, the percentage of the population using the Internet reached 57.28%.³ Facebook users increased from 4.2 million users in 2010 to 9.4 million users in 2011,⁴ and by the end of 2019, Facebook users in Egypt reached 42,400,000.⁵ According to the National Telecommunication Regulatory Authority (NTRA), the number of fixed broadband subscribers reached 799,000 by the second quarter of 2020 and the number of mobile broadband subscribers reached 45,707,490 by the second quarter of 2020.⁶ Despite the ICT revolution, the rise in penetration rate and the rapid change to virtual life as a result of the pandemic, around 43% of Egyptians still have no access to the Internet. Also, the increase in the internet penetration rate was associated with adopting restrictive regulations and laws that led to the shrinking of the virtual civic space and restriction of digital rights.

DIGITAL RIGHTS: LAWS AND LEGAL FRAMEWORK

Legislation is one of the tools that was used by the Egyptian government to close the virtual civic space and breach digital rights. Digital laws refer to a set of legislation and provisions that are adopted to regulate all online activities – inter alia – digital

developed to impose constraints on individuals' digital rights. In 2018, the Egyptian parliament passed Law No.175 of 2018 concerned with combating information technology crimes, "Cybercrimes law", and Law No.180 of 2018 which was concerned with media regulation. In addition, Law No.10 of 2003 which was concerned with regulating communication.



■ BLOCKING WEBSITES

The provisions of the law gave the power to the authority to block websites if they are deemed to harm national security. Article (1) of Law No.175 of 2018 in concern with combating information technology crimes states, "Cybercrimes law defines national security as everything related to the independence, stability, and security of the homeland and anything linked to affairs of the Presidency, the Ministry of Defense and General Intelligence ...". The same definition is also repeated in many laws pertaining to the internet use, without any interpretation or explanation of the concept of national security or clarification of its determinants.⁷ Thus, the authority has the right to determine what is considered security-oriented matters and what is not.

1. Internet World Stats, 'Internet User Statistics for Africa' <https://www.internetworldstats.com/stats1.htm> (Accessed 18 September/2020)

2. Noha Bakr, (2016) The Egyptian Revolution, in Stephan Calleya & Monika Wohlfeld (editors), Change & Opportunities in the Emerging Mediterranean, Mediterranean Academy of Diplomatic Studies.p.59, <https://www.researchgate.net/publication/265358472>

3. ITU, <https://www.itu.int/net4/ITU-D/ictkey/#/query>

4. MCIT, Op.Cit.,

5. Internet World Stats, Op.cit.,

6. National Telecom Regulator Authority (NTRA)-Egypt, <https://www.tra.gov.eg/en/industry/telecom-market/market-indicators/>

7. Maha Al Asouad, (2016) Right to information and the national security in Egypt, Cairo: Association of freedom of Thoughts and Expression –AFTE.

Some reports stated that from the Combating Information Technology Crimes law, the state aims to “*completely control the Internet, suppress its users, legalize state practices in censoring this space, blocking websites, and mass surveillance of communications*” and other reports added “*before the adoption of these “controversial” laws, the Egyptian legal environment lacked the legal cover and legal justification for the practice of blocking*”.

According to art (19) of Law 180 of 2018 which is concerned with regulating the press and media, the authorities have a right to block websites and electronic news for publishing false news. Besides these specific laws, art (102 bis) of the penal code criminalized fake news, labelling it as a national security crime if it harmed public interest. Article (2) of the Combat Terrorism Law No. 94 of 2015 described that the terrorism actions - *inter alia* - as breaching the public interest or endangering the safety of society and its interests, or casting terror among individuals. Art (29) of the same law added that “*everyone who establishes or uses a website on the internet to promote thoughts that lead to committing terrorism actions*”, shall be punished by imprisonment for a period not less five years.

Consequently, freedom of expression or circulating information and news could be classified as a terrorism action if it is considered, upon the absolute discretion of security authorities, to constitute harmfully to the public interest and order. In addition to Law No.10 of 2003, which is concerned with the regulation of communication, was the main legal tool used to shut down the Internet during the 2011 revolution. All these legal provisions make up the legal infrastructure used to criminalize the freedom of expression online and other digital rights.

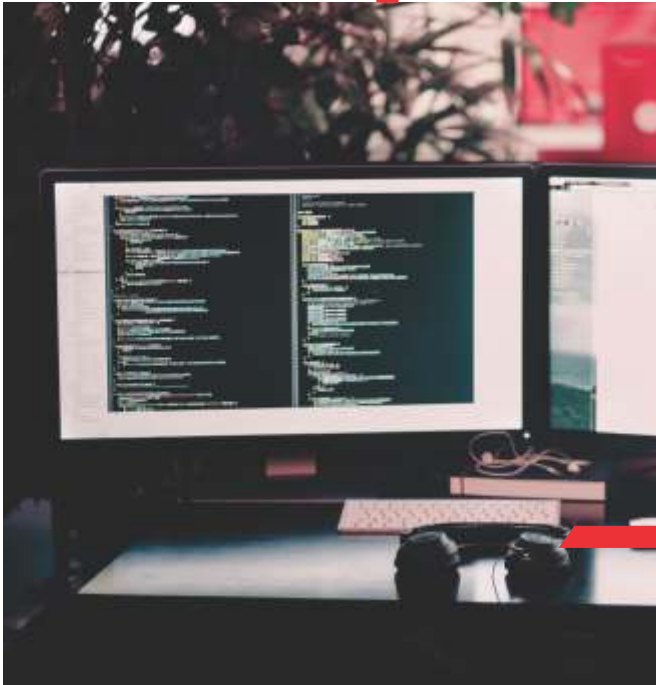
■ SURVEILLANCE

Article 6 of the Cybercrime law authorizes the investigation authority to issue a decision that allows surveillance and access to information and article 2 stipulates that Internet Service Providers are required to keep and store customer usage data for a period of 180 days, including data that enables user identification, data related to the information system content, and data related to the equipment used. This means the Internet Service Providers will possess the data related to all user activities, including phone calls, text messages, websites navigated, and applications used on smartphones and computers. In another context, article 25 of the cybercrime law criminalizes the breach of the principles and values of Egyptian families. Without the clarification and identification of the meaning of ‘principles and values of Egyptian families’, as a result in July 2020, some Egyptian women were arrested on charges related to this article, now known as the case of the Tik-tok’s girls.⁸

■ DATA PROTECTION

In July 2020, the Egyptian Parliament issued law No.151 of 2020 concerning the protection of personal data. The third article of promulgating provision of the law stipulates that “*the law will not apply to the personal data in the possession of national security bodies*”. Article 1 identifies the national security bodies by “*The Presidency of the Republic, the Ministry of Defense, the Ministry of Interior, the Intelligence Service and the Administrative Oversight Authority*” which reflect that all personal data are in the possession of national security bodies without real and legal justifications. The Egyptian legal framework was the tool used the most to abuse digital rights in the time of Covid-19.

8. Global freedom of expression Columbia University, The Case of the Egyptian TikTok Girls, <https://globalfreedomofexpression.columbia.edu/cases/the-tiktok-girls-case/>



“

Article 6 of the Cybercrime law authorizes the investigation authority to issue a decision that allows surveillance and access to information

IMPACT OF COVID-19 ON DIGITAL RIGHTS

The above-mentioned legal framework was used during the COVID-19 pandemic to suppress digital rights in particular freedom of expression online to circulate information and digital press freedom. Egyptian authorities adopted preventive measures to reduce the outbreak of the virus. By end of December 2020 and according to the Ministry of Health, Egypt had recorded 138,062 confirmed cases, out of which 112,105 have recovered, 7,631 died and 18,326 are still active cases.⁹

To respond to the pandemic outbreak, the Egyptian government adopted a partial lockdown policy¹⁰ such as suspending all events that are gatherings.¹¹ With the rapid outbreak of the virus, which increased from one single case to more than 5000 cases within two months, the citizens, civil society activists, journalists, and doctors began to “question” the announced figures, especially with the collapse of the medical systems in most developed countries and the failure to addressing the epidemic with recording tens of thousands of infected cases in a daily basis. Therefore, these preventive measures were associated with restrictive practices against individuals from diverse spectrums.

9. <https://www.worldometers.info/coronavirus/> last visit 1/1/2021 at 5:02 pm

10. Egyptian government, Prime Minister's decree No. (606) of the year 2020, published in official gazette –issue No. (12-Bis B) on 24 March 2020.

11. Egyptian government, Prime Minister's decree No. (606) of the year 2020, published in official gazette –issue No. (10-Bis) on 9 March 2020.

■ FREEDOM OF EXPRESSION

ONLINE IN 2020

The Egyptian state dealt with the information that was circulating about the pandemic as fake news; accordingly, many citizens were subjected to prosecution for spreading fake news. For instance, case No. 535 of 2020 which classified as a national security case, included doctors, journalists, civil society activists, ordinary citizens, researchers who published news of the spread of the pandemic or addressed the causes of infection or the death of a medical personnel. One example is that of the case of the arrest of a specialist in marketing medical products for his “criticism” of the state’s policies to encounter Coronavirus.¹² In the same context, many other journalists, lawyers, and civil society activists were arrested within Case No. (558) of 2020 - State Security case.¹³

It is worth noting that the cases of arrest and investigation took place in the period from March - June 2020, which is the same period that witnessed a significant daily increase in the number of infected people. Where the numbers of infected people escalated in an unexpected way from hundreds at the end of March (507), reaching (17,989) at the end of May and then the numbers jumped within one month to reach (46,898) infected people at the end of June, according to the publicly announced official statistics.

■ THE LEGAL CRITERIA OF FAKE NEWS

The above-mentioned practices and restriction on freedom of expression online imposed questions about the legality and constitutionality of the chosen procedures such as what are the legal criteria for fake news? What is considered fake news or freedom of expression? The legal definition of false news according to article 102 bis, 188 of the Egyptian Penal Code refers to “*publishing and broadcasting (intentionally and ill-intentionally) news, statements or rumors (false) that (which) disturb public peace, provoke panic among people, or harm their interests*”. As it is clear that the text does not define false news, but at the same time it sets standards and controls by which the crime of spreading false news can be described. The Egyptian Court of Cassation, in its decision No. (451) for the year 22 ,20/5/1952) stated that “*In order to apply the text of article 188 of the Penal Code concerning the publication of false news, the news should be false and the publisher is aware of this falsehood and intentionally publishing what it is false, and it added that the verdict must explain the falsehood of the news and the publisher knows of the falsehood of the news, otherwise the verdict is a shortage for not revealing the elements of the crime for which the appellant was indicted.*” Without a doubt, the pandemic not only had an adverse impact on digital rights but also revealed the inconsistencies in what false news was defined as.

Publishing and broadcasting (intentionally and ill-intentionally) news, statements or rumors (false) that (which) disturb public peace, provoke panic among people, or harm their interests.



FALSE NEWS DEFINITION

12. For more details on the case Egyptian Front for Human Rights report, <https://egyptianfront.org/ar/2020/07/fr-353-2020/>

13. For more details on the case Egyptian Front for Human Rights report, Minor report of Case 558 of the year 2020-National security, May 2020.

DIGITAL EXCLUSION

In terms of digital inclusion in Egypt, many people are excluded from access to internet for various reasons related to financial, technical and geographic issues. Refugees, one of the most vulnerable groups in Egypt, are still excluded from access to different digital rights in particular the right to connectivity. According to UNHCR-Egypt, *“The majority of refugees and asylum-seekers in Egypt were already extremely vulnerable before the outbreak of Covid-19 and have been directly impacted by the evolving circumstances. Many have lost their source of income and cannot afford to buy sufficient basic supplies or pay their rent.”*¹⁴

While internet access has been essential for refugees to work, access information and express their opinions; its importance has increased dramatically in the time of the Covid-19 pandemic. In September 2020, the Minister of Education announced the plan for the academic year 2020/2021. The plan adopted a hybrid system that included physical attendance alongside distance learning mechanisms through an online broadcast platform for virtual classes, the electronic Platform.¹⁵ The new distance learning system raises a question about the situation of refugee students who could not access the internet due to the lack of access to the technology needed to access the internet, lack of appropriate computer or mobile devices that connect them to the internet, and high service fee rates for internet access.

Lastly, refugee IDs documents were not recognised by Internet Service Providers so many could not register for internet services or buy mobile SIM cards. The UNHCR has indicated that one of the most significant challenges facing refugee students in light of the pandemic is limited access to hardware devices and the high cost of internet connectivity.¹⁶



Many people are excluded from access to internet for various reasons



14. UNHCR-Egypt, Fact sheet, July 2020.

15. Egypt, Ministry of Education, plan of the academic year 2020/2021, <http://portal.moe.gov.eg/Pages/single-news-view.aspx?NewsID=4646>

16. UNHCR, <https://www.unhcr.org/5e787bea6>

CONCLUSION AND RECOMMENDATIONS



- It is strongly recommended to review the different legal provisions related to fake news and put a clear definition and Criteria for the fake news.
- To ensure refugees' right to access to the Internet, connectivity, E-learning platforms, UNHCR and the Egyptian government should work together to ensure refugees have access to the needed software, hardware, and Internet and recognized refugees' ID card to present to the service providers.
- It is strongly recommended to monitor the application of cybercrime laws through using the different Parliamentary oversight tools.
- The availability of personal data should be upon a request of the national security bodies submitted to the judicial body and be available after a justified court decision.
- The lawyers have to use the strategic litigation mechanisms to protect digital rights.

***“UNHCR and the Egyptian government
should work together to ensure
refugees have access to
the Internet.”***



Ethiopia is the continent's second most populous nation, located in north-eastern Africa, in the Horn of Africa region. With over 112 million citizens,¹ Ethiopia is Africa's diplomatic capital and hosts the African Union's headquarters in its capital city, Addis Ababa.

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN ETHIOPIA

Ethiopia's telecommunication infrastructure is largely government-owned through a monopoly called Ethio Telecom.² Ethio Telecom provides almost all telecom services including fixed line and mobile and internet (dial-up, wireless, ADSL services etc.) The company also offers other services including domain registration and management of the country code top-level domain, .et, web hosting and Internet Protocol (IP) address service among others.

The Ministry of Innovation and Technology, MINT, is the main policy making body of government established in 2018 through proclamation 1097/2018. Its work is backed by two regulatory entities, the Ethiopian Telecommunications Agency (ETA) and the Information Network Security Agency (INSA).

Ethiopia took significant steps towards partial liberalization of its telecom market in 2020. The move is part of the wider liberalization of the economy under reforms by Prime Minister Abiy Ahmed Ali.

In June 2020, the government approved legislation to allow two more operators into the sector. The relevant bodies opened bids later in the year with two new operators expected

1. World Bank, population – total, Ethiopia (1960 – 2019): <https://bit.ly/3bqGrxa>

2. Ethio Telecom, About Ethio Telecom: <https://bit.ly/2XtdjX>

to be announced in February 2021. Government will also put up a 45% stake in Ethio Telecom as part of privatization efforts.

IMPACT OF COVID-19 REGULATIONS ON DIGITAL RIGHTS AND INCLUSION

Ethiopia has gained increasing notoriety when it comes to internet outages in recent years.³ The general digital rights landscape is seen as challenging within the context of existing legislation and the manner in which they are generally enforced.

Ethiopia was among a number of African countries that passed State of Emergency (SoE) legislation in the wake of the COVID-19 pandemic.

The law, Proclamation 3/2020 - A State of Emergency Proclamation Enacted to Counter and Control the Spread of COVID-19 and Mitigate Its Impact,⁴ was passed by the House of Peoples Representatives and subsequently assented to by Prime Minister Abiy Ahmed on April 8.

It ordered Cabinet to “stipulate details of the suspension of rights and measures to be adopted to counter and mitigate the humanitarian, social, economic and political damage that could be caused by the pandemic.”

The law triggered arrests, even as analysts criticized parts of the regulations,⁵ especially as applied to sharing of information on the virus situation in the country. Particular clauses were classified overly vague and left to interpretation of officials.

One of Ethiopia’s highly discussed legislations of 2019 was the Hate Speech and Disinformation law. Despite concerns by local and international analysts, it was approved by Cabinet in November 2019⁶ and accented to by President Sahle-Work Zewde on March 23, 2020, barely a week after Ethiopia recorded its first COVID-19 case.⁷ Internet rights group Access Now’s⁸ Berhan Taye, touched on the negative impact of the law amidst the pandemic saying, “Unfortunately, it does not look good so far for this troubling legislation, and that is especially frightening during COVID-19. Unless this legislation is revised, this may only be the beginning of a chilling period for the free press in Ethiopia”.

The first victim of the introduction of this legislation was journalist Yayasew Shimeles, who was charged with spreading false information about the government’s COVID-19 response. In the course of the year, seven journalists were arrested on different charges, according to a report by the Committee for the Protection of Journalists (CPJ).⁹ In total, three online journalists were arrested, according to a ‘census’ published by privately-owned Addis Standard.¹⁰ The trio were Nathaniel Gech of Wolaita Times, Medhanie Ekubamichael of Addis Standard and Bekalu Almirow of Awlo Media.

**Ethiopia has gained increasing
notoriety when it comes to
internet outages in
recent years.**

3. Quartz Africa, The internet is back on in Ethiopia but there is every chance it will go off again: <https://bit.ly/38xbghZ>

4. House of Representatives passes State of Emergency Law, March 2020: <https://bit.ly/3sdgE1u>

5. HRW, Ethiopia: Free Speech at Risk Amid COVID-19: <https://bit.ly/39jqYfR>

6. Ethiopia cabinet approves new law to fight false information, Bloomberg; November 19, 2019: <https://bloom.bg/3nyoWgE>

7. Ethiopia confirms first case of COVID-19, WHO Afro region, March 15, 2020: <https://bit.ly/39lO4nF>

8. Ethiopia's hate speech and disinformation law: the pros, the cons and a mystery, Access Now; May 19, 2020: <https://bit.ly/2Lou8Xv>

9. CPJ, Record number of journalists jailed worldwide, December 2020: <https://bit.ly/2Xv3hf2>

10. Addis Standard, Analysis – Ethiopia back in list of countries jailing journalists: <https://bit.ly/3nBLPQu>

Aside from the SoE regulation and the Hate Speech and Disinformation law, there are other legislations that have over the years been used by the government to stifle voices online. One legislation of significance is the Computer Crime Proclamation of 2016, parts of which contravenes international legislations ratified by Ethiopia – the Universal Declaration of Human Rights (UDHR) and the African Charter on Human and Peoples’ Rights (ACHPR). Others include the 2012 Telecom Fraud Offences Proclamation No. 761; Anti-Terrorism Proclamation No. 652 and Charities and Societies Proclamation No. 621 – both passed in 2009.

INTERNET SHUTDOWNS

The year 2020 was a challenging year in relation to internet access. There were three outages – two restricted and one nationwide. These shutdowns are in contravention of the National Constitution which under article 29¹¹ guarantees right of thought, opinion and expression and media freedom “without any interference.” Shutdowns also breach international human rights laws.

Analysts have stated that having one telecom operator made it easier to switch off the internet without following due process. In 2019, the internet was shut down eight times making the country one of the worst internet shutdown offenders, according to an Access Now report.¹² In 2020, the first outage in western Oromia lasted three months – from January till late March 2020.

The second and most impactful shutdown was nationwide, a measure imposed on June 30¹³ following the killing of a famed Oromo artiste Hachalu Hundessa, in the capital Addis Ababa. That blackout lasted over three weeks. In November, a total internet outage¹⁴ was imposed in the northern Tigray region when the government started the “State of Emergency and Rule of Law Operation” against the then regional government led by the Tigray People’s Liberation Front (TPLF). United Nations (UN) human rights Head, Michelle Bachelet, bemoaned the human rights and humanitarian impact in a statement released November 6.¹⁵ Ethio Telecom confirmed in late November that it had begun restoring service to parts of Tigray, days after Prime Minister Abiy announced



11. Ethiopia’s 1995 constitution: <https://bit.ly/39kWZnx>

12. Article 19, Ethiopia should guarantee internet access and access to information during the pandemic: <https://bit.ly/3bsrdYE>

13. Internet cut in Ethiopia amid unrest following killing of singer, Net Blocks; June 30, 2020: <https://bit.ly/39zU8Yj>

14. Internet disrupted in Ethiopia as conflict breaks out in Tigray region, Net Blocks; November 5, 2020: <https://bit.ly/3oCjQlc>

15. Ethiopia: ‘Halt the violence,’ resolve grievances peacefully, UN rights chief; UN News November 6, 2020: <https://bit.ly/38tjKLQ>



In 2019, the internet was shut down eight times making the country one of the worst internet shutdown offenders, according to an Access Now report.

the end of the operation.

Allied to the Tigray operation, government issued arrest warrants for some activists, writers and academics¹⁶ who it averred were using “a variety of media outlets to destroy the country.” Deputy Prime Minister, Demeke Mekonnen, in an opinion piece, highlighted the impact of media reportage and especially social media in swaying international opinion during the Tigray operation.¹⁷

ACCESS TO INFORMATION

The National Cybersecurity Agency (INSA) disclosed in December 2020¹⁸ that the TPLF had employed cyber attacks and the use of a social media misinformation army. The TPLF was said to have also targeted a number of national and private TV networks with the cyber attacks, all of which were thwarted. Tefyalew Tefera, the deputy head of INSA, also accused Oromia Media Network (OMN) and Ethio 360 Media of aiding the TPLF’s propaganda campaign. A month after the TPLF

operation ended officially, government’s special fact-checking outlets reported what it alleged was a TPLF act of sabotage in the Tigray capital Mekelle, which caused the internet outage.¹⁹

As at January 2021, the UN reported that communication services remained inaccessible in parts of the region as fighting continued between the TPLF and federal forces. Previously in July, following the Hachalu Hundessa protests that claimed over 80 lives, the government partly blamed social media for acting as an instigator.²⁰ One of the main arrests from this incident was of Jawar Mohammed, a media mogul turned politician.

He is facing terrorism charges over the death of a policeman during the protests. His Facebook page which had over a million followers was temporarily closed in June. According to his TV network, Oromia Media Network, the move was necessitated due to attempted hacking.²¹

16. The Telegraph: Ethiopia wants to arrest UK academic who nominated country’s PM for Nobel Peace Prize: <https://bit.ly/3oy3dXR>

17. ENA, The law enforcement operation in Tigray, DPM Demeke Mekonnen, January 2021: <https://bit.ly/3qfK3GF>

18. FBC, TPLF disseminating fake information via Twitter, December 2020: <https://bit.ly/3q8pLP3>

19. Ethiopia SoEFactcheck on Twitter @SOEFactCheck, December 2020: <https://bit.ly/3sgDuoP>

20. Context and updates on current issues, Ethiopia, Prime Minister’s office, July 2020: <https://bit.ly/3sdTfge>

21. OMN official Facebook page, July 2020: <https://bit.ly/38xu40n>

In the midst of such a blackout, the frustration towards the lack of access to information often forced people in Ethiopia and abroad²² to turn to less trusted outlets especially via social media. Ethiopia still lacks laws that deal with regulation of problematic online content. Subsequently, the government has often arbitrarily blocked, filtered or taken down contents that are critical of its activities and policies.



GENDER AND ACCESS TO THE INTERNET

Internet connectivity in Ethiopia is largely concentrated in the capital and major urban areas. Ethio Telecom continues to incrementally expand coverage to other areas in line with government policy to extend internet nationwide. Electricity penetration / access is at 45%,²³ more than double that of the internet as of 2018, according to the International Energy Agency (IEA). The government has plans to reach universal access by 2030.

Data Reportal statistics indicate that as of January 2020,²⁴ there were over 21 million internet users in Ethiopia, representing an increase of over half a million users within the space of a year. As of 2018, the internet penetration, according to the International Telecommunications Union (ITU) stood at

18.618%,²⁵ an indication that the majority of Ethiopians did not have access to the internet.

With respect to data affordability in Ethiopia, the Alliance for Affordable Internet (A4AI) in its 2020 Affordability Report noted that policies related to internet infrastructure and access played a key role in making broadband more affordable. It made special mention of Ethiopia's strides in the Affordability Drivers Index (ADI). The report notes, "One standout – Ethiopia – has seen its ADI score risen from 2.31% in 2014 to 20.37% in 2020, spurred by the opening up of its telecommunication market over the past two years."

However, a 2019 ITU report²⁶ found that sub-Saharan Africa's digital gender divide was persistent. The World Wide Web Foundation's Women's Rights Online report²⁷ noted, "Women are less likely than men to have access to and use the internet in developing and least-developed countries." Despite the great strides made to the affordability of the internet, Ethiopian women continue to face the same challenges that women across the continent face.

The Economic Intelligence Unit's Inclusive Internet index placed Ethiopia 93rd overall and 19th out of 26 African countries ranked²⁸ noting, "Some progress is evident in readiness, thanks to attention to broadband and e-inclusion strategies. But efforts to widen internet inclusion are severely constrained by low literacy levels, a weak competition environment and high cost (relative to income) of data".

22. VOA News: Ethiopia's diaspora seeking news amid communication blackout challenge, December 2020: <https://bit.ly/3brq03D>

23. IEA, Ethiopia Energy Outlook – Analysis: <https://bit.ly/3i2SemG>

24. Data Reportal, Digital 2020: Ethiopia: <https://bit.ly/3bqGUzq>

25. World Bank, Individuals using internet (% population) Ethiopia: <https://bit.ly/3i3p6vm>

26. ITU report, Measuring Digital Development – Facts and Figures, 2019: <https://bit.ly/2LkOoet>

27. Web Foundation report, Women Rights Online, October 2020: <https://bit.ly/3br2bcg>

28. EIU, Inclusive Internet Index 2020: <https://bit.ly/2MTClDF>

PRIVACY, DIGITAL IDS AND SURVEILLANCE

After the Economic Intelligence Unit's Inclusive Internet index rating was recorded, authorities unveiled a COVID-19 monitoring platform in response. The multipurpose platform was to serve as a medium of information and to enable people who might have come into contact with infected persons to self-report. However, given the fact that Ethiopia does not have a comprehensive data protection plan, analysts expressed concerns over the potential misuse and or abuse of personal data due to weak regulatory framework.²⁹

According to Alt Advisory's Data Protection Africa Fact Sheet on Ethiopia,³⁰ the country had yet to enact a data protection law. It has been over a decade since a draft comprehensive data protection law was circulated in 2009. Two current

laws, the Freedom of Information and Access to Information as well as the Computer Crime Proclamations of 2008 and 2016 respectively, have sections that touch on the area of data protection. At the continental level, Ethiopia has yet to sign the African Union Convention on Cyber Security and Personal Data Protection as of May 2020 despite the convention having been adopted in 2014.

Another area that came up prominently was the SIM card registration draft law).³¹ In August 2020, the Ethiopia Communications Authority (ECA) released a draft directive in relation to this. ECA stated that the purpose was to facilitate stakeholder consultations, an encouraging signal of government's involvement of civil society in policy making processes.

CONCLUSION AND RECOMMENDATIONS



Government must work towards a data protection policy and while doing so, work with relevant civil society players at home and across the region. Government must ratify the African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention) and incorporate its provisions on data protection in local legislation.

Bridging the digital gender divide must also be prioritized along with rapid expansion of telecom infrastructure especially in the hinterlands and other under served areas across the country. Government must also respect international legislation that it is party to especially with respect to internet shutdowns and the targeting through social media of activists and journalists deemed to be critical of the government.

The establishment of an ICT "enabling legal and regulatory environment" is one of the main pillars of the 2019 Digital Transformation Strategy. Yet there are challenges which need a concerted effort by the government and all stakeholders to guarantee full enjoyment of rights online. From legislation to infrastructure, policy roll out to human rights, there is equally a lot of potential in strengthening digital rights in Ethiopia.

29. State of Internet Freedom in Africa 2020, Resetting Digital Rights Amidst the COVID-19 fallout, CIPESA; September 2020: <https://bit.ly/3nC5Gz0>

30. Alt Advisory – Ethiopia, Data Protection Africa, March 2020: <https://bit.ly/35q0pnW>

31. ECA, Final Draft, SIM Card registration drive, 2020: <https://bit.ly/3q61Yzm>



Ghana is located on the Atlantic coast of west Africa, bordered on the North by Burkina Faso, East by Togo, West by Ivory Coast and South by the Gulf of Guinea. It has an estimated population of 29 million and covers an area of 238,533 sq km.¹

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN GHANA

Ghana returned to constitutional democratic rule in 1993 after many episodes of military dictatorships interspersed by short stints of civilian regimes. This occurred between 1966 when Ghana's first President, Kwame Nkrumah was overthrown and the adoption of the 1992 Constitution, which ushered into being the Fourth Republic.² The 1992 Constitution established a multi-party unitary presidential system of government premised on universal adult suffrage and a decentralised local government system. The Constitution reiterates its supremacy as a fundamental value of the state and establishes "*a Supreme Court empowered to interpret the Constitution and strike down acts and omissions of the other branches of government which are inconsistent with the provisions of the Constitution*".³ The Constitution also guarantees a comprehensive list of civil and political rights and a limited number of socio-economic rights,⁴ which are supplemented by the directive principles of state policy in Chapter 6 of the Constitution. While the directive principles of state policy were initially thought to be unenforceable, judicial pronouncements from the Supreme Court have clarified that all provisions of the Constitution (including the directive



Military dictatorship
interspersed by short stints of civilian regimes

1. CIA Fact Book available at <https://www.cia.gov/library/publications/the-world-factbook/geos/gh.html>

2. K Quashigah 'The 1992 Constitution of Ghana' (2013), available at http://www.icla.up.ac.za/images/country_reports/ghana_country_report.pdf (accessed 7 October 2020); see also MG Nyarko 'The impact of the African Charter and Maputo Protocol in Ghana' in VO Ayeni (ed) The impact of the African Charter and Maputo Protocol in selected African states (2016) 95.

3. MG Nyarko (as above); article 2 of the 1992 Constitution.

4. Chapter 5 of the 1992 Constitution.

principles) are enforceable, unless there is a specific internal qualification concerning the non-enforceability of the provision.⁵ The legal system is modelled on the common law tradition inherited from the British colonial administration.

INTERNET PENETRATION, DIGITAL INFRASTRUCTURE AND REGULATION OF DIGITAL RIGHTS

Ghana has four active mobile network operators:

- MTN (67.78 % of data and 57.07% of voice),
- Vodafone (15.49% of data and 20.95% of voice),
- AirtelTigo (15.81% of data and 20.25% of voice)
- and Glo (0.92% of data and 1.74% of voice%).⁶

These in addition to 52 registered internet service providers (ISPs)⁷ make the internet sector quite competitive and the introduction of fibre has improved quality and reduced the cost of using the internet.⁸ However, the dominance of MTN in the sector has led the National Communications Authority to declare MTN a 'significant market power', to enable the regulator to implement policies to allow more competition.⁹ In 2020, in order to improve network access in remote communities, the Ghana Investment Fund for Electronic Communications backed the deployment of 2000 new OpenRAN sites to help network operators reach under served communities.¹⁰ In the midst of the COVID-19 pandemic, the government decided to temporarily reduce the Communication Service Tax, which increased from 6% to 9% in 2019, to 5% to enable network operators to reduce tariffs.¹¹

The introduction of fibre has improved quality and reduced the cost of using the internet.



5. Ghana Lotto Operators Association & Others v National Lottery Authority [2007-2008].

6. Y Kazeem 'Ghana's move to curtail MTN's market share is about mobile money, not voice' available at <https://qz.com/africa/1866059/ghana-to-cut-mtn-market-share-to-avoid-kenya-safaricom-domination/> (accessed 25 November 2020).

7. National Communications Authority 'Internet Service Providers' available at <https://www.nca.org.gh/assets/Uploads/ISP-Operational.pdf>

8. Alliance for Affordable Internet 'Ghana: Expanding international connectivity' (2019) Good Practices Database. Washington DC: Web Foundation, available at <https://a4ai.org/studies/expanding-international-connectivity/>

9. Reuters 'Ghana to reduce MTN's telecoms market share' available at <https://www.reuters.com/article/ghana-mtngroup-idUSL8N2DL41B>

10. Alliance for Affordable Internet '2020 Affordability report' available at <https://a4ai.org/affordability-report/report/2020/>

11. As above; see also Ghana Chamber of Telecommunications 'Mobile industry modifies tariffs in accordance with amended communications service tax law', available at <https://telecomschamber.com/news-media/media-releases/mobile-industry-modifies-tariffs-in-accordance-with-amended-communication-service-tax-cst-law>

Ghana has a rapidly evolving, vibrant digital technology ecosystem that has grown exponentially since 2005.¹² Internet penetration was pegged between 30.3%¹³ and 48% as at January 2020 with 14.76 million internet users - a 1 million (7.5%) increase between 2019 and 2020.¹⁴ A majority of internet users (94%) connect through mobile internet at an average speed of 18.38 mbps.¹⁵ There were a total of 6 million social media users as at January 2020 representing 20% of the population, 98% of which are accessed via mobile.¹⁶ WhatsApp (82%), Facebook (71%), YouTube (62%) and Instagram (61%) are the most used social media platforms.¹⁷ Ghana has a very high mobile connection rate, with an estimated 39.97 million mobile connections as at January 2020, equivalent to 130% of the total population.¹⁸ Despite this impressive subscription rate, mobile penetration at the end of 2019 stood at a modest 55%. While still quite low, Ghana's mobile penetration rate is the highest in the West Africa region and above the Sub-Saharan Africa average of 44.8%.¹⁹

The communications sector is under the policy supervision of the Ministry of Communication and the National Communications Authority, while the Data Protection Commission is charged with the protection of the privacy of individual and personal data. The sector is regulated by the 1992 Constitution, the National Communications Authority Act, 2008 (Act 769), the Electronic

Communications Act, 2008 (Act 775), the Electronic Transactions Act, 2008 (Act 772), the National Information Technology Agency Act, 2008 (Act 771), the Communications Service Tax Act, 2008 (Act 754), the Data Protection Act, 2012 (Act 843)²⁰ and various regulations and guidelines issued under these laws.²¹

GENDER AND DIGITAL ACCESS

Significant strides have been made in closing the gender gap in internet access with one study suggesting that the gender gap in internet access was 5.8%, far below the global average of 21%.²² The gender gap however, increases to 14% when it comes to meaningful connectivity.²³ Poor service quality and availability in rural areas, coupled with high cost of data further exacerbates the gender divide in rural areas.²⁴ Recent data also suggests that women and girls are significantly under represented on social media platforms. For instance, only 38.4% of 1.4 million Instagram accounts reachable by advertisement are reported to be female users against 61.6% for men.²⁵ Similar ratios apply to LinkedIn subscriptions, with about 31.5% of the 1.4 million accounts reachable by advertisements belonging to females, while 68.5% belong to males. The figures are even worse for Twitter, with only 25.1% of the 555.5 thousand accounts reachable by advertisement belonging to females against 74.9% for males.²⁶

12. GSAM 'Country overview: Ghana – Driving mobile-enabled digital transformation'(2-17) 7, available at <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/Ghana-Country-Overview.pdf>

13. World Wide Web Foundation 'Women's rights online: Closing the digital gender gap for a more equal world' (2020) 12, available at <http://webfoundation.org/docs/2020/10/Womens-Rights-Online-Report-1.pdf>

14. Dataportal 'Digital 2020: Ghana', available at <https://datareportal.com/reports/digital-2020-ghana>

15. As above.

16. As above.

17. As above.

18. As above.

19. G Omondi 'The state of mobile in Ghana's tech ecosystem' (2020), available at <https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-in-ghanas-tech-ecosystem/>

20. <https://www.dataprotection.org.gh/resources/downloads/data-protection-act/38-data-protection-act-2012-act-843/file>

21. The database of legislation and regulations can be access at <https://www.nca.org.gh/regulatory-framework/legislations/>

22. World Wide Web Foundation 'Women's rights online: Closing the digital gender gap for a more equal world' (2020), available at <http://webfoundation.org/docs/2020/10/Womens-Rights-Online-Report-1.pdf>

23. As above, 12.

24. As above, 13-14

25. Dataportal 'Digital 2020:Ghana' available at <https://datareportal.com/reports/digital-2020-ghana>

26. As above.



There was a total of 6 million social media users as at January 2020 representing 20% of the population, 98% of which are accessed via mobile.

REGULATION OF SPEECH: HATE SPEECH, MISINFORMATION AND CRIMINAL DEFAMATION

Freedom of expression is guaranteed in the Constitution and generally respected in practice both online and print.²⁷ The repeal of the criminal defamation and sedition laws in 2001 has further enhanced the enjoyment of freedom of expression.²⁸

Parliament passed the Right to Information Act in March 2020, which was assented to by the President in May 2020.²⁹ However, there are occasional instances where security agencies have been reported to harass and arrest journalists who report on politically sensitive issues. For instance, in June 2019 two journalists from the website modernghana.com were arrested by personnel from the Ministry of National Security in connection with an article they published on the Minister. They were allegedly tortured while in custody and released two days later.³⁰



Journalists
harassed & arrested
by security agencies

27. Freedom House 'Freedom in the world 2020: Ghana' (2020), available at <https://freedomhouse.org/country/ghana/freedom-world/2020>

28. E Laryea & K Kwansa-Aidoo 'Going, going, gone! Implications of the repeal of criminal libel and sedition laws in Ghana' (2005) 8 Ghana Studies 127; O Anku-Tsede 'The media and offence of criminal libel in Ghana: Sankofa' (2013) 9 Journal of Law, Policy and Globalization 26; R Acheampong 'Repeal of the criminal libel law in Ghana: Challenges and prospects for journalism' (2017) 1 International Journal of Management and Scientific Research 79.

29. DW 'Are Ghanaians ready to take advantage of the right to information law?', available at <https://www.dw.com/en/are-ghanaians-ready-to-take-advantage-of-the-new-right-to-information-law/a-52171600>

30. As above.

While there is currently no specific law to counter disinformation, the Criminal and Other Offences Act³² and the Electronic Communications Act both contain provisions that can be used to prosecute online speech. Section 208 of the Criminal and Other Offences Act criminalises the publication or reproduction of *'any statement, rumour or report which is likely to cause fear and alarm to the public or to disturb the public peace knowing or having reason to believe that the statement, rumour or report is false'*.

While this is classified as a misdemeanor, the punishment for misdemeanor under section 296 of the Criminal Procedure Act indicates the penalty for misdemeanor as a punishment of up to three years' imprisonment, which would clearly be excessive if the maximum sentence were to be imposed. Similarly, section 76 of the Electronic Communications Act³³ prohibits *'knowingly sending a communication which is false or misleading and likely to prejudice the efficiency of life saving service or to endanger the safety of any person, ship, aircraft, vessel or vehicle'* by means of electronic communication. The penalty for infringing this section is a fine or term of imprisonment up to a maximum of five years or both.

In May 2020, it was reported that an individual was arrested and charged under section 76 of the Electronic Communications Act for disseminating a video on YouTube encouraging Ghanaians to kill police officers and burn the house of the president alleging that partial lockdowns that were imposed were a ploy by the government to lay 5G cables.³⁴

IMPACT OF COVID-19 REGULATION ON DIGITAL RIGHTS AND INCLUSION

The COVID-19 pandemic and regulations adopted to counter the impact of the pandemic have impacted on digital rights in various ways. In addition to some of the developments highlighted earlier, another significant development in light of the COVID-19 pandemic, was the adoption of the Establishment of Emergency Communications System Instrument, 2020 (E.I. 63) under section 100 of the Electronic Communications Act. EI 63 requires network operators and other communications services providers to place at the state's disposal their services for the mass dissemination of information in cases of emergency, including public health emergencies. In such emergencies the network operators are also required to provide subscriber information to the National Communications Authority and other state agencies when requested, including caller and called numbers, merchant codes, mobile station international subscriber directory number codes, international mobile equipment identity codes and site locations, roaming files and location log files.³⁵

While this instrument was adopted in the context of enabling contact tracing in combating the COVID-19 pandemic, the broad powers have been criticized as potentially providing an avenue to be deployed for mass surveillance in violation of the right to privacy.³⁶

31. Criminal and Other Offences Act, 1960 (Act 29), available at <https://www.wipo.int/edocs/lexdocs/laws/en/gh/gh010en.pdf>

32. Criminal Procedure Act, 1960 (Act 30).

33. Electronic Communications Act, 2008 (Act 775), available at <https://www.moc.gov.gh/sites/default/files/downloads/Electronic%20Communications%20Act-775.pdf>

34. Disinformation Tracker 'Ghana', <https://www.disinformationtracker.org> (accessed 24 November 2020); D Apinga 'Kill police Officers, burn Akufo-Addo's house – Social media alarmist' available at <https://www.theghanareport.com/kill-police-officers-burn-akufo-addos-house-social-media-alarmist/>

35. Section 1 of EI 63, available at <https://verfassungsblog.de/wp-content/uploads/2020/05/E.I.-63.pdf>

36. K Agyeman-Budu 'Constitutionalism and COVID-19 in Ghana', available at <https://ancl-radc.org.za/node/627>

On a positive note, in May 2020 the government of Ghana launched the Digital Financial Services Policy³⁷ aimed at, among others, improving financial inclusion through the use of digital platforms. Even though the policy has been on the drawing board for some years now, there are indications that its eventual launch provides an important tool in the arsenal of the government's COVID-19 response, which inevitably includes measures to cope with social distancing, which requires less reliance on cash.³⁸

The Criminal and Other Offences Act and the Electronic Communications Act both contain provisions that can be used to prosecute online speech.

CONCLUSION AND RECOMMENDATIONS

While Ghana has made some good progress in expanding access and providing a liberal regime on digital rights, including the recent launch of the Digital Financial Services Policy, there are still concerns that need to be addressed by the government and keenly watched by civil society and other stakeholders.

For instance, the glaring digital divide between genders and between rural and urban areas requires continuous attention and improvement.

One of the measures that can be adopted to address this challenge is taking another look at the cost of accessing the internet and ensuring that tariffs and other taxes imposed by the government that impacts on affordability are reduced or removed.

Government should also ward off the temptation to use the COVID-19 pandemic as an excuse to engage in mass surveillance or curtail online expressions through the wrongful use of 'fake news' or misinformation laws.



37. Ministry of Finance 'Digital Financial Services Policy' (2020), available at https://mofep.gov.gh/sites/default/files/acts/Ghana_DFS_Policy.pdf

38. Consultative Group to Assist the Poor (CCAP) 'Ghana launches world's first digital finance policy amid COVID-19' (May 2020), available at <https://www.cgap.org/blog/ghana-launches-worlds-first-digital-finance-policy-amid-covid-19>



Kenya is an Information and Communication Technology hub, informally known as the 'Silicon Savannah' for its innovations in technology. That does not, however, mean that Kenya is not immune to the digital divide.

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN KENYA

The cost of internet access is one of the most expensive in the region which has led to the digital exclusion of mostly youth and women. This has consequently led to violations of human rights such as the right to access to information. The country is home to hundreds of technology companies and ICT start-ups. The state of the digital spectrum in Kenya is in focus in this segment of the report. The data in this section was obtained through a review of the various reports of the ICT authorities in the country, individual company reports as well as credible media reports.

IMPACT OF COVID-19 ON DIGITAL RIGHTS AND INCLUSION

The COVID-19 pandemic has brought to the fore the inequalities in access to the internet and digital technologies in Kenya. The untimely pandemic has also been a timely reminder of the stark inequalities in internet access and digital technologies among young people in Kenya. The enjoyment of freedom of expression online in 2020 in the country was characterized by a surge in the numbers of internet users due to the fact that the government did not restrict access.



Freedom
of Expression online

As of 2020, Kenya had an internet penetration of approximately 87%. This high rate is mainly because Kenya is home to M-PESA, which is a mobile wallet provider and the secure payment system encourages internet access.¹ According to the Communication Authority of Kenya, internet subscriptions in Kenya rose about 5.1% between April and June 2020 as demand for the service surged amid stay-at-home measures imposed by the government as a result of the COVID-19 pandemic. Subscriptions increased to 40.9 million in June 2020, up from 38.9 million in the period ending March 2020. The Communication Authority of Kenya attributed the rise to increased demand for access to information online, coupled with transfer of more services to the digital space during the pandemic period.²

Additionally, the country has a largely independent judicial system and has developed jurisprudence in the area of digital rights. Courts of law have issued progressive and liberal judicial pronouncements geared towards ensuring that the digital rights of the country's citizens are respected, their privacy is guaranteed and that the citizens are able to access courts for redress in case of an alleged violation, pursuant to the country's Bill of Rights. Additionally, Kenya has a robust Bill of Rights and Article 35 specifically provides for access to information. The Access to Information Act, 2016 seeks to operationalize this Constitutional provision. Further, the Data Protection Act seeks to offer data protection. Despite the challenges presented by the COVID-19 pandemic that re-directed the country's attention, Kenya made some positive strides in digital rights and digital inclusion in the year 2020. Some key developments included the following:



PRIVACY, DIGITAL IDS AND SURVEILLANCE

■ Appointment of a Data Commissioner

Pursuant to the Data Protection Act No. 24 of 2019, President Uhuru Kenyatta nominated Immaculate Kassait as Kenya's Data Commissioner.³ The Commissioner is expected to put in place structures and systems for the protection of personal citizen's data as per the directions given by the High Court in the Huduma Number case. The Huduma number that was rolled out beginning December 2020 presented challenges relating to data protection and privacy. The Data Commissioner will be responsible for establishing and maintaining a register of data controllers and data processors; exercising oversight on data processing operations and receiving and investigating any complaint by any person on infringements of the rights under the Act. The Act, for instance, requires that personal data can only be "collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes."⁴

1. See Share of internet users in Africa as of March 2020, by country, <https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/>
 2. Fourth Quarter Sector Statistics Report for the Financial Year 2019/20 (April-June 2020), <https://ca.go.ke/wp-content/uploads/2020/10/Sector-Statistics-Report-Q4-2019-2020.pdf>

3. Immaculate Kassait sworn in as Data Commissioner, <https://www.kbc.co.ke/immaculate-kassait-sworn-in-as-data-commissioner/>

4. Data Protection Act, 2019 Available at http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct_No24of2019.pdf

■ Huduma Number/ National Integrated Identity Management System (NIIMS) Case

The government of Kenya introduced a national database: the National Integrated Identity Management System. The Huduma Number proposals were challenged in the High Court of Kenya by human rights organizations due to, among others, a need for public participation and an argument that the proposals sought to disenfranchise already marginalized groups in Kenya such as stateless persons. One more controversial aspect of this government project was the fact that the registration for the Huduma Number was a prerequisite to the provision of government services such as healthcare. The High Court subsequently determined that the government move was constitutional as long as that information was properly protected. The court also observed that any collection of DNA and the recording of a person's precise location was intrusive and unconstitutional as it was a breach of their privacy.⁵

The petitioners disagreed with particular sections of the High Court's judgment on this matter and they filed an appeal at the Court of Appeal. This appeal is yet to be heard and conclusively determined.

Notably, the Huduma Bill does not have sufficient provisions on data protection measures. The introduction of a centralized population register with the sharing of data across a range of functional government and/or private databases and users for a wide range of services and transactions presents a risk to privacy that is categorically different from the prevailing situation where the data is stored in separate databases. The Bill proposes various penal measures for non-compliance with various provisions of the Bill.⁶ The hope is that the Huduma number will be implemented in strict compliance with the decision of the High Court in the case so as to protect citizen's personal data.

HATE SPEECH, MISINFORMATION AND CRIMINAL DEFAMATION LAWS

The Computer Misuse and Cybercrimes Act⁷

In July 2019 the Senate moved to the High Court to challenge the constitutionality of 24 laws that were passed by the National Assembly without the involvement of the Senate, one of the chambers of Parliament. Kenya is a bicameral legislature with a two-chamber Parliament. After hearing and determining the petition, the High Court of Kenya voided a number of bills that were passed by the National Assembly that did not involve the Senate. The laws that were nullified included the Computer Misuse and Cybercrimes Act, Kenya's principal ICT legislation. The High Court suspended their ruling for nine months to grant parliament adequate time to right the wrongs as pointed out by the court. The National Assembly has threatened to file an appeal against this judgment. The implication of the decision of the High Court is that the laws will cease to be in application at the lapse of the nine months, in compliance with the court order.

5. Huduma Namba: Kenya court halts biometric ID over data fears: <https://www.bbc.com/news/world-africa-51324954>

6. Seven Things You Should Know About Huduma Number, <https://icj-kenya.org/news/latest-news/271-seven-things-you-should-know-about-huduma-namba>

7. High Court nullifies 23 laws passed without Senate's approval, <https://www.businessdailyafrica.com/bd/news/high-court-nullifies-24-laws-senate-s-approval-2725652>



“

Kenya made some positive strides in digital rights and digital inclusion in the year 2020.

DIGITAL EXCLUSION

■ Gender and ICT

Many women in Kenya do not have access to mobile phones and some possess only a SIM card which means that they rely on friends and neighbours to access telephony services. It is important to understand the challenges that women face in accessing digital resources. Three main challenges that are often identified include

affordability, relevance and lack of digital skills amongst members of particular genders. The country's digital infrastructure is less robust and there is a rural-urban divide as well as gender digital exclusion in parts of the country especially in the North.

CONCLUSION AND RECOMMENDATIONS



- Government should seek to address the digital inclusion inequalities during and after the COVID-19 pandemic.
- Government ought to address the gender inequality gap to ensure that both men and women as well as young people have unrestricted access to the internet.
- Government must ensure that the planned Huduma number roll-out does not infringe on human rights and its implementation is as per the court decision in the Huduma number case.



Case Study: The threat to data privacy in Kenya in the time of COVID-19

Compiled by Ekai Nabenyio

Even though the COVID-19 pandemic is global, the development and implementation of contact tracing has taken place only on national levels. At the onset of the COVID-19 pandemic, different methods were used by the Kenyan government to contain the spread of the pandemic. This included a mandatory quarantine order for all persons travelling into Kenya. Chali Baluu (name changed), a Kenyan citizen, reported human rights violations to the Kenya Human Rights Commission, complaining that his communication devices, specifically his mobile phones, were being monitored by government authorities. Numerous incidents were also reported on the State's tapping of phones and eavesdropping on private communications. Additionally, as a COVID-19 patient, Chali Balu indicated to the Kenya Human Rights Commission (KHRC) that while placed under mandatory quarantine at Jomo Kenyatta International Airport in Nairobi, in compliance with the government directive, they were placed under 24/7 surveillance.

The challenge faced by the KHRC in monitoring the veracity or otherwise of these violations included the fact that it was not easy to prove monitoring of communication devices despite the seriousness of the allegations made. Individuals reported incidents to the KHRC in which they were placed under mandatory quarantine for periods more than the stated 14 days. This meant more surveillance for longer or indefinite periods. Further, the fact that staff of KHRC worked virtually meant that they received and handled these reports of violations virtually. This affected the credibility that is easier to prove during face to face communication. It also means that some cases of those less tech-savvy victims that would have otherwise paid a visit to the offices of the Commission may have gone unreported. Journalists that attempted to relay the information on COVID-19 human rights violations to the general public were often arrested as surveillance was extended to media houses, and vandalism was reported. The Media Council of Kenya did raise a complaint against this violation which essentially violated the right to access information guaranteed under the Constitution of Kenya, 2010. Article 35 (1) of the Constitution of Kenya states as follows:



Every citizen has the right of access to--

(a) information held by the State; and

(b) information held by another person and required for the exercise or protection of any right or fundamental freedom.

(2) Every person has the right to the correction or deletion of untrue or misleading information that affects the person.

(3) The State shall publish and publicize any important information affecting the nation.

Regional and international human rights instruments such as The Declaration of Principles of Freedom of Expression and Access to Information in Africa demand that for any restriction on access to information held by public authorities to be allowed by law, it must have a legitimate aim, be necessary, proportionate to the aim of safeguarding public health, and must also be restricted to only the existence of the crisis. This means that any limitations of human rights should be justified. Information accessibility is a key component of the right to health and countries such as Kenya are urged to comply. When officials do not publish health information proactively, populations suffer adverse health impacts and cannot fully enjoy their right to health as guaranteed. Kenya needs to be open and transparent, responsive and accountable to the citizens in the fight against COVID-19.

The reduction in the public's right to know about the activities of their governments is counter-productive to the effort in combating the COVID-19 outbreak. The right to information is crucial for ensuring public awareness and trust, fighting misinformation, ensuring accountability as well as developing and monitoring implementation of public policies aimed at solving the crisis. It is crucial that the right to information is maintained during the emergency as much as possible.



Case Study: Safe-guarding Kenyans' data amidst a pandemic

Compiled by Ekai Nabenyio

Contact tracing, as a public health management process of identifying persons (including healthcare workers) who have had contact with individuals with probable or confirmed COVID-19 infection, has been applied in Kenya, as in other countries. Contact tracing is meant to identify potential secondary cases that may arise from a primary COVID-19 case. This intervention has helped avoid further onward transmission by victims. The implementation of contact tracing in Kenya by the Ministry of Health, in coordination with law enforcement, has not been without controversy and has raised various human rights concerns. Important considerations include the effectiveness of contact tracing and the concomitant impact on privacy and human rights. The shortcomings of contact tracing go beyond privacy considerations and potentially infringe on other human rights. While the various accounts as narrated by the respondents are true, the names that have been used in this case study have been deliberately modified to hide the true identity of the respondents.

A journalist at The Standard Media Group received reports from Wanjiru Kemboi whose phone calls and other communications were believed to be intercepted by government surveillance agencies. It was also apparent that the affected individuals did not understand their digital rights. Wanjiru who had been subjected to the 14-day mandatory quarantine period contacted the journalist as she had a strong suspicion that her mobile phones were tapped, although she seemed to not be concerned about it. Wanjiru had an experience in which a National Intelligence Service official contacted her, as a patient that was supposed to be on self-quarantine, warning Wanjiru against going to the market and mingling with others on a day when she actually attempted to go to the market. Wanjiru Kemboi complied with the order and retreated back to quarantine. This was a clear testament that the patient was being monitored by the National Intelligence Service in liaison with the Health Surveillance agencies. This meant that the COVID-19 patient lived in constant fear while in private confinement and did not have an assurance about the protection of their privacy. It was also not clear what the extent of the penetration of the surveillance by the National Intelligence Service, and the Health Surveillance, was.



This clearly violated the individual's right to privacy, even in the face of the COVID-19 pandemic, as guaranteed in the Bill of Rights of the Constitution of Kenya, 2010. This revelation raises questions as to how the COVID-19 patient's data is used and how long it should be stored on national security databases. The concern here is the possibility of surveillance by the State, particularly should data use and storage not be legally safeguarded. Individuals' right to privacy can be affected by digital data collection and processing. In developing solutions to address crises, State institutions and regulators should do their utmost to balance the right to privacy and the right to information when there is a potential conflict between them. Numerous other cases were reported, especially after the journalist penned an article to report cases of increased tapping of phone calls by State agencies.

In conclusion, injurious contact tracing that violates human rights breeds suspicions between the State and the citizenry. To right the wrongs that have characterized contact tracing in Kenya, it is recommended that there is an urgent need for Health Surveillance authorities and officers of the National Intelligence Service to comply with the provisions of the Data Protection Act, 2019, as far as the protection of citizen's private data is concerned. The State should take appropriate measures to safeguard data and to regulate who has access to the same.

The Government of Kenya introduced the mSafiri App, a brain-child of a collaboration between Kenya's Ministry of Health and the Ministry of Transport, in containing the spread of the virus. The app was designed to provide critical data that would help trace back the movements of infected or suspected COVID-19 cases. This Digital Health Surveillance tool necessitated the need for the government to be transparent on how the data collected was used but the lack of guiding principles, as far as contact tracing is concerned, was a point of concern raised. There were concerns by particular patients that the Government of Kenya was not able to manage these technologies and therefore contracted third parties-technology companies. As a result, this has presented an opportunity for abuse of health surveillance data as there are no known Data Sharing Agreements with such third parties. This is critical as it is feared that intra-government use of data in Kenya may be mostly utilised for security reasons; there is a need to safeguard against this.



Malawi is a landlocked country that borders Tanzania, Zambia and Mozambique. The country has an estimated population of 17.7 million people, of which 85% live in rural areas.¹ The Gross Domestic Capital (GDP) per Capita is estimated at USD \$516.80.²

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN MALAWI

Most women work in the agricultural sector which is a backbone of Malawi's economy. Of those in non-agricultural waged employment, 21% are women and 79% are men and the numbers have remained the same over the years. In spite of various structural reforms in recent years, Malawi continues to rank as one of the least developed countries in the world, constantly affected by high levels of poverty and climate change vulnerabilities such as flooding and excessive rain.

The advent of internet and exponential growth of access to it and other Information and Communication Technologies (ICTs),³ have made digital rights become indispensable to the way people around the world exercise and enjoy their fundamental human rights.⁴ Malawi, like other African countries, has enacted a number of laws that contain provisions on digital rights.⁵ These provisions recognise that the same rights that people have offline, such as freedom of expression, access to information, and the rights to privacy, must also be protected in digital spaces.



**Access to
Information**

1. World Bank. (2020). World Bank Indicators. <http://data.worldbank.org/indicator/SP.POP.TOTL>

2. World Bank. (2019). World Bank Indicators. <http://data.worldbank.org/indicator/SP.POP.TOTL>

3. <https://www.gp-digital.org/wp-content/uploads/pubs/african-declaration-a-positive-agenda-for-rights-online.pdf>

4. https://cipesa.org/?wpfb_dl=287

5. <https://africadigitalrightshub.org/wp-content/uploads/2020/03/Data-Protection-Code-of-PracticeEnglish-Soft-Copy.pdf>

This article aims at assessing the status of digital rights in Malawi for 2020. The study uses a literature review and key informant interviews to generate an understanding on the current debates and issues surrounding the state of digital rights in Malawi. The article analyses the laws and policy frameworks on digital rights particularly those that govern the telecommunication sector, the media, social media, privacy and security and law enforcement. The article discusses thematic areas related to internet access and infrastructure; impact of covid-19 regulations on digital rights; and privacy, digital IDs and surveillance.

POLITICAL LANDSCAPE AND DIGITAL RIGHTS

Malawi is a multi-party state and has been a relatively peaceful country. In May 2020, the country made history when a rerun of presidential elections was conducted after the first results of the May 2019 were annulled by the Constitutional court. The opposition candidate, Dr. Lazarus Chakwera, under the political umbrella “Tonse Alliance”, won the presidential election with a 58.9% majority. The annulment came after months of sustained citizen protests against electoral fraud marred with systemic irregularities. Most of the protests were led by the Human Rights Defenders Coalition (HRDC).⁶ They organised and spread their messages using social media such as WhatsApp, Facebook, and Twitter. Consequently, Malawi received international praise as a beacon of democracy for being the second in Africa to re-run its presidential election after a court annulment, and the very first time in history for an opposition presidential candidate to win the election.



INTERNET AND ICT ACCESS

Despite momentous victory for democracy in the country in 2020, Malawians still face systemic threats of human rights in the digital space.

International Telecommunication Union (ITU) statistics show that 14% of the population use the internet in Malawi while 52% have mobile phones. Access to mobile broadband is estimated at 25.5% and fixed line broadband is 0.06%.⁷

There are also gender disparities when it comes to ICT ownership in the country. About 34.2% of women own a mobile phone, 3.9% own a desktop computer, while just 5.2% of them have internet access compared to their male counterparts.⁸

Likewise, 3.0% of the population have access to internet access in rural areas compared to 24.3% in urban population. Computer access in rural areas remains at 2.1% against 19.2% in urban areas. In Malawi, Airtel (Mw) and Telecom Networks Malawi remain the two dominant mobile operators in Malawi, while Malawi Telecommunication Limited (MTL), remains the only fixed service provider.

6. <https://afrobarometer.org/publications/ad354-malawians-support-2019-post-election-demonstrations-split-government-power-limit>

7. <https://www.itu.int/net4/ITU-D/idi/2017/>

8. https://giswatch.org/sites/default/files/gisw2019_web_malawi.pdf

The Malawi Communication and Regulatory Authority (MACRA) regulates the telecommunication sector in the country.

Poor access to ICT services such as the internet are largely attributed to poor ICT infrastructure and high tariff charges imposed on ICT services. These include 16.5% value added tax (VAT) on internet services, 17.5% VAT on mobile phone and services, and 10% on excise duty on mobile text messages and mobile data transfers.⁹ Access to the Internet is cost-prohibitive to the majority of Malawians. For instance, a monthly data bundle of 10 Gigabytes (GB) costs \$21 with both Airtel and Telecom Networks Malawi (TNM). This cost is equivalent to half the minimum monthly wage of the majority of Malawians. In addition, the Inclusive Internet Index 2020, which measures internet affordability, availability, relevance of content and readiness, ranks Malawi 97 out of 100 countries.

FREEDOM OF EXPRESSION AND ONLINE SURVEILLANCE

The Electronic Transactions and Cyber Security Act of 2016 restricts citizen participation in the digital space.¹⁰ Section 24(2)(e) of the Act states that online communication may be restricted in order to “protect order and national security,” while Section 24(2)(f) states that online communication may be restricted in order to “*facilitate technical restriction to conditional access to online communication.*”¹¹ Further, Section 31(1) of the Act requires that “online content providers to conspicuously display on their webpage the full name, domicile, telephone number, email address of the editor if a natural person; and in the case of a legal entity, the

corporation name, postal and physical address of the registered office, telephone number and email address and registration number of the editor”.¹² This provision gives penalties of fines or a maximum of 12 month prison sentence, and places restrictions on encryption.

This provision is also similar to Section 3 of the Printed and Publication Act, 1947. Although, no one has been charged with this provision, its presence limits citizens’ rights to anonymity, more so that the provision carries a hefty punishment-custodial sentence of 12 month and a heavy fine of MWK 5000,0000 (\$6,600).

In addition to these pieces of legislations, there are also other adverse laws that were inherited from the British colonial rule (1891-1964) and during the one party system dictatorial government era (1964-1994), which threaten participation of Malawian citizens both offline and online. For instance, Sections 50 and 51 of the Penal Code, which establishes the offence of sedition, while Section 4 of the Protected Flag, Emblems and Names Act, makes it an offence to “*do an act or utter any words or publish or utter any writing calculated to insult, ridicule or to show disrespect*” to “*the president, the national flag, armorial ensigns, the public seal or any protected emblem or protected likeness*”.¹³ These laws combined have in one way or the other perpetuated digital rights violations in Malawi. The digital rights violations have taken many forms including access restriction to the internet, criminalisation of some forms of online communication, and state online surveillance.¹⁴

9. Kaiyatsa.M.(2020, August). Digital rights remain under threat in Malawi despite historic win for democracy.

<https://advoc.globalvoices.org/2020/08/05/digital-rights-remain-under-threat-in-malawi-despite-historic-win-for-democracy/>

10. <https://crm.misa.org/upload/web/e-transactions-act-2016.pdf>

11. <https://crm.misa.org/upload/web/e-transactions-act-2016.pdf>

12. <https://crm.misa.org/upload/web/e-transactions-act-2016.pdf>

13. <https://crm.misa.org/upload/web/17-laws-of-malawi-protected-flag-emblems-and-names.pdf>

14. <https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/malawi/>



“

The digital rights violations have taken many forms including access restriction to the internet, criminalisation of some forms of online communication, and state online surveillance

DATA PRIVACY, PROTECTION AND DIGITAL IDENTITY

Data privacy and protection remains an elusive issue in the country. Government departments such as the Immigration, Road Traffic Directorate, National Registration Bureau (NRB), Malawi Electoral Commission (MEC), National Statistics Organisation (NSO), and service providing institutions such as hospitals and education institutions, as well as the banks continue to collect vast amount of personal data.¹⁵ Recently, telecom companies in the country have also been collecting large amounts of a lot of personal data, more so with the introduction of mandatory SIM card registration as entailed in the Malawi Communication Act of 2016 entails. However, there is no available data on how much information each of these bodies collects or how

well they are complying with existing laws such as the Electronic Transaction Act, 2016 and Access to Information Act, 2016. In addition, the majority of ordinary Malawians are not even aware of the implications of digital identity collection on their privacy.

Moreover, Malawi does not have a stand-alone privacy and protection law.¹⁶ Consequently, data privacy and protection of citizens continues to be at risk, which is in itself a violation of digital rights violations. Moreover, a lack of comprehensive data protection laws in the country, also means that there is no single body mandated to regulate the collection of personal data in the country.

15. https://www.researchgate.net/publication/341151585_State_of_Internet_Freedom_in_Malawi_2019_Mapping_Trends_in_Government_Internet_Controls_1999-2019

16. https://www.researchgate.net/publication/335136113_State_of_Internet_Freedom_in_Malawi_Privacy_and_Personal_Data_Challenges_and_Trends_in_Malawi?_sg=eL8QxUyOjicWRRsr_lcfz8lwzG9-NEjiXsxeSvke9x4uoR3VNhfC_YOjYHfad9B07TtbQivjH2nyA3spuZJO-11Q_Qvpe4PaaOWnzCOX.gjBACMVxEB4mFX1tfP8Q6QILtFBHKf1s-Q9CVzPz1Tm--E6eu1CY7lkvXhSsJo8ogQErUf9g4UJwzetsAWYqX

IMPACT OF COVID-19 REGULATIONS ON DIGITAL RIGHTS

Like other countries in the world, Malawi was not spared of the COVID-19 pandemic. Mobile phones, internet, social media, and other digital platforms which were supposed to be enablers of women and girls empowerment, instead became weapons against them. Due to restrictive movements and other measures imposed by government, many women and girls were victimised online in the form of cyberstalking, online harassment, online defamation and cyber bullying among others.¹⁷ Consequently, little attention is paid to address this issue which is increasing at an unprecedented rate in the country.¹⁸

Although digital rights violations continue to take center stage at both national and global agenda, in 2020, we have seen the Malawi government making some notable commitments to promote human rights in the digital space in this regard. Soon after President Chakwera was inaugurated as the 6th President of the Republic of Malawi, he categorically promised to operationalise the Access to Information Act of 2016.¹⁹ Indeed on 30th September, the Act was operationalised.²⁰ Civil society and international government organisations applauded the government for taking this decisive action. The operationalization of this Act will eliminate the culture of secrecy, and will make the government more transparent and accountable to its citizens. However, there are still other challenges that need to be addressed before the Act can be fully operational. For instance, Section 7 of the same Act demands *“the establishment of a Public Information Commission to oversee the implementation of this Act”*. However, no such body has been commissioned to perform such oversight functions.²¹

***Digital platforms became weapons
against women.***



17. https://africaninternetrights.org/sites/default/files/Donald_Flywell-1.pdf

18. <https://www.apc.org/en/pubs/tackling-gender-based-cyber-violence-against-women-and-girls-malawi-amidst-covid-19-pandemic>

19. <https://malawi24.com/2020/09/19/cso-hails-govt-for-operationalizing-ati/>

20. <https://www.nyasatimes.com/un-commends-malawi-for-operationalization-of-access-to-information-law/>

21. https://www.right2info.org/laws/malawiaccessinfo.pdf/at_download/file

Equally important, Malawi's leading telecoms TNM and Airtel reduced data prices of internet.²² Airtel announced new prices with reductions of up to 40% with increased profit of 588% in 2019,²³ while TNM also reduced data prices on July 30, 2020, despite the company recording 10% profit reductions in 2019 compared to 2018.

While some citizens considered data price reductions as a welcome development, others criticized the move as cosmetic in nature since little positive impact change is being felt by the citizens. Nevertheless, there has been improvement in participation of citizens online due to this reduction in data prices of the internet.

CONCLUSION AND RECOMMENDATIONS



From the foregoing, it is evident that 2020 was a mixed bag in the context of digital rights in Malawi. Digital rights violations such as costly internet access, cyber violence and against women and girls, state online surveillance, absence of online personal privacy and data protection continue to threaten freedom of expression of citizens in the digital space. This is further exacerbated by weak policy and regulatory frameworks, and use of draconian laws inherited from both the colonial era and during the one party's dictatorial era (1964-1994) which have yet to be repealed. Nevertheless, the current government leadership under President Chakwera, has also shown some political commitments to ensure that internet and ICTs devices become affordable and accessible to all Malawians. This has been demonstrated by scaling down the prices of internet bundles, continued establishment of telecentres in rural areas, operationalization of the Access to Information Act of 2016, among others. Of recent, there have been no reported cases of civic space crackdowns as compared to the same year in 2019.

Based on this conclusion, the recommendations are as follows:

- Government should urgently develop a stand-alone data protection law to ensure that citizens' personal data are protected both in the physical and online spaces.
- Government should repeal draconian laws which infringe the freedom of expression of citizens online such as the Sedition Act, Penal code, and the Electronic Transaction and Cyber security Act.
- Government should review the National Action Plan to Combat all forms of gender based violence and integrate online gender based violence issues. This will ensure women and girls' online safety and security, and where such misconduct occurs proper due process must be complied with.
- Government needs to remove high tax charges imposed on importation of ICT gadgets to ensure accessibility and affordability of ICT services for the marginalised population. This will narrow the digital inequality that currently exists in the country.

22. <https://cipesa.org/2020/08/malawi-telcos-reduce-data-prices-in-response-to-cipesa-chrr-campaign-2/>

23. <https://times.mw/airtel-profit-up-by-588/#:~:text=Malawi%20Stock%20Exchange%20recent%20entrant,by%20the%20company%20has%20shown.>



Namibia is a southern African country with a population of 2.5 million inhabitants. Having gained independence in 1990, democracy is generally regarded as thriving and the rule of law is intact. Although it is an upper-middle-income country, Namibia has one of the highest rates of income inequality in the world.¹

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN NAMIBIA

Article 21 of the Constitution of the Republic of Namibia guarantees “freedom of speech and expression, which shall include freedom of the press and other media,” providing for legitimate restrictions under 21(2) including on grounds of “national security, public order, decency or morality, contempt of court, defamation or incitement to an offence.”² For years Namibia has enjoyed the highest rank in Africa on the global press freedom index, with an improvement in ranking from 26th in 2018 to 23rd in 2019 and 2020 out of 180 countries assessed.³



International Telecommunication Union (ITU) data reveals that, in 2014, 35.5 in every 100 inhabitants had a mobile broadband subscription⁴ and by 2018 the figure had risen to 59.3 in every 100.⁵ The 2018 Measuring the Information Society Report called Namibia “one of the frontrunners in Africa on ICT development”.⁶ With growing digitization, it is even more important for fundamental freedoms to be protected online as well as offline.

1. 'Namibia Overview', <https://www.worldbank.org/en/country/namibia/overview>

2. Constitution of the Republic of Namibia, https://www.constituteproject.org/constitution/Namibia_2010.pdf

3. RSF, <https://rsf.org/en/namibia>

4. Measuring the Information Society Report 2015, <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf>

5. Measuring the Information Society Report 2018, <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf>

6. Measuring the Information Society Report 2018, p.126, <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf>

ENJOYMENT OF FREEDOM OF EXPRESSION ONLINE

Human rights online, especially the right to privacy, freedom of expression, freedom of opinion and the right to access information, are some of the key issues in the Namibian digital rights and inclusion realm.

Social media is increasingly being used to express dissent, and in retaliation politicians have been calling for its regulation as a means of fighting misinformation and cybercrime.⁷ For the past few years, politicians and government officials have issued stern warnings and threats citing the “irresponsible use”⁸ of social media, claiming it endangers lives.⁹

A proposal to regulate social media is said to have divided members of Parliament in mid-2019.¹⁰ However, in February 2020, the Ministry of ICT confirmed plans to regulate it.¹¹ Although the government says that the regulations are only aimed at preventing the grooming of school girls such measures could be seen to amount to unnecessary restriction on online expression.

IMPACT OF COVID-19 REGULATIONS ON DIGITAL RIGHTS AND INCLUSION

In April 2020, as part of regulations to curb the spread of COVID-19, Namibia outlawed the publication of false or misleading statements related to the virus, including on social media.¹² Consequently a man was arrested under the regulations in June 2020.¹³

In April 2020, the Namibian government enforced e-learning countrywide as a response to the pandemic.¹⁴ This decision has been criticised as the country has a low technology roll out, with only 30% of schools having access to the internet.¹⁵



7. 'Vice president wants to censor social media', <https://www.namibiansun.com/news/vice-presidentwants-to-censor-social-media>

8. 'Government warns against irresponsible use of social media', <https://newerlive.na/posts/govt-warns-against-irresponsible-use-of-social-media>

9. 'Social media endangers lives', <https://www.namibiansun.com/news/social-media-endangerslives/>

10. 'MPs divided on social media gagging', <https://www.namibian.com.na/190767/archive-read/MPs-divided-on-social-media-gagging>,

11. 'Govt mulls social media protection', <https://www.namibian.com.na/197767/archive-read/Govt-mulls-social-media-protection>

12. 'Covid-19 'fake news' now a crime', <https://www.namibian.com.na/200224/archive-read/Covid19-fake-news-now-a-crime>

13. 'Man arrested for spreading fake Covid-19 news', <https://www.namibian.com.na/91561/read/Man-arrested-for-spreading-fake-Covid-19-news>

14. 'Govt ponders e-learning for schools', <https://www.namibian.com.na/199902/archive-read/Govt-ponders-e-learning-for-schools>

15. '70% of Govt schools without internet', <https://allafrica.com/stories/201910080121.html>

A July 2020 paper by the Association for Progressive Communications (APC) has highlighted that the move posed “serious discriminatory elements to those not connected to and unable to afford the internet, and interfered with the right to development and access to knowledge, a principle set out in the African Declaration on Internet Rights and Freedoms.”¹⁶

There were serious failures in data protection during COVID-19, with anecdotal reports of women reporting unsolicited contacts from unknown men who claimed to have obtained their numbers from the shop registers instituted as contact tracing measures. The media reported a case of a stolen attendance register,¹⁷ and also suggested that many people were using false names in these registers, possibly due to security concerns.¹⁸ Nine months after their introduction, the government has rescinded the requirement for customer registers in public places citing lack of authenticity of information provided.¹⁹

INTERNET ACCESS

Namibia's technology sector is hindered by a lack of affordable access, and poor-quality service.²⁰ The 2020 Inclusive Internet Index, which assesses internet availability, affordability, relevance of content and readiness, ranked Namibia 84th out of 100 countries, with a score of 41.2% for availability

and 54.8% for affordability indicators respectively. ITU data indicates that, as of June 2018, the percentage of individuals using the internet in Namibia is 36.8%²¹ in comparison to 14.8% in 2014.²²

A National Broadband Policy was launched in early 2020 with the aim of achieving reliable and affordable broadband access services for all.²³ The policy's five-year implementation action plan seeks to ensure 95% broadband coverage by 2024, as well as to operationalise the Universal Access and Service Fund.²⁴

PRIVACY, DIGITAL ID AND SURVEILLANCE

While the right to privacy is provided for under Article 13 of the Namibian Constitution,²⁵ the country does not yet have a data protection and privacy law. Nonetheless, there are indications of progress in this area, as the government is currently drafting a data protection policy.²⁶ In February 2020, a multi-stakeholder consultation took place²⁷ and further stakeholder consultations on a proposed Bill were conducted between September and October.²⁸ In the absence of a data protection law, data breaches have been reported even from government databases.²⁹ The country has been called “a safe haven for cybercrime”,³⁰ and without a cybercrime law,³¹ many citizens have fallen victim to grooming, revenge pornography and online fraud.³²

16. Compulsory e-learning in Namibia's public schools, https://africaninternetrights.org/sites/default/files/Nashilongo_Gervasius.pdf

17. 'Covid-19 customer register stolen', <https://www.namibian.com.na/206001/archive-read/Covid-19-customer-register-stolen>

18. First name 'Apple', last name 'Tomato', <https://www.namibian.com.na/96668/read/First-name-Apple-last-name-Tomato>

19. Govt to tighten COVID-19 rules <https://www.namibian.com.na/97414/read/Govt-to-tighten-Covid-19-rules>

20. 'Namibia's internet costs are too high', <https://www.namibiansun.com/news/namibias-internetcosts-are-too-high2019-03-05>

21. Measuring the Information Society Report 2018, <https://www.itu.int/en/ITU/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf>

22. Measuring the Information Society Report 2015, <https://www.itu.int/en/ITU/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf>

23. 'Namibia launches national broadband policy', <https://southern-timesafrica.com/site/news/mict-namibia-launches-national-broadband-policy>

24. 'Govt targets 95% broadband coverage by 2024', <https://newerlive.na/posts/govt-targets-95-broadband-coverage-by-2024>

25. Namibian Constitution, <https://www.lac.org.na/laws/annoSTAT/Namibian%20Constitution.pdf>

26. 'Data Protection Laws of the World',

<https://www.dlapiperdataprotection.com/index.html?t=law&c=NA#:~:text=The%20Namibian%20Government%20is%20currently,of%20their%20personal%20data%2C%20and>

27. 'GLACY+: Stakeholders' Consultation Workshop on the Data Protection Bill in Namibia', <https://www.coe.int/en/web/cybercrime/-/glacy-stakeholders-consultation-workshop-on-the-data-protection-bill-in-namibia>

28. Highlights for September pg14x- Council of Europe <https://rm.coe.int/cybercrime-coe-update-2020-q3/16809fd8fa>

29. 'SSC leak exposes personal info online', <https://www.namibian.com.na/178310/archive-read/SSC-leak-exposes-personal-info-online>

30. 'Namibia a safe haven for cybercriminals', <https://newerlive.na/posts/namibia-a-safe-haven-for-cybercriminals>

31. 'Cybercrime in Namibia', <https://www.namibian.com.na/165301/archive-read/Cybercrime-in-Namibia>

32. 'Many Namibians fall victim to online fraud', <https://www.nbc.na/news/many-namibians-fall-victim-online-fraud.20124>



A National Broadband Policy was launched in early 2020 with the aim of achieving reliable and affordable broadband access services for all.

In 2017, the Communications Regulatory Authority of Namibia (CRAN) enforced a provision within the 2009 Communications Act requiring mandatory SIM card registration through telecommunications operators.³³ The registration exercise was later abandoned as civil society and media raised concerns.³⁴ However, SIM card regulations may be reviewed as part of the ongoing review of the Communications Act.³⁵

Part 6 of the Communications Act provides wide-ranging powers for the interception of communications, and Article 70 (1) legislates for the establishment of an interception centre for the purposes of national security and combating crime.³⁶

Overall, there is a high perception of state-sponsored surveillance among civil society and the media, particularly by the Central Intelligence Service, as reported by a Namibian newspaper in a detailed three-part report.³⁷

33. 'Spy agency wants SIM cards registered', <https://www.namibian.com.na/163120/archive-read/Spy-agency-wants-SIM-cards-registered>

34. 'Ripe for surveillance abuse – Unpacking Namibia's SIM card registration limbo', <https://action-namibia.org/ripe-for-surveillance-abuse-unpacking-namibias-sim-card-registration-limbo/>

35. 'Namibia undertakes review of communications law', <https://www.commsupdate.com/articles/2019/10/11/namibia-undertakes-review-of-communications-law/>

36. Communications Act, 2009, https://www.nbc.na/sites/default/files/pdf/Namibia%20Communications%20Act%208%20of%202009_0.pdf

37. Action Access to Internet, 'The rise of the Namibian surveillance state (Part I)', <https://action-namibia.org/rise-namibian-surveillance-state/>; 'The Rise of the Namibian Surveillance State: Part 2', [https://www.namibian.com.na/174788/archive-read/The-Rise-of-the-Namibian-Surveillance-State-Part-2](https://www.namibian.com.na/174788/archive-read/The-Rise-of-the-Namibian-Surveillance-State-Part-2;); 'The rise of the Namibian surveillance state: Part 3', <https://www.namibian.com.na/175475/archive-read/The-rise-of-the-Namibian-surveillance-state>

HATE SPEECH, MISINFORMATION AND CRIMINAL DEFACTION LAWS

While freedom of speech is constitutionally guaranteed, constitutional protections for national security, public order, and public morality provide legal grounds for restricting media freedom.³⁸ Defamation is a criminal offense under common law, and there have been a number of successful court cases for defamation.³⁹

Racial discrimination is currently regulated under the Racial Discrimination Prohibition Act of 1991.⁴⁰ However, hate speech in Namibia is not outlawed, and in 2008 the UN criticised the country for not outlawing hate speech, especially towards minority groups.⁴¹

Misinformation related to COVID-19 has recently been outlawed and is punishable with a fine of up to 2,000 Namibian Dollars (USD 134) or imprisonment of up to six months.⁴²

THE EXTENT OF DIGITAL EXCLUSION AND ITS IMPACT ON HUMAN RIGHTS

The Internet is largely expensive and inaccessible in Namibia leaving many digitally excluded.⁴³ Research conducted by the Alliance for Affordable Internet (A4AI) in 2019 has revealed that 1GB of data in

Namibia cost 8.57 USD.⁴⁴ Telecom Namibia charges N\$139.00 for prepaid 1GB, equivalent to USD9.32.⁴⁵

There has been some positive strides towards greater digital inclusion. In its 2017/22 strategic plan, the Ministry of ICT (MICT) aimed to ensure network coverage of mobile phones and internet “to all corners of the country” (p. 23).⁴⁶ MICT also established 25 multi-purpose community centres in remote parts of Namibia, complete with internet infrastructure (p. 2).⁴⁷

In 2016, MICT made a commitment to provide the entire nation with cellular phone coverage by mid-2020, in order to make information more accessible, affordable and relevant, through a program implemented by parastatal Mobile Telecommunications Limited (MTC).⁴⁸ As part of this initiative, MTC intends to erect 500 new towers throughout the country.⁴⁹

Digital exclusion is particularly felt by the education sector, where 70% of government schools are not connected to the internet.⁵⁰ The Deputy Minister of Education, Arts and Culture confirmed that, out of 1,897 government schools across the country, only 590 schools are connected to the internet.⁵¹

***Defamation is a criminal
offense under common law***

38. Constitution of the Republic of Namibia, https://www.constituteproject.org/constitution/Namibia_2010.pdf

39. For example, 'Hamata to pay for defamation', <https://www.namibian.com.na/119662/archive-read/Hamata-to-pay-for-defamation>; <https://namiblii.org/na/judgment/high-court-main-division/2017/103>

40. <https://laws.parliament.na/annotated-laws-regulations/law-regulation.php?id=375>

41. 'UN report lambasts Nam for hate speech', <https://www.namibian.com.na/41758/archive-read/UN-report-lambastes-Nam-for-hate-speech>

42. 'Covid-19 fake news now a crime', <https://www.namibian.com.na/200224/archive-read/Covid19-fake-news-now-a-crime>

43. 'Namibia's Internet Costs are too High', <https://www.namibiansun.com/news/namibias-internet-costs-are-too-high2019-03-05>

44. The Alliance for Affordable Internet, https://a4ai.org/extra/mobile_broadband_pricing_usd-2019Q2

45. <https://internetpkg.com/namibia-internet-packages/>

46. Ministry of Information and Communication Technology (MICT) 2017/22 Strategic Plan, p.23, <http://www.mict.gov.na/documents/32978/266786/MICT+STRATEGIC+PLAN+2017-2022/3596bd32-0aa5-498a-b4c9-b396af9e8c1a>

47. Ministry of Information and Communication Technology (MICT) 2017/22 Strategic Plan, p.2, <http://www.mict.gov.na/documents/32978/266786/MICT+STRATEGIC+PLAN+2017-2022/3596bd32-0aa5-498a-b4c9-b396af9e8c1a>

48. 'MTC aims to connect 20 000 in rural areas', <https://neweraalive.na/posts/mtc-aims-connect-20-000-rural-areas>

49. 'MTC to erect 500 new towers', <https://www.namibian.com.na/174168/archive-read/MTC-to-erect-500-new-towers>

50. 'Namibia: 70 Percent of Govt Schools Without Internet', <https://allafrica.com/stories/201910080121.html>

51. '32% of public schools not equipped for online learning', <https://www.telecom.na/media-centre/212-internet-exchange-point-launched-in-windhoek>



DIGITAL INFRASTRUCTURE

With support from the African Union and the African Bureau for the Internet Society, Namibia launched an Internet Exchange Point (IXP) in 2014.⁵² The functionality and performance of the point is undetermined as not much has been written about it. However, according to Pauina Magongo, a member of the committee in charge of the IXP, the local IXP has been facing challenges dating from 2017 and for sometime now, the equipment has neared obsolete.⁵³

Other ICT infrastructures in Namibia also include the Western African Cable System (WACS) which arrived in the country in early 2011.⁵⁴ The submarine presence in the country ought to have brought cheap bandwidth and translated into many possibilities in the ICT sector of the Namibian economy, but the cables have reportedly been damaged a number of times since arrival.⁵⁵

The 2020 Inclusive Internet Index ranks Namibia overall at 84 out of 100 researched

countries and places the country at 21.2% on the infrastructure category, highlighting that while the country is 100% covered by the 2G network, 3G network only covers 53% of the country while the 4G network coverage is even further lower at 39% with no 5G deployment reported. The report has rated Namibia 0 (zero) on indicators regarding both government and private sectors initiatives to make Wi-Fi-available.⁵⁶

Section 57 of the Communications Act 2009 (Act No. 8 of 2009) provides for the establishment of a Universal Service Fund, implemented under CRAN and funded by a levy of licensed operators' turnover.⁵⁷ However, the fund has never become operational as the Supreme Court ruled in 2018 that collection of the levy was unconstitutional.⁵⁸

GENDER AND ICT

The 2020 Inclusive Internet Index reported that Namibia's gender gap in internet access stands at 14.1%, with 64% of males and 55% of females being internet users.⁵⁹ In 2012, only 25.8% of women had an internet-enabled mobile phone compared to 36.9% of men.⁶⁰

A community of women in technology exists in Namibia, although the area continues to be male dominated. However, female developers are reported to be part of the Google and Facebook developers' circle.⁶¹ Recently a group of women hackers won an innovation challenge held by UNDP.⁶²

52. 'Internet Exchange Point Launched in Windhoek', <https://www.telecom.na/media-centre/212-internet-exchange-point-launched-in-windhoek>

53. Telephonic Interview, November 18, 2020, Paulina Magongo

54. 'WACS Submarine Cable Lands in Swakopmund Today', <https://www.telecom.na/media-centre/260-wacs-submarine-cable-lands-in-swakopmund-today>

55. 'WACS undersea cable damaged again', <https://www.we.com.na/news/wacs-undersea-cable-damaged-again2020-03-30>

56. The Inclusive Internet Index 2020, <https://theinclusiveinternet.eiu.com/explore/countries/NA/>

57. Government Gazette 8 June 2015, <https://www.lac.org.na/laws/2019/6886.pdf>

58. 'Supreme Court rules against Cran levy', <https://www.namibian.com.na/68353/read/Supreme-Court-rules-against-Cran-levy>

59. The Inclusive Internet Index 2020, <https://theinclusiveinternet.eiu.com/explore/countries/NA/performance/indicators/>

60. 'Lifting the Veil on Gender ICT Indicators in Africa', p.29, https://www.researchinAfrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_13_-_Lifting_the_veil_on_gender_ICT_indicators_in_Africa.pdf

61. Namibia Women inTech; <https://namtechwomen.com/about-us>

62. 'Female 'hackers' take the lead', <https://www.we.com.na/news/female-hackers-take-the-lead2020-08-18/>


The 2020 Women's Rights Online Report Card on Namibia⁶³ gave the country a score of 29% based on its assessment in the categories of internet access and women's empowerment; relevance of content and services; online safety; affordability; and digital skills and education. The report indicates that only 47% of Namibian women have access to the internet and that there is no national policy recognising technology as a tool for fighting gender inequalities.

Online violence against women also remains a challenge.⁶⁴ The 2020 Women's Rights Online Report Card also reveals that the lack of

cybercrime and data protection legislation in Namibia puts women at risk of violence and in vulnerable positions, in the cases of non-consensual image sharing (also known as revenge pornography), as well as with regard to online blackmail and sexualised hate speech.⁶⁵

Women in political and prominent positions are frequently targets of online harassment and bullying. The Internet Society Namibia Chapter in 2019 organised a Digital Forum for Women in Political and Prominent space aiming at engaging and empowering women with skills to mitigate online violence.⁶⁶

CONCLUSION AND RECOMMENDATIONS



Namibia is actively pursuing greater digital inclusion, and is also making progress towards protections in relation to data protection and cybercrime. However, to date the balance has been skewed too much towards state control and intervention, and too little towards the genuine protection of its citizens and connectivity. Issues around gender and technology need urgent interventions, as women face online harms and at the same time are more likely to be digitally excluded.

In concluding further, the following recommendations ought to be considered;

Infrastructures: Greater effort needs to be realised in creating awareness of the benefits and usage of the IXP locally and how that translates into economic and internet security issues. There is a need to translate the country's benefits of the WACS and how that translates into the greater connectivity of the country.

Namibia must operationalise the Universal Service Fund as set out in the Communications Act in order to effect equitable access to the internet.

Digital Inclusion: Namibia should adopt the UN Broadband Commission pricing for data of 1GB of mobile data priced at no more than 2% of monthly GNI per capita. Both government and private sectors should make Wi-Fi available in public places and in addition Government should ensure the connection of all schools to the Internet.

63. 'Women's rights online report', <http://webfoundation.org/docs/2020/08/GenderReport-Namibia.pdf>

64. 'Addressing 'Revenge Porn' in Namibia', <https://ohrh.law.ox.ac.uk/addressing-revenge-porn-in-namibia/>

65. Women's rights online report' <http://internet-society.na/wp-content/uploads/2020/07/GenderReport-Namibia-FINAL-ONLINE-VERSION.pdf>

66. 'Call for anti-online bullying law', <https://www.namibian.com.na/84148/read/Call-for-anti-online-bullying-law>

The implementation plan of the Broadband Commission needs to be closely evaluated to ensure success of broadband access throughout the country.



Privacy and Protection Online: With the Data Protection Bill said to be drafted and the Cybercrime Bill headed for finalisation, the country should ensure protection and privacy that protects the citizens especially women and other vulnerable communities.

Social Media: There is evidence that social media has facilitated greater involvement in public discourse and also allowed for increased access and sharing of information. Overall social media has also increased internet usage and uptake in the country. Given these developments and others, talks to regulate social media should considerably be halted.

Namibia is actively pursuing greater digital inclusion, and is also making progress towards protections in relation to data protection and cybercrime.



Nigeria is cited as the largest economy in Africa,¹ with an average GDP of N39,089,460.61 million (\$100,611.0703)² in nominal terms.³ With a population of 208 million,⁴ Nigeria has several natural resources including crude oil, natural gas, coal, iron and tin.

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN NIGERIA

Over the years, the country's economy has been heavily dependent on revenue from crude oil, however, with the declining global oil prices in recent times and its ripple effect, compounded by rising poverty and insurgency, the country has focused on diversifying the economy with the spotlight on its non-oil sector, especially agriculture, financial services and telecommunications/ICT. The downturn in crude oil prices and oil production shortages significantly contributed to the country's recession in 2016,⁵ the first since 1991.

The impact of COVID-19 on the Nigerian economy has been vast and though most industries recorded immense losses, the ICT/ Telecommunications industry is one of the few that have not only survived the effects of the pandemic, but saw rapid growth due to increase in demand.⁶ Statistics from the Nigerian Communications Commissions (NCC) show that the telecoms industry contributed 14.3% to the Nigerian GDP as at Q2 2020, up from 10.6% in Q4 2019.



14.3%
was contributed by
the telecoms industry
to the Nigerian GDP
as at Q2 2020

1. <https://www.bloomberg.com/news/articles/2020-03-03/nigeria-now-tops-south-africa-as-the-continent-s-biggest-economy>.

2. Official exchange rate as at the 18th of December 2020 - 1 USD = 388.520

3. National Bureau of Statistics. "Nigerian Gross Domestic Report (Q3 2020)".

4. <https://www.worldometers.info/world-population/nigeria-population/>

5. According to the Nigerian National Bureau of Statistics GDP Q4 2016 Report, there was a steady decline in the economy from Q1 2015 to Q4 2016.

6. According to statistics from the Nigerian Communication Commission, active internet subscriptions increased from 128,723,188 in January 2020 to 136,114,413 in March 2020 to 147,148,307 by July 2020 when some states in the country began easing restriction measures, shorturl.at/elCGP [Accessed 7 January 2020]

This growth is understandably so, as the industry has seen a spike in demand for internet and telecommunication services. This points to the reliance of these telecommunication tools to mitigate, to an extent, the consequences of COVID-19, especially as it is related to the business environment and social interactions. Apart from their importance to businesses and general social interactions during this period, digital technologies have generally been instrumental in the transfer of information, entertainment, financial services, advocacy, and other activities in Nigeria.

The reliance on these digital tools has demonstrated their importance to Nigeria. With an increasing list of possible interactions in the digital space, the importance of proper legislative governance cannot be over emphasized. The presence of Nigerians in the digital world means the exposure to new kinds of threats to their rights, the likes that would render pre-established laws insufficient. In order to protect the interests of Nigerians online, the legislative houses and relevant government agencies have been making measured efforts towards creating the appropriate legal atmosphere.

Along with the conversations on the protection of Nigerians rights online arises the importance of inclusion. With all the recognizable benefits of the digital economy, barriers to access means exclusion from these benefits. For a developing country like Nigeria, with nearly 40% of the population living below the poverty line, the discussion around digital inclusion should be an important topic. All these and more make the conversations around digital rights and inclusion important to the democracy and the economic strength of Nigeria.



DIGITAL ECONOMY POLICY AND STRATEGY

In October 2019, the Nigerian government renamed its Communications Ministry as the Ministry of Communications and Digital Economy in a move that suggested that the country has realised the importance of the digital economy to the overall well being of its economy. In June 2020, the country released a national digital economy policy and strategy to “transform Nigeria into a leading digital economy providing quality life and digital economies for all”. However, in what seems like conflicting actions, Nigeria has taken measures, within the same time, to restrict the digital space. The country has been pushing for regulation on social media. As at the time of writing this report, there are two proposed regulations aimed at curbing “hate speech”⁷ and fighting “fake news”⁸ in Nigeria. These two bills, as observed by the Committee to Protect Journalists, serve to restrict civil liberties in Nigeria. The Protection from Internet Falsehood and Manipulation Bill, for example, gives the government, through the Nigeria Police Force, the power to restrict access to internet services and determine the falsity or otherwise of information shared by Nigerian citizens on digital platforms.

7. The Hate Speech (Prohibition) Bill 2019 has passed the first reading <https://www.nassnig.org/documents/bill/10613>.

8. The Protection from internet falsehoods and manipulation and other related matters Bill 2019 has passed the second reading, <https://placbillstrack.org/view.php?getid=6649>

Digital inclusion has become a digital rights issue. This position became amplified with the COVID-19 pandemic realities and the limitations imposed by the pandemic. The ability to learn, engage, work and do business relied on internet connectivity and ability to use digital devices and platforms. Those who could not afford internet access or who could not use digital devices may have had their life come to a halt. At the beginning of the implementation of lockdown measures, leaders of Nigeria's federating units, the Nigerian Governors Forum, began to implement an earlier agreement with communications stakeholders to reduce the cost of right of way (RoW).⁹ The cost of RoW has long been identified as one of the impediments to ensuring reliable broadband internet connectivity in the most remote areas of Nigeria.¹⁰

According to the Nigerian Communications Commission (NCC), Nigeria needs about 120,000 km of fiber cables to achieve its goal of ubiquitous broadband access but only about 38,000 km of cables have been laid.¹¹ Internet connectivity became a key infrastructural need to ensure students continue learning as schools were closed as part of the lockdown measures, with impacts on the right of students to education.



**Digital inclusion has
become a digital
rights issue.**

The importance of digital inclusion cannot be over emphasized. The United Nations' Sustainable Development Goals (SDGs) 2020-2030¹² includes digital inclusion¹³ as part of the plan towards global prosperity, especially fostering inclusion in least developed countries. A report published by the Nigerian Bureau of Statistics in May 2020 highlights that 40% of the total population, or almost 83 million people, live below the country's poverty line of 137,430 naira (\$381.75) per year.¹⁴

Therefore, inclusion is important in order to achieve the economic potential of Nigeria. Digitally excluded Nigerians could lack the skills, confidence and motivation, along with having limited or no access to equipment and connectivity. This creates additional layers of social exclusion and exacerbates social and economic problems.

IMPACT OF COVID-19 REGULATIONS ON DIGITAL RIGHTS

To contain the spread of and cushion the effect of the COVID-19 virus, the federal government of Nigeria implemented a number of health, social, and economic measures including travel bans, movement restrictions and deployment of food supplies and financial assistance, among others. In essence, the declaration of measures aimed at curbing the spread of the coronavirus seem to have provided the ground to breach digital rights including rights to privacy and freedom from unlawful surveillance. Increased levels of surveillance, circumvention of freedom of speech

9. <https://nairametrics.com/2020/01/25/state-governors-finally-agree-to-reduce-row-charges-for-telcos/>

10. <https://www.nigeriacommunicationsweek.com.ng/right-of-way-issues-frustrate-broadband-penetration/>

11. <https://www.thecable.ng/ncc-need-120000km-optic-fiber-network-38000km-covered>

12. The 2030 Agenda for Sustainable Development seeks to build on the Millennium Development Goals, a United Nations agenda geared to meet the needs of the world's poorest by the year 2015. The 2020 agenda sets out to achieve sustainable development in its three dimensions – economic, social and environmental – in a balanced and integrated manner by the year 2030.

13. Target 9.c: Access to ICT - Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020.

14. <http://nigerianstat.gov.ng/download/1092>



The importance of digital inclusion cannot be over emphasized. The United Nations' Sustainable Development Goals (SDGs) 2020-2030 includes digital inclusion as part of the plan towards global prosperity, especially fostering inclusion in least developed countries.

and mismanagement of private information/data are some of the violations Nigerians have had to deal with during this period. For example, the Nigerian Minister of Communications and Digital Economy is reported to have cited data mining, based on SIM registration data, as a way to identify the financial status of Nigerians in order to provide adequate aid.¹⁵ In another instance of the undisguised violation of privacy, the Minister of Humanitarian Affairs and Disaster Management, Sadiya Farouq, at a press briefing at the State House, disclosed plans to provide financial aid to Nigerians using information directly sourced from Biometric Verification Number (BVN) linked to bank accounts and confidential data provided to mobile networks.

PRIVACY, DIGITAL IDs AND SURVEILLANCE

Section 37 of Nigeria's 1999 Constitution guarantees the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications.¹⁶ The right to privacy in Nigeria is underpinned by the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Although the provision in the constitution does not specifically mention "data", it is arguable that information on homes, correspondences and telephone conversations are captured in the definition of personal data.¹⁷

15. <https://www.icirnigeria.org/covid-19-controversy-trails-ministers-decision-to-mine-data-of-phone-users-without-consent/>

16. Lfn

17. Olumide Babalola, Data Protection And Privacy Challenges In Nigeria (Legal Issues). March 9, 2020, available at <https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues>

Nigeria's National Identity Management Commission (NIMC) declared plans to develop a digital ecosystem to create an enabling environment for the effective and efficient mass enrolment of Nigerians and legal residents in Nigeria. The system would be a centralized and secure national identity database where digital identities are issued to everyone in the form of the National Identification Number (NIN).¹⁸ This process has continued despite the lack of sufficient legal protection for personal data. Although a Nigerian Data Protection Regulation (NDPR) was issued by the National Information Technology Development Agency in 2019, it does not reflect a comprehensive data protection

framework as it does not establish an independent data protection commission.

Even though the International Principles on the Application of Human Rights to Communications Surveillance¹⁹ stipulates when limits apply to the right to privacy, the body of legislation in Nigeria²⁰ contains a number of provisions on the state's legal right to surveillance, and the Nigerian government has a history of extrajudicial surveillance on its citizens.

Therefore, inclusion is important in order to achieve the economic potential of Nigeria.



An investigative report by Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy at the University of Toronto in Canada reported that Nigeria had acquired Signaling System 7 (SS7), a protocol suite developed for exchanging information and routing phone calls between different wireline telecommunications companies.²¹

Unfortunately, this is not a once-off occurrence²² in Nigeria. Government-led extra judicial surveillance is a contravention of the state's duty to preserve the intrinsic right to privacy, and the protection from arbitrary interference with its citizens' privacy.

¹⁸ NIMC website, <https://www3.nimc.gov.ng/digital-identity-ecosystem/>

¹⁹ Section 45 of the 1999 Constitution, the Terrorism (Prevention) Act (Ammended 2013) and the CyberCrime (Prevention) Act, 2015

²⁰ Full investigative report available at

<https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/>

²¹ DSS Bugs 70% Of Mobile Phones In Abuja, <https://www.independent.ng/dss-bugs-70-mobile-phones-abuja/>

²² DSS Bugs 70% Of Mobile Phones In Abuja

FREEDOM OF EXPRESSION

ONLINE IN 2020

The right to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference is constitutionally backed by Section 39 of the 1999 Nigerian Constitution.²³ The provision goes further to establish that every person is entitled to own, establish and operate any medium for the dissemination of information, ideas and opinions.²⁴ In consideration of this, government-backed violations of the right to expression online is a dissension from its mandate to protect this right. A notable example of this violation is the imposition of sanctions by the National Broadcasting Commission on three Nigerian television stations, Channels TV, Arise TV and Africa Independent Television for transmitting footage obtained from “unverified and unauthenticated social media sources”.²⁵

There have also been multiple reports of arrests arising from the use of social media platforms. Babatunde Olusola, a university student, was arrested for allegedly operating a parody account in the name of Nigeria’s former President, Goodluck Jonathan, on Twitter.²⁶ Twitter rules state that users are allowed to create parody, newsfeed, commentary, and fan accounts on the social media platform, provided that the accounts follow certain requirements, including stating that the account is unaffiliated with the target of the parody.²⁷ Babatunde Olusola followed this rule by having ‘Not GEJ’²⁸ on the bio of the twitter parody account, as a declaration of its non affiliation with the former president but he was still arrested. There were also multiple arrests²⁹ of Nigerian citizens for protesting against police brutality as part of youth-led protests held in October 2020, tagged [#EndSARS protests](#).

Backed by the right to expression online, Nigerians are using social media and online platforms to speak on pertinent issues in the country. The earlier referenced [#EndSARS movement](#)



23. 1999 constitution

24. Section 39(2) of the Constitution. The exemption to this right is the right to own, establish or operate a television or wireless broadcasting station for any purpose whatsoever.

25. <https://www.premiumtimesng.com/news/more-news/423162-endsars-nbc-imposes-n3m-sanction-each-on-ait-channels-arise-tv.html>

26. Story available at punch newspaper online

<https://punchng.com/student-arrested-for-opening-jonathan-parody-account-denied-access-to-lawyers/> accessed

27. Twitter rules on Parody accounts, <https://help.twitter.com/en/rules-and-policies/parody-account-policy>

28. The initials of Former President Goodluck Ebele Jonathan

29. There were multiple reports of indiscriminate arrests of Nigerian citizens protesting against the Special Anti-Robbery Squad. Report available at <https://cutt.ly/SjkXezw> [Last accessed 8 January 2021]

which recommenced in 2020 after an unconfirmed video of a SARS police officer shooting a young Nigerian went viral, received widespread support, financial and otherwise from Nigerians, Nigerians in diaspora and the international community. Digitally supported movements such as this are not unfamiliar in Nigeria. In 2012, along with physical protests, Nigerians took to social media to magnify their rejection of the removal of fuel subsidy by using the hashtag #OccupyNigeria.³⁰

The #BringBackOurGirls³¹ hashtag brought attention to the campaign for the return of 276 schoolgirls abducted from Chibok, a village in Borno State, Nigeria, by a group of militants known as Boko Haram on the 14th of April, 2014. The online campaign hashtag #NotTooYoungToRun was used by Nigerians to advocate for greater youth inclusion in legislative houses in Nigeria, a campaign that culminated in the passing of the Age Reduction Act, popularly known as the Not Too Young to Run Act.

The use of social media as a tool for activism to highlight these and other issues in Nigeria can not be understated.

In an attempt to regulate the online environment in Nigeria, the legislative houses are attempting to pass the Protection from Internet Falsehood, Manipulations and other Offences Bill,³² nicknamed the Social Media Bill.³³ The provisions of the bill seek to criminalise the transmission of ‘false statements’ as defined in the bill with the intention of curbing the spread of misinformation and fake news. Critics of the bill have pointed out that the provisions contained are an attempt to suppress free speech online and silence dissenting voices by the government.³⁴

Conversely, the 2019 Digital Rights and Freedom Bill has, as part of its objectives, the protection of freedom of expression, assembly and association online. The bill was passed by both houses of the National Assembly in 2019, however, the President declined signing the bill on the grounds that it “covers too many technical subjects and fails to address any of them extensively.”³⁵ The bill has since been revised, but would have to go through the legislative processes all over again before it can get a chance to be signed into law. Signing this bill into law would be a positive step forward in protecting free expression online, giving citizens a more comprehensive legal framework for seeking redress in the event of violations.

Conversely, the 2019 Digital Rights and Freedom Bill has, as part of its objectives, the protection of freedom of expression, assembly and association online.

30. Occupy Nigeria Protest, available at <https://cutt.ly/2jzrl76> [Last accessed 9th January 2021]

31. Chibok Schoolgirls Kidnapping, available at <https://cutt.ly/pjzelSO> [Last Accessed 9th January 2021]

32. Protection from Internet Falsehood, Manipulations and Other Offences Bill

33. The bill has passed second reading in the Senate but the report of a March 2020 Public Hearing has not been released.

34. There is currently a petition to kill the bill

<https://www.change.org/p/the-national-assembly-of-the-federal-republic-of-nigeria-stop-the-social-media-bill-you-can-no-longer-take-our-rights-from-us>

35. President Buhari in his letters to the Senate on his decision to decline the Digital Rights and Freedom bill mentioned that the bill covers too many technical subjects and “fails to address any of them extensively. News available at <https://cutt.ly/NjkThwv> [Last accessed 8 January 2021]

THE EXTENT OF DIGITAL EXCLUSION AND ITS IMPACT ON HUMAN RIGHTS

The concept of social inclusion entails equal access to tools and resources by members of the society. On the other hand, social exclusion conceptualises the exclusion of members from access to these tools. In the 21st century, digital tools have become an integral part of human lives, from economic globalization to revolutionising social interactions.

As earlier stated, the telecommunications industry alone contributed up to 14.3% to Nigeria's GDP in the first half of 2020. Certainly, with all of the benefits of the digital revolution, exclusion from access opposes the important theory of social inclusion. All of the positive contributions of the internet manifest themselves after the technology is accessible and the population has learned how to use the technology at least on a very basic level.³⁶ Highlighting the importance of digital inclusion, Sustainable Development Goal 9 establishes 'increasing digital inclusivity in developing countries³⁷ as a target'. Nigeria is considered as a developing country, with up to 40% of the entire population living below the poverty level.³⁸

Apart from access to economic benefits as provided by access and usage of digital tools, digital exclusion disconnects certain groups of people from enjoying some basic human rights such as the right to participate in government and free elections, right to education, the right to adequate living standards, and the right to social security in today's context. For instance, the proposed digital ecosystem in Nigeria would mean the digitally illiterate/marginalised might not have the tools to vote, open bank accounts or receive certain information. Several factors are responsible for digital exclusion, including disability, literacy levels, poverty, culture and language. Digitally excluded people can lack skills, confidence and motivation, along with having limited or no access to equipment and



connectivity. This can create additional layers of social exclusion and exacerbate social and economic problems.³⁹

Internet penetration in Nigeria stood at 42% in January 2020.

36. The Digital Divide and Human Rights - What the EU should do at the World Summit on Information Society, (2005) Anne Peacock, a doctoral researcher in the Law Department of University of Essex, available at <https://cutt.ly/9hTDNfi>

37. Sustainable development Goal 9c - Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020, <https://sdgs.un.org/goals/goal9>

38. Statistics from the National Bureau of Statistics, available at 2019 POVERTY AND INEQUALITY IN NIGERIA.cdr - National ...nigerianstat.gov.ng > download [Accessed 9 December 2020]

39. Missing footnotes

The National Digital Economy Policy Strategy 2020-2030⁴⁰ targets 70% broadband⁴¹ penetration in 4 years.⁴² Some of the strategies for achieving this goal would include developing effective regulation of the ICT and digital sector in a way that enables development, improving digital literacy, deployment of fixed and mobile

infrastructure to deepen the broadband penetration in the country and supporting government digital services. The success of this strategy will attract benefits such as greater digital inclusion.

CONCLUSION AND RECOMMENDATIONS



In the 21st century, digital tools have become an integral part of human lives, from commercial globalization to revolutionising social interactions. As earlier stated, the telecom/ICT industry alone contributed up to 14% to the Nigerian GDP. The industry attaining this level of influence with a penetration of only 42% is a strong indicator of its economic benefit to the Nigerian economy. As earlier posited, with all of the benefits of the digital revolution, exclusion from access opposes the important theory of social inclusion. Also, it has been acknowledged that ICTs offer a range of fundamental and methodological contributions that empower sustainable development and implementation of the Sustainable Development Goals.⁴³ With the established link between the economy, social inclusion and ICT/ digital tools, efforts towards digital inclusion, protection of rights online and investment in the ICT/ telecom industry by the Nigerian government and stakeholders in the industry is of paramount importance.

Promoting the utilization of ICT/ telecommunication tools will not be complete without re-emphasizing the State's responsibility to preserve the rights of its citizens on these platforms. The point of enacting laws and subsidiary legislation that adequately protect the digitally connected and foster digital inclusion cannot be overemphasized. There is also a general sense of distrust in law enforcement agencies and in the judicial system in Nigeria by the public, especially the underprivileged. Along with this distrust is the level of illiteracy which inadvertently affects the understanding of rights, impeding the ability to assert these rights.⁴⁴ In fostering or increasing trust in judicial processes, Nigeria would benefit from awareness campaigns on human rights, offline and online, directed especially at those who may have been deliberately misinformed about their rights, or those who are uninformed about the same, and ensuring access to justice when violations occur.

40. About digital inclusion and exclusion, Citizens Online Webpage, <https://www.citizenonline.org.uk/digital-inclusion/> [Accessed 9 December 2020]

41. The National Digital Economy Policy Strategy 2020-2030, developed by the Nigerian Communications Commission,

42. 2020 – 2024 Nigeria's National Digital Economy Policy and Strategy

43. How ICT Can Accelerate the Implementation of the Sustainable Development Goals by Darine Ameyed, November 8, 2018. Available at <https://cutt.ly/ojczSZW> . [Last Accessed 10 January 2021]

44. There is a link between literacy and the assertion of human rights in Nigeria as posited by Apeh, Elaigwu Isaac (Ph.D) in his paper 'Literacy Promotion for Human Rights Awareness and Protection - The case for Nigeria', available at <https://cutt.ly/fjcs8AS> [Last accessed 9th January 2020]



Case Study: The looming threat to data privacy for Nigerians in a pandemic

Compiled by Khadijah El-USman

Nigeria recorded its first COVID-19 case in February 2020 and like many other countries, had to scramble to put resources together to tackle the ensuing effects. And with unprecedented times came unprecedented measures. Governments had to rapidly identify and ensure care for cases, trace and quarantine their contacts and monitor disease trends. Countries like Belgium, Malaysia and Singapore developed web applications and used mobile devices to keep track of their citizens.

Nigeria, on the other hand, has a controversial history with health surveillance with little to no regard for the rights to personal privacy. This was evident from the Governors' Forum trying to use mobile companies like MTN to trace movements, to applications like Stay-SafeNG being developed for contact tracing for COVID-19.

For the average Nigerian affected by COVID-19, their experiences with contact tracing and health surveillance were small scale but helped to give a bigger picture of the problem at hand. For Dr Ade (name changed), after he and a few of his colleagues had come down with COVID-19 like symptoms and eventually tested positive, the hospital undertook contact tracing for him and his colleagues. He described the procedure as “making venn diagrams of clusters of patients we had all seen” and eventually found that all the doctors in question had seen the same patient.

The hospital had its own COVID-19 unit reporting back to the Nigeria Centre for Disease Control (NCDC) who did the contact tracing. Ade noted, “My hospital has the privilege of having all patient information digitized so it was very easy to get contact information of the patients involved,” meaning different organizations and the COVID-19 unit had access to patient information without their consent. He alluded further that from his knowledge of epidemiology, “when dealing with a highly infectious disease, you can access patient information pertinent to that issue, meaning address and phone number.”



With that in mind, is it questionable why in Lagos State, the Nigerian Institute of Medical Research developed a seven-page Google form to be filled by all those who required testing for COVID-19 at the peak of the pandemic. The form required various details, including office address and next of kin. Eventually, if the person tested was positive then the contacts were traced. There were COVID-19 centers in each local government area with health workers equipped with mobile devices ready to assist those who did not have access to digital tools, although most of these workers were not trained on the principle of confidentiality.

The data of people who tested negative or were never infected, including that of their next of kin, were uploaded into a third party database, leaving the question of who stores this data, and how long it will be kept in light of the lack of data protection laws, unanswered.

On the other hand, Dayo, another respondent in Abuja, had a different experience when the NCDC came to test him and his colleagues. There had been an outbreak in his office and everyone had to get tested. Dayo noted that the process was not very digitized; “it was a very manual process.” The NCDC representatives came with numerous forms that posed various questions and to Dayo, “many of the questions did not seem necessary but they came with a counselor to seek your consent. Even though it felt like an invasion of privacy, I could see the point”. To Dayo, it did not seem like any of the information being taken was going to be inputted into a system or database. Dayo shared that if this information were to indeed be inputted into a system, he would be worried about his privacy and the stigma that could come with certain information. Dayo went further to report that this fear had many of his colleagues inputting fake information on the NCDC forms. Should there be any abuse of privilege in the near future, Nigeria's lack of comprehensive data protection laws leaves Dayo and others like him vulnerable.

Public health data is usually personally identifiable and sensitive, often revealing details about a person's lifestyle, behaviors, and health. With not only the government involved, but also third-party actors including application creators and pandemic volunteers being privy to the data of Nigerians, there needs to be a call for accountability. There is a need to address the right to personal privacy, especially related to public health issues, and utilising a human rights approach in creating policies that have the capacity to not infringe on people's rights.



Case Study: Covid-19 Digital Contact

Tracing: Lessons From A Nigerian Experience

Compiled by Adeboye Adegoke, with support from Temitope Opeleyeru

Much of our lives now revolve around the use of technology, which makes our work easier and faster, but technology is never a substitute for the quality of work required in its application.

In the wake of the COVID-19 pandemic, the world looked towards technology for succor as different stakeholders were working to stem the tide of the pandemic, to protect lives and revive the global economy. While the virus was spreading rapidly in 2020 with no effective antiviral therapy or vaccine, the world focused on managing the pandemic by containment. It is therefore understandable that technology was considered useful to facilitate pandemic containment strategy. Google and Apple, two of the world's leading technology companies, announced a partnership, on COVID-19 contact tracing technology and were quick to assure privacy protection in their proposed rollout, affirming that user privacy and security are central to the design. There is documented evidence of privacy protection in the adoption of contact tracing applications in managing COVID-19 by European governments. Those efforts may have contributed to the eventual flattening of their incidence curves, despite challenges with low adoption, and privacy and security concerns.

In Nigeria, like many African countries, the government announced lockdowns, proposed the use of mobile data for COVID-19 surveillance, introduced new legislation and more. Notably, there was news of the development of digital contact tracing applications by both State and non state actors. These are measures with clear implications for digital rights, particularly the right to privacy. In order to understand the extent to which contact tracing measures were deployed by the Nigerian government, I carried out a survey to provide much-needed insight. This article is centered on stories from key informants who are either health professionals or COVID-19 survivors in Abuja, Nigeria.

Dr. Olajumoke Precious works for the Nigeria Center for Disease Control (NCDC) in Abuja. She has never tested positive for the virus but she interacts with patients. Her description of the contact tracing measure employed by



NCDC is completely manual. She recognises that contact tracing is for surveillance, which involves identification, listing, and following up on certain persons who may have had contact or been in the immediate vicinity of the infected person. According to her:

“We do this by interrogating the activities of the case, or activities and roles of the people around the case, since the onset of symptoms. We also probe for places visited within 2-14 days prior to the onset of symptoms. We extract contact information like where the person lives, people around them, the family of the carrier and in cases where the person is dead, we visit the health facilities where the deceased was admitted before he or she died”.

From a survivors’ perspective, Joseph Nikoro, a multi-level marketer and farmer, provided the phone numbers of people he remembered he came in contact with, to health officials, and they told him to call them to ask if they have come in contact with any other persons. Available evidence clearly shows that technology was barely leveraged in all of these measures despite the hype around the efficacy of contact tracing measures, including digital contact tracing methods, and evidence that such apps were introduced in Nigeria.

Looking at the digital rights landscape in Nigeria, it is worrying to see the application of similar digital tracing technology during protests such as the October 2020 #EndSARS protest. While the Nigerian government struggles to demonstrate the effectiveness of the application of technology to fight criminality, terrorism, or stem the tide of a pandemic that represents an existential threat to humanity - which are the reasons usually avowed for buying these technologies - it has never failed to apply these technologies in targeting human rights defenders, critics and protesters. The Nigerian government’s failure to trace bandits and terrorists, who are at the epicenter of the country’s security challenges, remains a mystery despite huge investments in surveillance technologies. The sum of 9 billion naira (US\$22.8 million) was budgeted in 2020 for surveillance-related activities and equipment.

The swiftness with which government critics and protesters are digitally traced and arrested gives a clear indication of the danger of giving a government that has a history of clamping down on dissenting voices more intrusive power to further sinister objectives. These technologies barely serve legitimate purposes other than being a tool for intimidation and harassment of those who



hold dissenting opinions. Eromosele Adene is still facing trial after being tracked, arrested, and charged for his involvement in the #EndSARS protests. Salihu Tanko Yakasai was tracked, arrested and sacked for criticising the President's handling of security issues in the country in a series of tweets, in which he asked the President to resign.

Technology is not a magic wand and is more likely to be used as a tool of intimidation by governments that have clampdown agendas. It is a tool that finds its most noble use in serving the objectives of diligent and competent actors so a governance structure that is bedeviled by incompetence and other anti-democratic tendencies will not effectively deploy surveillance tools for progressive uses. Rather, such governments will find technology tools useful in closing the civic space and shutting down opposition voices. This is why it is important for the technology and civic ecosystem to insist on a proper legislative framework, judicial accountability, and mandatory transparency in the application of surveillance technology.



Rwanda is a small landlocked country in East Africa with a population of approximately 12.6 million people, according to the National Institute of Statistics of Rwanda.¹ The capital Kigali is ever growing with smart technology services and rising urbanization that have shaped the city over the past two decades.

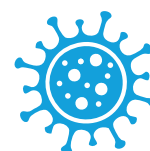
INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN RWANDA

The capital Kigali, plays both administrative and economic roles. This year the COVID-19 pandemic has hampered various areas of the country's life including digital rights, economy and public health as the government fought the deadly virus by introducing several measures to contain the outbreak.

The country is considered one of the most politically stable with a fast growing economy and social-economic transformation in Africa. The Rwandan government led by president Paul Kagame has received widespread global praise and financial support from donors and international financial institutions over the past two decades for its development model.² Since the 1994 genocide against Tutsis, in which about 800,000 people lost their lives according to the United Nations, the political landscape has been dominated by the ruling Rwandan Patriotic Front (RPF) with other small political parties allies in what is known as the National Consultative Forum of Political Organizations.³

President Kagame has won three elections in 2003, 2010 and 2017. Mr. Kagame is often praised for turning the east African country into a development model. However, his



COVID-19
*affected digital
rights, economy
and public health*

1. National Institute of Statistics of Rwanda: November 2020, <http://www.statistics.gov.rw/>

2. The Loyalty of Keeping Rwandans abroad in Check: BBC News Africa: 19 November 2020, <https://www.bbc.com/news/world-africa-54801979>

3. National Consultative Forum of Political Organization, <http://forumfp.org.rw/index.php?id=42>

leadership style is often criticized by human rights organizations and opposition over a poor human rights record, silencing critics, media and a weak civil society.⁴

ICT SECTOR AND POLICIES

Rwanda's Ministry of ICT and Innovation coordinates ICT related policies and programs followed by a regulatory authority, the Rwanda Utilities Regulatory Authority (RURA). RURA was created by the Law N° 39/2001 of 13th September 2001 with the mission to regulate certain public utilities including telecommunications networks and/or telecommunications services, among others. This law was further reviewed and replaced by Law N°. 09/2013 of 01/03/2013,⁵ giving RURA the mandate to regulate telecommunications, information technology, broadcasting and converging electronic technologies, including the internet and any other audio-visual information and communication technology. Additionally, Rwanda Information Society Authority, an agency affiliated to the Ministry of ICT helps the government in digitizing Rwanda.⁶

Rwanda's telecommunication market is composed of two mobile network operators, 24 Internet Service providers (ISPs), one 4G wholesaler and network provider, two network facility providers, and one capacity reseller as of September 2020. The major telecom operators are MTN-Rwanda and Airtel.⁷ Liquid Telecom, formerly Rwandatel,

provides ASP and other internet services such as household broadband. Internet penetration stands at 62,9 % as of March 2020, according to data from the telecom regulator.⁸ However, affordability of devices and low access to broadband widen the digital gap. Data shows 37 % of households don't own phones, while 74.3 % of mobile subscribers rely predominantly on 2G or slower 3G internet services.⁹

In 2000 Rwanda established 'Vision 2020', the country's transformation blueprint to achieve a knowledge based economy status and middle income by 2020. The National Information and Communication Infrastructure (NICI) plans (2000 – 2015) were adopted to guide ICT programs linked to Vision 2020. The country's network coverage is high at 93.5 % for 3G while 4G coverage stands at 96.6 % as of January 2020.¹⁰ Fiber optic is estimated to cover over 3,300 km according to Korea Telecom Rwanda network.¹¹ However, the actual use of broadband is still lower based on the number of active subscribers reported by mobile network operators.¹² While Internet penetration is increasing at 62,3 % as of June 2020, 4G penetration is still low at 5.1% according to data from the regulator.¹³ 74% currently rely on 2G with limited services, namely sms and voice, according to the World Bank.¹⁴ As of September 2020, the cumulative rate of electrification that enables connection and access was 56.7 % of households. The country hopes to connect 100 % of households by 2024 while the

4. Rwanda Country Profile, BBC News: 17 September 2018, <https://www.bbc.com/news/world-africa-14093238>

5. Rwanda's official Gazette, 2013, https://rura.rw/fileadmin/docs/report/Official_Gazette_no_14_bis_of_08_04_2013.pdf

6. Rwanda Information Society Authority, 2017, <https://www.risa.rw/home/>

7. Report for Licensed ICT operators, 2020, https://rura.rw/fileadmin/Documents/ICT/statistics/Report_for_Licensed_ICT_Operators_as_of_Septemembr_2020.pdf

8. Report of Internet subscriptions per category, 2020, <https://rura.rw/index.php?id=164>

9. Accelerating Digital Transformation in Rwanda, 2020, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/912581580156139783/rwanda-economic-update-accelerating-digital-transformation-in-rwanda>

10. Accelerating Digital Transformation in Rwanda, 2020, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/912581580156139783/rwanda-economic-update-accelerating-digital-transformation-in-rwanda>

11. Korea Telecom Rwanda, 2020, <https://www.ktrn.rw/about>

12. Accelerating Digital Transformation in Rwanda, World Bank, 2020, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/912581580156139783/rwanda-economic-update-accelerating-digital-transformation-in-rwanda>

13. ICT and Telecom statistics, 2020, https://www.rura.rw/fileadmin/Documents/ICT/statistics/ICT_and_Telecom_Statistics_report_as_of_June_2020.pdf

14. Accelerating Digital Transformation in Rwanda, 2020, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/912581580156139783/rwanda-economic-update-accelerating-digital-transformation-in-rwanda>

productive users will all be connected by 2022, according to the public energy agency.¹⁵ Telecentres have also helped citizens access digital services especially in rural areas.¹⁶ At the end of the third NICI plans in 2015, the country adopted the Smart Rwanda 2020 Master Plan to advance the country's digital transformation agenda till 2020 and beyond.¹⁷ Despite infrastructure achievements, digital rights and inclusion are still a dream for many amid widening gender and other digital gaps. In 2020, COVID-19 worsened the situation on various fronts including privacy, online freedom of expression, surveillance, digital identity, access.¹⁸

VIOLATIONS OF ONLINE FREEDOM OF EXPRESSION AND COVID-19

Several measures hindered online freedom of expression as a number of bloggers, online content producers sharing content on YouTube, and a photographer were arrested for allegedly flouting COVID-19 rules. In 2018, the country enacted Law N° 60/2018 of 22/8/2018 on prevention and punishment of cybercrimes. The law is criticized for using terrorism and national security as a justification for some of its repressive provisions.¹⁹ On 13th July 2020, photographer Reuben Hamuli was arrested for “publishing and spreading rumors online”.²⁰ According to the police, the man used his Twitter page to make “false” claims that he was wrongfully arrested. Article 39 was cited in this

case.²¹ The law could be abused to restrict free speech especially the article on publishing rumors.

In April 2020, several media practitioners were arrested for allegedly violating COVID-19 guidelines.²² They include Théoneste Nsengimana, a director of Umubavu TV, an online TV channel. Additionally, Dieudonné who runs Ishema TV, a YouTube channel, was arrested a few days after running a report on alleged rights abuses blamed on the army in a Kigali neighborhood. The Committee to Protect Journalists called on Rwandan authorities to facilitate journalists and media workers to do their work without “interference”.²³

Furthermore, criminal defamation provisions in the Penal code of Rwanda have been used to charge media professionals and critics.²⁴ However, in 2018 and 2019 those provisions have been repealed from the penal code.²⁵

***In 2020, COVID-19 worsened
situations on various fronts
including privacy, online
freedom of expression,
surveillance, digital
identity, access.***

15. Electricity access, Rwanda Energy Group, <https://www.reg.rw/what-we-do/access/>

16. Rwanda Telecentre Network, 2020, <https://rtn.rw/about/>

17. Smart Rwanda Master Plan, 2015,

https://www.minict.gov.rw/policies?tx_filelist_filelist%5B%40widget_O%5D%5BcurrentPage%5D=2&cHash=16083ab4b0499921686749e2c5213490

18. “Rwanda: Lockdown Arrests, Abuses Surge”, “End media Crackdown, Mass Arbitrary Arrest”, Human Rights Watch, 24 April 2020,

<https://www.hrw.org/news/2020/04/24/rwanda-lockdown-arrests-abuses-surge>

19. State of Internet Freedom in Rwanda, 2019,

20. “Man arrested for publishing rumours”, The New Times, July 13, 2020, <https://www.newtimes.co.rw/news/covid-19-man-arrested-publishing-rumours>

21. Law on prevention and punishment of cybercrimes, 2018,

https://rura.rw/index.php?id=104&tx_news_pi1%5Bnews%5D=603&tx_news_pi1%5Bday%5D=27&tx_news_pi1%5Bmonth%5D=9&tx_news_pi1%5Byear%5D=2018&cHash=cf6a0de5282574dd3c3a8081a6348b83

22. Cabinet Communique, 2020,

23. “Multiple Journalists arrested throughout covid-19 lockdown period”, 9 September 2020,

24. CIPESA, State of Internet Freedom in Rwanda, 2019, https://www.opennet.africa.org/?wpfb_dl=103

25. “Rwanda court repeals law that bans satirical cartoons”, Reuters, 24 April 2019, <https://www.reuters.com/article/us-rwanda-politics-cartoons-idUSKCN1S02B0>

Despite the repeal of provisions that can be used to hinder freedom of expression online and offline, some are still skeptical and believe there are other means to silence critics. “When it comes to political space and press freedom in Rwanda, Kagame’s regime seems allergic to real progress. His statement on defamation may lead to the scrapping of the law, but that doesn’t make him a visionary who should be embraced just yet”, wrote Fred Muvunyi, a Rwandan journalist, former chairman of Rwanda’s media self-regulation body.²⁶ “Other means exist to persecute critics or clamp down on the opposition”, he added.

PRIVACY AND SURVEILLANCE

In 2019, Rwanda ratified “The African Convention of Cybersecurity and Personal Data Protection”.²⁷ Rwanda’s cabinet approved the country’s draft data protection and privacy law in October. The purpose of the draft law is to provide a mechanism through which the protection and privacy of personal data will be “ensured”. In an editorial titled, “Data protection long overdue, fast-track it” Rwanda Today newspaper said the bill was overdue: “Given the increasing number of Rwandans who have access to digital services, the enactment of this law is long overdue.

Millions of Rwandans are already accessing digital platforms for social networks, studying and work.²⁸ However, the draft law is silent on critical privacy issues raised about personal data such as digital identity and others.

In 2020, surveillance and tracking tools were used to curb the spread of COVID-19, but the lack of transparency could affect people’s rights to privacy. In July, police revealed that the identities of COVID-19 rules’ violators would be digitally recorded to inform “serious actions” in case of recidivism.²⁹ In May, the Rwandan government deployed digital tools to monitor positive cases and to track infections. The applications used phone data profiles to trace people who had been in contact with COVID-19 patients. The system could monitor and geo-fence the people in localized isolation centres to ensure they did not leave their areas of confinement.³⁰ Private WhatsApp, Skype messages and emails have been used as evidence in court cases raising concerns over privacy violation and surveillance.³¹ Communication interception was used to gather evidence in a case of Diane Rwigara, a government critic, but the prosecution lost the case in 2018 for insufficient evidence.³²

In 2020, surveillance and tracking tools were used to curb the spread of COVID-19, but the lack of transparency could affect people’s rights to privacy.

”

26. “Opinion: Rwanda’s Paul Kagame- an enemy of the media parading as a statesman”, DW, 2 May 2019, <https://www.dw.com/en/opinion-rwandas-paul-kagame-an-enemy-of-the-media-parading-as-a-statesman/a-48562042>

27. “AU Convention is finally part of Rwandan Law”, 2019, <https://www.newtimes.co.rw/opinions/au-convention-finally-part-rwandan-law>

28. “Editorial: Data Protection Law Long overdue, fast-track it”, 11 November 2020, <https://rwandatoday.africa/rwanda/opinion/editorial-data-protection-law-long-overdue-fast-track-it-3018844>

29. “Covid19:Police Outlines tough measures against errant violators”, 24 July 2020, <https://www.ktpress.rw/2020/07/covid-19-police-outlines-tough-measures-against-errant-violators/>

30. “Rwanda opts for digital tools in COVID-19 contact tracing”, 2 May 2020, <https://allafrica.com/stories/202005040293.html>

31. State of Internet Freedom in Rwanda, 2019,

32. “Rwandan court acquits the Rwigaras”, 2018, <https://www.theeastafrican.co.ke/news/ea/Rwandan-court-acquits-the-Rwigaras/4552908-4884232-ypfb4s/index.html>



“

Private WhatsApp, Skype messages and emails have been used as evidence in court cases raising concerns over privacy violation and surveillance.

ACCESS AND COST TO THE INTERNET AND TECHNOLOGIES

Despite growing internet penetration, many remain excluded due to mainly poverty as a result many cannot access digital devices, lack internet connection, while others lack digital literacy skills. The average monthly price of 1GB monthly was US\$0.56 in 2018, equivalent to 5.1 percent of the median monthly income. This is more than double the Alliance for Affordable Internet's target of 2% making the cost unaffordable to most citizens.³³ Currently 1,5 GB of 3G costs on average 2 USD which is still unaffordable for many.³⁴ In spite of this, the cost of internet in Rwanda is said to be one of the most affordable in Africa.³⁵

During the COVID-19 lockdowns, education was one of the areas affected by digital exclusion mainly due to the lack of affordability. “A big number of students or parents do not have laptops or smartphones, and most of them cannot access assignments that teachers have been sending through WhatsApp groups since the COVID-19 closure,” said a college principal.³⁶ Data from the World Bank shows 37% don't own phones while the majority relies on 2G services with limited features.³⁷

33. Accelerating Digital Transformation in Rwanda, 2020, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/912581580156139783/rwanda-economic-update-accelerating-digital-transformation-in-rwanda>

34. Airtel, Internet services bundles, <https://airtel.co.rw/internetservice/databundle>

35. “Rwandans spend 7% of their income on Internet”, 2020, <https://www.newtimes.co.rw/news/report-rwandans-spend-7-their-income-internet>

36. “Leading a school during covid-19 crisis: an interview with a school leader”, page 12, 21 September 2020, <https://rwanda.vvob.org/news/online-and-distance-learning-educational-response-covid-19-crisis>

37. Accelerating Digital Transformation in Rwanda, 2020, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/912581580156139783/rwanda-economic-update-accelerating-digital-transformation-in-rwanda>

GENDER AND ACCESS

Gender equality has been at the center of Rwanda's policies to bridge the digital divide. Programmes such as "Girls in ICT mentorship and networking", "Digital Ambassador", "Women in TECH" play a key role. However, women still lag behind in ICT. Figures show that computer literacy is still low but much lower among females than males aged 15-30 years (10.7% compared to 13.8%). The increase since 2014 to 2018 has been very low. The same trend has been observed for the females and males aged 15-24 and in the population aged 15 and above.³⁸ Data from RURA shows that as of June 2020, 26% of telecom staff, that employs 1,127 people, are female while 74% are men.³⁹

Expanding access to digital devices at all households and schools; increasing connectivity and improving access to digital content are some of the solutions to the digital divide.⁴⁰ When measured against the Declaration on the Principles of Freedom of Expression and Access to Information in Africa, concerns rise. Especially in respect to freedom of expression. This is evidenced mainly by strict media regulation such as the process for authorization to set up media organizations and accreditation.⁴¹ In respect of the right to information, Rwanda enacted law N° 04/2013 of 08/02/2013 relating to access to information,⁴² which despite being a progressive law, access to information remains a challenge.⁴³

Despite growing internet penetration, many remain excluded due to mainly poverty as a result many cannot access digital devices, lack internet connection, while others lack digital literacy skills.



38. National Gender Statistics Report, 2019, <https://www.statistics.gov.rw/publication/national-gender-statistics-report-2019>

39. Quarterly ICT statistics report, June 2020, https://rura.rw/fileadmin/Documents/ICT/statistics/Quarterly_ICT_Statistics_report_as_of_June_2020_.pdf

40. Online and distance learning: Education response to the COVID-19 crisis, 21 September 2020, <https://rwanda.vvob.org/news/online-and-distance-learning-educational-response-covid-19-crisis>

41. Safeguarding Civil Society in East Africa, 2017, <https://smallmedia.org.uk/work/safeguarding-civil-society-east-africa>

42. Law relating to access to Information, 2013,

43. "Despite a Progressive law, Access to Information", 2020, <https://panafricanvisions.com/2020/11/despise-a-progressive-law-access-to-information-remains-a-challenge-in-rwanda-report/>

CONCLUSION AND RECOMMENDATIONS



The state of digital rights and inclusion in Rwanda in 2020 has been largely impacted by the COVID-19 pandemic during lockdown and other restrictions that followed. This has been manifested in justified surveillance practices that lacked transparency and raised concerns over privacy and digital rights violation as highlighted in multiple reports cited. Old practices that result in the country's legislations with provisions that can hinder freedom of expression online and offline continued in 2020. Despite the increasing internet penetration, the digital divide is widening as many cannot access and use internet broadband due to high costs of internet services and digital devices, mainly mobile phones. Data shows the digital gender gap remains a key challenge despite the country initiating some impressive programmes to include women in the ICT sector and empowering them to participate in wider digital transformation.

By expanding access to digital devices and internet services to households, this could help decrease the digital divide, especially if done in partnership with telecom firms, digital services providers, telecentres and other ICT stakeholders.

Government should also invest more in digital infrastructures to boost the enabling environment by incentivizing telecom operators and other ICT investors to connect the rural population. The high network coverage without active use does not work to close the digital divide.

Despite the removal of criminal defamation provisions in the country's revised penal code; the article on publishing rumors that is in the cybersecurity law is vague and should be either revised or repealed because it could hinder freedom of expression online.

The gender digital divide hinders the country's progressive gender equality achievements, that aim to boost digital skills among women. These should be further strengthened for better results and authorities should encourage more women to join the ICT sector by sensitizing telecom companies to hire more women and include gender promotion in the employment policy.

The recently approved data protection draft law should be fast-tracked but revised to include other data protection provisions that touch on digital identity and the transparent use of personal data by private and public companies.



South Africa, with a population of 58.5 million,¹ is ranked as the second-largest economy in Africa, but remains one of the world's most unequal societies.²

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN SOUTH AFRICA

Notably, South Africa retains a good reputation in respect of internet rights and freedoms, being ranked as the continent's best-performing country in the Inclusive Internet Index for 2020.³ In recent years, there have been increased efforts to move towards an inclusive digital environment. However, South Africa still faces substantial hurdles in advancing digital rights, and many of the existing inequalities, barriers to access, and structures of discrimination have been magnified by the global pandemic.⁴



Inclusive digital environment

To demonstrate some of the key developments in 2020, this report predominantly relies on desktop research as well as insights from practical experience of working on digital rights in South Africa. This report focuses on key developments throughout 2020 relating to the triad of information rights.⁵

1. The World Bank, (2019) "Population, total – South Africa", <https://data.worldbank.org/indicator/SP.POP.TOTL?locations=ZA>

2. Statistics South Africa, (2019) "Inequality Trends in South Africa: A multidimensional diagnostic of inequality" <http://www.statssa.gov.za/publications/Report-03-10-19/Report-03-10-192017.pdf>. See also, International Monetary Fund (IMF) (2020) "Six Charts Explain South Africa's Inequality", <https://www.imf.org/en/News/Articles/2020/01/29/na012820six-charts-on-south-africas-persistent-and-multi-faceted-inequality>. See Bloomberg, (2020) "Nigeria Tops South Africa as the Continent's Biggest Economy", <https://www.bloomberg.com/news/articles/2020-03-03/nigeria-now-tops-south-africa-as-the-continent-s-biggest-economy>

3. Inclusive Internet Index 2020, (2020) <https://theinclusiveinternet.eiu.com/explore/countries/ZA/>. For further context on internet access in Africa and South Africa, see International Telecommunications Union, (2019) "Time series of ICT data for the world", https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/ITU_Key_2005-2019_ICT_data_with%20LDCs_28Oct2019_Final.xls, and Statista, "Internet user penetration in South Africa from 2017 to 2023", <https://www.statista.com/statistics/484933/internet-user-reach-south-africa/>

4. See University of Chicago Law School - Global Human Rights Clinic, (2020) "Access Denied: Internet Access and the Right to Education in South Africa" <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1000&context=ghrc> and Freedom House, (2020) "South Africa", <https://freedomhouse.org/country/south-africa/freedom-net/2020>

5. The triad of information rights includes access to information, freedom of expression, and the right to privacy.

First, the report reflects on the impact of COVID-19 on the advancement of digital rights. Second, it discusses recent developments in relation to freedom of expression. Third, the report touches on South Africa's privacy landscape. Fourth, the challenges pertaining to internet access and digital exclusion are highlighted. The report concludes with a set of brief recommendations that seek to navigate South Africa's trajectory towards one of access, inclusion, and respect of fundamental rights.

IMPACT OF COVID-19 ON DIGITAL RIGHTS AND INCLUSION

Several of the South African government's responses to COVID-19 implicated, to varying degrees, the triad of information rights. Commendably, through the adoption of regulations, the Independent Communications Authority of South Africa (ICASA) temporarily released a high demand spectrum to assist with easing network congestion, to ensure good quality broadband services, and to facilitate the lowering of costs for internet users.⁶ Additionally, regulations were published on zero-rating health and educational sites.⁷ Mobile network operators MTN and Vodacom further provided zero-rated access to websites providing health and educational resources.⁸ These were important steps for digital inclusion, and illustrated the potential for more meaningful efforts to advance universal access to the internet.

However, of concern, were the regulations that implicated the right to freedom of expression. The dissemination of disinformation in the context of the pandemic was noted as a major concern, prompting the publication of regulations in terms of which it is an offence to publish any disinformation, through any medium, including social media about COVID-19.⁹ Further directions required electronic communications services, licensees, over-the-top providers and internet



6. Information and Communications Technology ("ICT") COVID-19 National Disaster Regulations Notice 238 of 2020, <https://www.icasa.org.za/legislation-and-regulations/ict-covid-19-national-disaster-regulations>. This has recently been extended to March 2021, with an inclusion of licensing fees. See ICASA, "Fees for the extended use of the temporary radio frequency spectrum", 27 November 2020: <https://www.icasa.org.za/news/2020/fees-for-the-extended-use-of-the-temporary-radio-frequency-spectrum>

7. Amendment of ICT COVID-19 National Disaster Regulations 43707 of 2020, https://www.gov.za/sites/default/files/gcis_document/202009/43707gen500.pdf

8. Business Tech, (2020) "MTN announces massive price cuts and free data", <https://businesstech.co.za/news/telecommunications/383443/mtn-announces-massive-price-cuts-and-free-data/>, and Fin24, (2020) "Vodacom to slash data prices by at least 30%, clients get free access to some websites", <https://www.news24.com/fin24/Companies/ICT/vodacom-to-slash-data-prices-by-at-least-30-20200310>

9. Regulations issued in terms of the Disaster Management Act 57 of 2002 (2020) at regulation 11, https://www.gov.za/sites/default/files/gcis_document/202003/regulations.pdf

service providers to remove fake news related to COVID-19 from their platforms.¹⁰ Finally, a much-debated response pertains to the contact tracing methods adopted by the government. Responses in this regard have gone through several iterations, but ultimately resulted in regulations that incorporated several important privacy safeguards, including user notification and an express provision that the interception of the content of communications is not permitted. Notably, a judge was appointed to exercise oversight of the contact tracing program.¹¹ The most recent development in this regard is the COVID Alert SA app, that uses Bluetooth contact-tracing, which is said to rely on privacy-protecting technology.¹² Some of these responses have raised concerns among privacy activists.¹³

FREEDOM OF EXPRESSION

By in large the constitutionally protected right to freedom of expression is well respected in South Africa.¹⁴ In 2020, the Constitutional Court reaffirmed that “it is no exaggeration to characterise the right to freedom of expression as the lifeblood of a genuine constitutional democracy that keeps it fairly vibrant, stable and peaceful. More importantly, free expression is an indispensable facilitator of a vigorous and necessary exchange of ideas and accountability.”¹⁵ Despite this, there are some developments relating

to freedom of expression both on and offline that warrant further monitoring.

■ ENJOYMENT OF FREEDOM OF EXPRESSION ONLINE IN 2020

The use and enjoyment of freedom of expression online is becoming increasingly popular in South Africa, particularly as more users join social media networks to access and disseminate information. It is estimated that there are 22 million active social media users in South Africa.¹⁶ Online spaces create new and exciting opportunities for the advancement of freedom of expression. However, some challenges have arisen when navigating these contemporary spaces. Highlighted below are some of the interesting developments relating to freedom of expression online.

The first relates to a case about a defamatory Tweet.¹⁷ In November 2020, the Supreme Court of Appeal finding that the statement published on Twitter was defamatory and unlawful, accepted that “the rise of social media will continue to focus attention on this area of the law”, noting the far reach of content published by ordinary members of society.¹⁸ The Court further referenced concerns around mis- and disinformation on social media.¹⁹ This marks a noteworthy step towards the development of legal understandings of defamation in the context of social media in South

10. Electronic Communications, Postal and Broadcasting Directions issued under Regulation 10(8) of the Disaster Management Act 57 of 2002 (2020) at regulation 5.1, <https://powersingh.africa/wp-content/uploads/2020/03/COVID-19-Electronic-Communications-Postal-and-Broadcasting-Directions-issued-in-terms-of-the-Disaster-Management-Act-26-March-2020.pdf>

11. Id.

12. See COVID Alert SA App, (2020), <https://sacoronavirus.co.za/covidalert/>

13. See for example Razzano, (2020) “Digital Hegemonies for COVID-19”, <https://globaldatajustice.org/covid-19/digital-hegemonies-south-africa> and Nortier, (2020) “COVID Alert SA app: The fine balance between public health, privacy and the power of the people”, <https://www.dailymaverick.co.za/article/2020-10-13-covid-alert-sa-app-the-fine-balance-between-public-health-privacy-and-the-power-of-the-people/>

14. Section 16 of Constitution provides that “everyone has the right to freedom of expression” subject to certain forms of speech that are not protected. South African Constitution, (1996), <https://www.gov.za/documents/constitution-republic-south-africa-1996>

15. *Economic Freedom Fighters and Another v Minister of Justice and Correctional Services and Another* [2020] ZACC 25 at para 1, <http://www.saflii.org/za/cases/ZACC/2020/25.html>

16. Datareportal, (2020) “South Africa”, <https://datareportal.com/reports/digital-2020-south-africa>

17. The case was brought by Trevor Manuel, a prominent South African politician and former Minister of Finance against the Economic Freedom Fighters (EFF), South Africa's third-largest political party, as a result of a statement published by the EFF on Twitter in March 2019. *Manuel v Economic Freedom Fighters and Others* [2019] ZAGPJHC, <http://www.saflii.org/za/cases/ZAGPJHC/2019/157.html>. This matter raised interesting questions about Twitter defamation, the ordinary social media user, and the implication of ongoing publication. For further commentary see Singh, (2019) “Social Media defamation online: Guidance from Manuel v Eff”, <https://altadvisory.africa/2019/05/31/social-media-and-defamation-online-guidance-from-manuel-v-eff/>

18. *EFF and Others v Manuel* [2020] ZASCA 172, at paras 57 and 64, <http://www.saflii.org/za/cases/ZASCA/2020/172.pdf>

19. Id at paras 112-113.



The use and enjoyment of freedom of expression online is becoming increasingly popular in South Africa, particularly as more users join social media networks to access and disseminate information.

Africa.²⁰

The second development concerns a trend in which companies are misusing court processes to quash freedom of expression, to stifle and restrict speech, and to intimidate those who are critical of them.²¹ In April 2020, amidst South Africa's lockdown occasioned by COVID-19, a mining house operating in South Africa unsuccessfully sought to prevent community activists from using the media and social media to level concerns and criticism against the mine. The application if successful would have set a dangerous precedent which would have a chilling effect on free speech both on- and offline.

Fortunately, the application was withdrawn, and the community activists can continue sharing information and express opinions.

The third is the publication of the Draft Films and Publications Amendment Regulations by the Minister of Communications and Digital Technologies.²² The Regulations were set to provide greater clarity and direction on how content that is distributed online for commercial gain is classified.²³ However, the regulations caused an uproar, with concerns that the regulations were draconian and an attempt to censor the internet.²⁴ Civil society organisation Media Monitoring Africa (MMA)

20. It is necessary to note that this matter did not relate to criminal defamation. criminal defamation remains in South Africa, it is not frequently used, and there have been suggestions to do away with it. See Freedom House above n 4.

21. Right2Know Campaign, (2020) "Mine abandons attempt to silence community activists", <https://www.r2k.org.za/2020/09/23/statement-mine-abandons-attempt-to-silence-community-activists/>

22. Films and Publications Act, 65 of 1996, as amended, Draft Films and Publications Amendment Regulations, 2020, https://www.gov.za/sites/default/files/gcis_document/202007/43495gen361.pdf

23. Kamineth et al, (2020), "Film and Publications Amendment Act: Protecting, not censoring, our citizens in the digital age", <https://www.dailymaverick.co.za/article/2020-08-27-film-and-publications-amendment-act-protecting-not-censoring-our-citizens-in-the-digital-age/>

24. Malinga, (2020), "Citizens reject 'Internet Censorship Act', threaten court action", <https://www.itweb.co.za/content/rxP3jqBmBe9MA2ye>

submitted comments on the Draft Regulations noting that there are “significant consequences for the exercise of rights online, particularly the right to freedom of expression”.²⁵ Further to this, MMA submitted that it is concerned that the Draft Regulations create a framework that is unenforceable and unworkable, which is far from ideal given that “the current regulatory and policy framework regarding ICTs and online content in South Africa is confusing, uncertain and uncoordinated, which may be exacerbated by the broad scope of the Draft Regulations.”²⁶ There is likely to be further movement on the Draft Regulations in 2021, either in the form of a further amendment, or in the form of publication.

■ HATE SPEECH AND INCITEMENT

In terms of unprotected expression, it is necessary to note that the legal understanding of hate speech in South Africa is under consideration. This follows a finding by the Supreme Court of Appeal in 2019 which found the hate speech provisions of the Promotion of Equality and Prevention of Unfair Discrimination Act (Equality Act) unconstitutional.²⁷ The Constitutional Court is currently seized with two hate speech matters that are likely to have a significant bearing on South Africa’s legal definition for hate speech which will in turn impact how hate speech is tested both on- and offline.²⁸ Unfortunately, and amidst the legal uncertainty, there has also been a rise in the dissemination of

hurtful and harmful content across social media platforms, with online manifestations of xenophobia,²⁹ gender discrimination and harassment,³⁰ and racial tensions.³¹

A further notable development relates to the recent ruling by the Constitutional Court regarding incitement.³² The Constitutional Court declared the provision relating to incite in the Riotous Assemblies Act inconsistent with the right to freedom of expression.³³ This matter concerned statements that allegedly encouraged people to occupy land, resulting in a criminal charge for inciting people to trespass. The majority of the Constitutional Court made some notable pronouncements regarding the import of the right to freedom of expression. While this matter was not about online incitement it is important to note that the Cybercrimes Bill, which was passed by both Houses of Parliament on 2 December 2020 and is now pending before the President for signature, deals with incitement in Chapter 2.³⁴ This judgment may have an impact on how malicious communication is circumscribed in the Bill, which could impact how incitement online is understood and addressed.

Online manifestations of xenophobia, gender discrimination, harassment and racial tensions.

25. Media Monitoring Africa, (2020), “Draft Films and Publications Amendment Regulations, 2020: Written Submission by Media Monitoring Africa”, <https://mediamonitoringafrica.org/wp-content/uploads/2020/08/200817-MMA-Submission-on-the-Films-and-Publications-Amendment-Regulations.pdf>
26. Id.

27. The case concerned statements published in a news article which allegedly contravened section 10 of the Equality Act for advocating hatred based on sexuality. This prompted a challenge to the constitutionality of section 10. In 2019, the Supreme Court of Appeal declared the section unconstitutional and invalid. The Constitutional Court must decide whether to confirm the declaration of unconstitutionality. *Qwelane v South African Human Rights Commission and Another* [2019] ZASCA 167, <http://www.saflii.org/za/cases/ZASCA/2019/167.html>

28. See *South African Human Rights Commission v Masuku* case resources, <https://collections.concourt.org.za/handle/20.500.12144/36612?show=ful>.

29. Centre for Analytics and Behavioural Change (2020) “Interim report on xenophobia on South Africa Social Media”, <https://drive.google.com/file/d/1aEKfwQfo-gower4Te9FIWRBj5NYql2li/view>

30. Iyer et al, (2020) “Alternate Realities, Alternative Internets: African Feminist Research for a Feminist Internet”, https://www.apc.org/sites/default/files/Report_FINAL.pdf. See further, Gender Links (2018) “Glass Ceilings: Women in South African Media Houses”: <http://www.womeninnews.org/ckfinder/userfiles/files/Glass-Ceilings-Report-19-October-2018.pdf>

31. Barlett, (2020) “In South Africa, Racial Tensions Simmer Amid a Pandemic”, <https://foreignpolicy.com/2020/06/12/south-africa-coronavirus-pandemic-racial-tensions/>

32. *Economic Freedom Fighters and Another v Minister of Justice and Correctional Services and Another* above n 15.

33. Section 18(2)(b) of the Riotous Assemblies Act criminalises the incitement of others to commit “any offence”. The South African Parliament has until November 2022 to rectify the constitutional defect in the Act.

34. Cybercrimes Bill B6D-2017, <https://pmg.org.za/bill/684/>



■ MIS- AND DISINFORMATION

Further to the above, concerns regarding the criminalisation of mis- and disinformation are on the rise following oscillating responses to disinformation by the South African Police Service (SAPS). SAPS has on two separate occasions issued warnings regarding the dissemination of disinformation being shared across social media. The first warning suggested that the publication, distribution, disclosure, transmission, circulation or spreading of false information or fake news is an offence.³⁵ In the second warning SAPS pleaded to members of the public to not disseminate disinformation.³⁶ Apart from the COVID-19 regulations disinformation is not a criminal offence in South Africa. Prior to this, South Africa had signalled its election not to criminalise disinformation. This is most notably illustrated in the marked difference between the Cybercrimes and Cyber Security Bill³⁷ and the more recent Cybercrimes Bill.³⁸ The former criminalised the dissemination of false data messages.

This has been removed from the most recent version of the Cyber Bill which does not include provisions that would make it an offence to publish inherently false data messages. Therefore, the remarks by SAPS are concerning and appear to align with troubling regional trends towards disinformation.³⁹

THE RIGHT TO PRIVACY

South Africa's privacy landscape has seen important data protection developments and potential advancements around digital IDs on the one hand, and a lack of adequate protection in relation to various surveillance practices on the other. While the right to privacy is constitutionally protected in South Africa,⁴⁰ its application in the digital environment is an emerging concept for many people who are beginning to grapple with evolving understandings of why privacy is important, what personal information means, and the implications of different ways in which state and non-state actors may be eroding privacy rights.

■ DATA PROTECTION AND DIGITAL IDS

During 2020, the President brought the substantive provisions of South Africa's data protection law – the Protection of Personal Information Act (POPIA)⁴¹ – into force, with a one-year grace period for compliance. This was a welcomed development for data protection, both to ensure much needed regulatory compliance, but also to ensure that the right to privacy is meaningfully realised in the information age.⁴²

35. SAPS, (2020) "Media Statement: Angry protesters harm racehorses at stables in Port Elizabeth", <https://www.saps.gov.za/newsroom/msspeechdetail.php?nid=28349>

36. SAPS, (2020) "Media Statement: Police caution the public against the incessant peddling of fake news relating to human trafficking and kidnapping of women and children", <https://www.saps.gov.za/newsroom/selnewsdetails.php?nid=28467>

37. No. 40487 of 2016 at section 17(2), <https://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf>

38. Cybercrimes Bill above n 34.

39. See Communiqué of the 40th Ordinary Summit of SADC Heads of State and Government, (2020)

https://www.sadc.int/files/8115/9767/2537/Communique_of_the_40th_SADC_Summit_August_2020_-ENGLISH.pdf. During the Summit Member States were urged to take pro-active measures to mitigate external interference, the impact of fake news and the abuse of social media, especially in electoral processes.

40. Section 15 of the South African Constitution.

41. 4 of 2013, <https://www.justice.gov.za/infoereg/docs/InfoRegSA-POPIA-act2013-004.pdf>

42. Singh, (2020) "Why POPIA is about rights – not just compliance", <https://altadvisory.africa/2020/06/23/why-popia-is-about-rights-not-just-compliance>

POPIA will come into effect on 1 July 2021.⁴³ In December 2020, the Official Identity Management Policy was published for comment.⁴⁴ The Policy forms part of South Africa's efforts to enhance identity management and digital identity development. The Policy, still in a nascent stage, will likely have a significant bearing on South Africa's identity management framework which is set to enable an inclusive digital population register that is secure, accurate and confidential.

■ SURVEILLANCE

From a surveillance perspective, there have been two interesting jurisprudential developments. A constitutional challenge to various provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA),⁴⁵ which authorises state surveillance, is presently before the Constitutional Court.⁴⁶ It has been argued that RICA is unconstitutional for failing to provide adequate safeguards, and for creating a chilling effect on the right to privacy and associated constitutional rights, including freedom of expression, freedom of the media, and access to courts. Another notable development relates to developing jurisprudence in response to applications for the roll-out of CCTV video surveillance networks in the city of Johannesburg.⁴⁷ Privacy activists are concerned that this is being done in the absence of an enabling

legal framework which is contrary to the constitutionally protected right to privacy.⁴⁸ It is hoped that effective and appropriate safeguards will be implemented soon as the use of new technologies may threaten the enjoyment of privacy rights.

INTERNET ACCESS

■ PROHIBITIVELY HIGH DATA COSTS

South Africa's prohibitively high data costs remain a primary obstacle to access and connectivity, and in turn a primary barrier to the exercise of digital rights.⁴⁹ Recent statistics suggest that approximately 63% of people in South Africa are part of the digital population as internet users; however, it appears that only 10.4% of South African households can access the internet at home, for people living in rural areas this figure sits at 1.7%.⁵⁰ The stark rural/urban digital divide remains a concern. Fortunately, there have been several indicators that state and non-state actors are seeking to facilitate access to the digital environment. Following the 2019 recommendations of the Competition Commission that data prices in South Africa were too high and that pricing structures are "anti-poor",⁵¹ mobile telecommunications networks have begun decreasing their prices. This is likely to contribute positively to advancing internet access in South⁵²

43. The Presidency, (2020) "Commencement of certain sections of the Protection of Personal Information Act, 2013", <http://www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013>

44. Department of Home Affairs, (2020) "Draft Official Identity Management Policy", https://static.pmg.org.za/Draft_Official_Identity_Management_Policy_Version_with_Call_for_Comments.pdf

45. 70 of 2002, https://www.gov.za/sites/default/files/gcis_document/201409/a70-02.pdf

46. See Constitutional Court case resources for access to pleading and updates on the matter, <https://collections.concourt.org.za/handle/20.500.12144/36631>

47. Vumacam (Pty) Ltd v Johannesburg Roads Agency and Another 14867/2020, <https://powersingh.africa/wp-content/uploads/2020/07/vumacam-judgment.pdf>

48. Id. See further written submissions by Right2Know Campaign who intervened as amicus curiae, <https://powersingh.africa/2020/07/22/vumacam-pty-ltd-v-johannesburg-roads-agency-and-another/>

49. UNHRC, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (2011) (accessible at https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

50. Statista, (2020) "Digital population in South Africa as of January 2020" <https://www.statista.com/statistics/685134/south-africa-digital-population/> and Statistics South Africa, (2018) 'General Household Survey' (2018)

51. Competition Commission Data Services Market Inquiry, (2019) (accessible at <http://www.compcom.co.za/wp-content/uploads/2019/12/DSMI-Non-Confidential-Report-002.pdf>)

52. ICASA, (2020) "Communications & Digital Technologies Ministry and ICASA welcome steps taken by the Competition Commission to facilitate data prices reduction at the retail level of the market", <https://www.icasa.org.za/news/2020/communications-digital-technologies-ministry-and-icasa-welcome-steps-taken-by-the-competition-commission-to-facilitate-data-prices-reduction-at-the-retail-level-of-the-market>



Africa. Additionally, ICASA has begun an application process for the allocation of high demand spectrum.⁵³ ICASA is also working with various stakeholders to better understand, among other things, the state of the mobile retail market.⁵⁴ The final outcome of this process will likely have a positive impact on access and connectivity in South Africa. These steps by ICASA are set to generate a significant improvement in accessing the digital environment. A further development set to improve access was seen in the performance agreement signed by President Ramaphosa and Communications and Digital Technologies Minister Stella Ndabeni-Abrahams.⁵⁵ The agreement confirms that the Minister must ensure that 80% of the population have access to the internet by 2024 and the current cost of mobile data must be reduced by 50%.

■ DIGITAL INFRASTRUCTURE

Further to the above efforts, there have been promising indicators illustrating the advancement of South Africa's digital infrastructure. 5G has been the most notable digital infrastructure development of 2020. Most major mobile networks are offering or working towards offering access to 5G networks for its clients.⁵⁶ The Draft Policy on the rapid deployment of electronic communications networks was published in 2020.⁵⁷ The draft policy is intended to "provide clarity on the deployment of electronic communications networks and facilities".⁵⁸

The publication of the Report of the Presidential Commission on the 4th Industrial Revolution was an important moment for South Africa's digital landscape.⁵⁹

53. ICASA, (2020) "Invitation to Apply (ITA) notice to invite applications for the radio frequency spectrum licences for International Mobile Telecommunication (IMT) Spectrum band", <https://www.icasa.org.za/legislation-and-regulations/ita-for-the-radio-frequency-spectrum-licences-for-imt-spectrum-bands>.

54. ICASA, (2020) "Public Hearings on the Mobile Broadband Service Inquiry", <https://www.icasa.org.za/news/2020/public-hearings-on-the-mobile-broadband-services-inquiry>. This follows the 2019 publication and call for comment on the Discussion Document which makes various preliminary findings in respect of the current state of the retail market, spectrum, site access, roaming and mobile virtual network operators. See ICASA, (2019) "Discussion Document on The Markey Inquiry Into Mobile Broadband Services", <https://www.icasa.org.za/legislation-and-regulations/discussion-document-on-the-market-inquiry-into-mobile-broadband-services>.

55. Performance agreement between President Cyril Ramaphosa and Minister of Communications and Digital Technologies, (2020), https://www.gov.za/sites/default/files/The/PA_comm-dig-ndabeni-abrahams.pdf

56. Labuschangne, (2020) "South Africa's 5G prices and coverage – Vodacom vs MTN vs Rain", <https://mybroadband.co.za/news/5g/369289-south-africas-5g-prices-and-coverage-vodacom-vs-mtn-vs-rain.html#:~:text=Rain%20was%20the%20first%20to,Vodacom%20and%20MTN%20in%202020.&text=Rain%20claims%20its%20Premium%205G,150Mbps%2D200Mbps%20given%20enough%20spectrum>

57. Proposed policy and policy direction on rapid deployment of electronic communications networks and facilities, (2020), <https://www.ellipsis.co.za/wp-content/uploads/2015/11/Draft-Policy-Direction-on-Rapid-Deployment-of-Electronic-Communications-Networks-and-Facilities-22-July-2020.pdf>

58. It is necessary to note that the draft policy has caused a significant public outcry, chiefly, because the policy envisages permitting electronic communications network service licensees the right to enter upon and use private land for the deployment of such networks and facilities. See Winks, (2020) "Stella's 5G rollout plan raises tempers and questions of constitutionality", <https://citizen.co.za/news/south-africa/government/2330147/stellas-5g-rollout-plan-raises-tempers-and-questions-of-constitutionality/>

The Report indicates that digital literacy and the development of 4IR infrastructure will be prioritised. Further, the Report recommends that South Africa develops a geostationary telecommunications satellite, which would provide quality connectivity to marginalised communities in the SADC region.

■ DIGITAL EXCLUSION

Unfortunately, the efforts towards access and infrastructure may remain inconsequential without appropriate steps to bridge the digital divide and meaningfully advance digital literacy skills.⁶⁰ Without the requisite skills, meaningful and active participation with online services is unlikely.⁶¹

In South Africa, the pervasive digital divide runs across historical lines of oppression and is exacerbated in the context of access to digital literacy skills.⁶² A recent report found “the discriminatory access to the internet further undermines the right to equality and non-discrimination, guaranteed both by the Constitution and under international human rights law.”⁶³ In the context of health care, particularly when it comes to accessing health-related information during times of crisis, digital exclusions can have a significant impact on information rights, which in turn may implicate an array of other rights.⁶⁴

The gender-digital divide, while not as pervasive in South Africa as other parts of the region, still exists with 60% internet access for men and 52% for women.⁶⁵ However, a key concern in the context of equality and inclusion relates to online gender-based violence.⁶⁶ It is necessary to note that during the lockdown in South Africa, United Nations Women released a statement calling for an end to cyber violence against women and girls in South Africa, while no statistics were referenced, the statement in and of itself is indicative of a significant problem.⁶⁷

Markedly, a multi-stakeholder group has called for a responsible approach to regulating domestic violence facilitated by technologies.⁶⁸ This follows a law reform process in which South Africa’s Parliament is revising various laws to address the scourge of gender-based violence in the country. It is hoped that through this process there will be a greater recognition that South African laws need to be responsive to contemporary and evolving challenges.

The discriminatory access to the internet further undermines the right to equality and non-discrimination

59. Report of the Presidential Commission on the 4th Industrial Revolution, (2020), <https://altadvisory.africa/wp-content/uploads/2020/11/Report-of-the-Presidential-Commission-on-the-Fourth-Industrial-Revolution.pdf>

60. Universal Access to the Internet and Free Public Access in South Africa (2019) (Universal Access) (accessible at <https://internetaccess.africa/universal-access/>)

61. Media Monitoring Africa (2020) “Submissions on the Draft National Youth Policy for 2020-2030 (NYP2030)”, <https://mediamonitoringafrica.org/wp-content/uploads/2020/03/200316-MMA-Submission-on-the-NYP2030.pdf>

62. Violence Prevention Through Urban Upgrading, ‘Bridging the New Digital Divide’ (2019) (accessible at <http://vpuu.org.za/ict4d/digital-divide-south-africa/>)

63. Global Human Rights Clinic of the University of Chicago Law School; ALT Advisory, Acacia Economic and MMA, ‘Access Denied: Internet access and the right to education in South Africa’ (2020) at 17 (faccessible at <https://internetaccess.africa/wp-content/uploads/2020/09/Access-Denied-Report-2020-FINAL-min.pdf>)

64. Association for Progressive Communications (APC), (2020), “Closer than ever: Keeping our movements connected and inclusive – APC’s response to the covid-19 pandemic”, https://www.apc.org/sites/default/files/closerthanever_pp.pdf

65. Sornger et al, (2020), “Bridging the Gender Digital Gap”, https://www.g20-insights.org/policy_briefs/bridging-the-gender-digital-gap/. See also Power, (2020) “The gender digital divide and COVID-19: Towards feminist internet regulations in Southern Africa”, https://africaninternetrights.org/sites/default/files/Tina_Power.pdf

66. Iyer et al above n 30.

67. UN Women, (2020) “Press statement: Calls for attention to cyber violence and its devastating effect on women and girls in South Africa”, <http://www.un.org.za/press-statement-calls-for-attention-to-cyber-violence-and-its-devastating-effect-on-women-and-girls-in-south-africa/>

68. Research ICT Africa, et al (2020) “Submissions on the Domestic Violence Bill”, <https://altadvisory.africa/wp-content/uploads/2020/10/Domestic-Violence-Amendment-Bill-B20-%E2%80%932020-Joint-Submissions-by-RIA-APC-ALT-FWA.pdf>

CONCLUSION AND RECOMMENDATIONS

The trajectory in advancing digital rights in South Africa has had some promising developments; however, barriers to access, the existing gaps in legal frameworks and certain regulatory developments have raised cause for concern.

Three key recommendations arise.

- First, efforts towards effectively advancing meaningful access and digital literacy need to be prioritised, with universal, meaningful access for all persons in South Africa being the target.
- Second, jurisprudential developments and law reform processes need to be responsive to contemporary challenges, and need to ensure that adequate and effective protections are afforded to all those who need it.
- Finally, all decisions, at a legislative, policy or institutional level, must be informed by the Constitution and South Africa's commitments to international human rights law.

South Africa stands at a critical junction: one path tends towards a harmful digital environment that neglects human rights imperatives, whereas the other advances the formation of a safe, accessible, and inclusive online world. The hope is that as we move into 2021, South Africa chooses the latter.





Tanzania is a country in East Africa with a population of over 55 Million, according to the Tanzania Bureau of Statistics.¹ Tanzania has been under the rule of Chama Cha Mapinduzi (CCM), the dominant ruling party, with fierce opposition growing in the last decade as more opposition parties emerge.²

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN TANZANIA

The communication sector is under the Ministry of Transport, Work, and Communication. However, an independent body called The Tanzania Communication Regulatory Authority (TCRA) handles regulation in this sector. TCRA was established under the TCRA Act no. 12 of 2003.³

Tanzania has taken a turn for the worse in the last five years as far as digital rights are concerned, with an increase in the legislation of laws restricting the enjoyment of internet freedoms. Over the last five years, several pieces of legislation have been passed as laws, amended to further restrict the online space in various ways. Legislation such as the Cybercrimes Act (2015) has been used to prosecute online users perceived to be critical of the persona of the president or other authorities in power. This was followed up by laws such as the Electronics and Postal Communications (SIM card regulation, online content regulation and statistics) Act.



Legislation of Laws
restricting the enjoyment
of internet freedom

This report has drawn its information and data from doing desk research, reviewing news, policy briefs, country reports, shadow reports, policies and regulations as well as the

1. National Bureau of Statistics: Tanzania Figures, June 2019,

2. www.nationsonline.org/oneworld/tanzania.htm

3. www.tcra.go.tz

Constitution of the United Republic of Tanzania. These sources were captured from official government websites such as the TCRA, Parliament's website as well as news from reputable media, civil society organizations, human rights activist's social media handles among others. This country report addresses the impact of COVID-19 regulations on digital rights and inclusion, enjoyment of Freedom of expression online, privacy, digital IDs and surveillance, internet access, hate speech, misinformation and criminal defamation laws, the extent of digital exclusion and its impact on human rights, gender and digital infrastructure.

IMPACT OF COVID-19 REGULATIONS ON DIGITAL RIGHTS AND INCLUSION

On the 16th of March 2020, Tanzania reported its first case of Coronavirus,⁴ since then the country last reported a total of 509 and then stopped publishing information.⁵ However, for a country that has already been at crossroads with the fulfillment of human rights across the region and a president critiqued for ignoring human rights, the pandemic didn't change the dynamics of practice but rather intensified the situation. In the light of the pandemic and how the region has taken proactive measures in different capacities to overcome the challenges, Tanzania has denied its citizens their right to information as well as freedom of expression even via avenues such as social media. When the US Embassy in Tanzania issued a high health alert message to its citizens

regarding the unknown state of COVID-19 in Tanzania, Kwanza TV shared this information on Instagram and was thus the reason its license was suspended.⁶

ENJOYMENT OF FREEDOM OF EXPRESSION ONLINE IN 2020

Throughout 2020, several media outlets have been suspended for a few days up to several months. In July 2020, the Contents Committee of the Tanzania Communications Regulatory Authority summoned Kwanza Online TV stating that their Instagram account featured a post that was unpatriotic and negative to the country. Following the summons, Kwanza TV stated that they were not given enough time to respond to the charges. The regulator shortly thereafter issued a statement⁷ that the broadcaster had published misleading content that contravened professional standards, and hence was suspended for 11 months.⁸

Activists and human rights organizations had argued about the implications and use of the recent legislation that was passed such as the Electronic and Postal Communication Act, 2010 (EPOCA) online content regulation and the Cybercrimes Act among others. Their use became more apparent as elections drew near and a clampdown was initiated to block online avenues as spaces of assembly, mobilization, and information sharing. In months leading up to the election, activists, inspired by a well-known religious leader, with the influence of online activists initiated an online protest that ran right up to elections demanding an independent electoral commission.⁹ This mobilization was mostly

4. VOA: Tanzania Confirms First Case of Coronavirus, March 2020, <https://www.voanews.com/science-health/coronavirus-outbreak/tanzania-confirms-first-case-coronavirus>

5. Worldometer: Tanzania COVID Cases, November 2020, <https://www.worldometers.info/coronavirus/country/tanzania>

6. Reporters without borders: Tanzania suspends another media outlet over its COVID-19 coverage, July 2020, <https://rsf.org/en/news/tanzania-suspends-another-media-outlet-over-its-covid-19-coverage>

7. TCRA Twitter Handle: Taarifa kwa Vyombo vya Habari, July 2020, https://twitter.com/TCRA_Tz/status/1280137947199782919?s=20

8. CPJ: Tanzania bans Kwanza Online TV for 11 months citing 'misleading' Instagram post on COVID-19: July 2020, <https://cpj.org/2020/07/tanzania-bans-kwanza-online-tv-for-11-months-citing-misleading-instagram-post-on-covid-19/>

9. Twitter: Maria Sarungi tweets on wearing white attires as a silent protest requesting an independent electoral body, June 2020, <https://twitter.com/mariastsehai/status/1277572130851479552?lang=en>

done online via Twitter with many of their followers tweeting pictures while dressed in white as a silent protest. Among the prohibited contents in the new online content regulations included “content that is involved in planning, organizing, promoting or calling for demonstration, marches or the like which may lead to public disorder”.¹⁰

PRIVACY, DIGITAL IDS AND SURVEILLANCE

While Tanzania does not yet have a data protection and privacy policy, its constitution does guarantee the right to privacy, however this is not reflected in relevant laws effectively. The Electronics and Postal communication (SIM card regulations) Act 2020 was published on 7 February 2020 making it mandatory for all SIM card users in Tanzania to register their SIM cards biometrically.¹¹ The move to register SIM cards with biometrics comes under the condition that one possesses a national identification number (NIN) and/or ID to get registered; however, without a law governing data protection and privacy, this could prove harmful. Individuals are required by this law to provide personal data that is accessible by public agencies such as telecoms. Laws in Tanzania are yet to guarantee the right to communicate anonymously on the internet removing the right to anonymity.

Activists and human rights organizations had argued about the implications and use of the recent legislation that were passed.



INTERNET ACCESS

Recently the Tanzania Communications Regulatory Authority reported an increase of mobile internet subscribers to 27 million with slightly over a million new users gained within the first two quarters of the year 2020.¹² According to Research ICT in Africa, 1GB in Tanzania as of the second quarter of 2020 cost \$2.17¹³ making it the highest in the East African region despite the fact that in September 2019 it had the lowest costs in the region. Their research compares the prices of 1GB of daily mobile internet by taking into account the mean charges of the total Internet Service Providers (ISPs) in each country. In comparison to the standard of living of Tanzanians, whose GDP per capita as of 2019 according to the world bank is at \$1122,¹⁴ makes bread or broadband a choice for many users. Due to food insecurity, data is not a priority in their daily lives leading to self-censorship or withdrawal from internet usage. While internet users have grown, the gender digital gap, as well as rural and urban access gaps, still exist with the decentralization of opportunities limited.

10. TCRA: The Electronics and postal communications (online content regulations), 2020,

[https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20\(Online%20Content\)%20Regulations,%202020](https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20(Online%20Content)%20Regulations,%202020)

11. Clyde and Co: SIM card registration in Tanzania, July 2020, <https://www.clydeco.com/en/insights/2020/07/sim-card-registration-in-tanzania>

12. Tanzania Communications regulatory authority: Quarterly communication statistics, September 2020, <https://www.tcra.go.tz/publication-and-statistics/statistics>

13. Research ICT Africa Mobile Pricing (2020), https://researchictafrica.net/ramp_indices_portal

14. World bank data indicator (2019), <https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=TZ>



“

The Electronics and Postal communication (SIM card regulations) Act 2020 was published on 7 February 2020 making it mandatory for all SIM card users in Tanzania to register their SIM cards biometrically.

HATE SPEECH, MISINFORMATION AND CRIMINAL DEFAMATION LAWS

Tanzania does not have a specific law that addresses hate speech as some countries do however it has some pieces of legislation that address some of these concerns. The Online Content Regulation (2020) in section 16, section 3(m) states that among prohibited content includes “content that promotes or favors what would raise sedition, hatred, racism...” The same regulation also addresses concerns on “content that aims to publish information for the purpose of ridicule, abuse or harming the reputation, prestige or status of Tanzania”.¹⁵

THE EXTENT OF DIGITAL EXCLUSION AND ITS IMPACT ON HUMAN RIGHTS

Tanzanian students in primary school are required to learn ICT studies in a subject called “Tehama” however majority of public schools do not have access to computers or the internet, making it more of a theoretical subject. Access to the internet is more prevalent in urban areas than rural areas, making access a challenge as large infrastructure investments are made in urban areas where the market is wider. The result of this is the lack of decentralization of opportunity as well as the majority being denied access to rights such as the right to access to information.

¹⁵ Section 16 of the online content regulations (2020), [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKewj55tnO-JPuAhWGUCaKHQonBpsQFjAAegQIAxAC&url=https%3A%2F%2Fwww.tkra.go.tz%2Fdocument%2FThe%2520Electronic%2520and%2520Postal%2520Communications%2520\(Online%2520Content\)%2520Regulations%2C%25202020&usg=AOvVaw0WCGjGOL_OjzqPC3XhiYGk](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKewj55tnO-JPuAhWGUCaKHQonBpsQFjAAegQIAxAC&url=https%3A%2F%2Fwww.tkra.go.tz%2Fdocument%2FThe%2520Electronic%2520and%2520Postal%2520Communications%2520(Online%2520Content)%2520Regulations%2C%25202020&usg=AOvVaw0WCGjGOL_OjzqPC3XhiYGk)

GENDER AND ICT

While laws such as the Cybercrime Act address concerns such as cyberbullying, they are not gender-centric as they do not address gaps in terms of online violence, stalking, harassment, and illegal use of images/videos, especially for women.

Tanzania's lack of data protection and privacy policy leaves special groups such as women vulnerable to technology-related gender-based violence leading to self-censorship and withdrawal from the use of the internet.

CONCLUSION AND RECOMMENDATIONS



Tanzania has lost the reputation of upholding democracy and rights whether it is online or offline. With the use of rule of law and the recent shutting off of the internet, they have further distanced themselves from protecting civic spaces, the so-called “front porches of democracy”, by limiting the freedoms and rights of the people.

To ensure that citizen's voices are not silenced nor their avenues of exercising rights are not denied, it's essential that Tanzania revisits its constitution and ensure that the rights and freedoms guaranteed such as Article 16 of the Constitution that recognizes the right to privacy. This article states that “every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications.”¹⁶ The Constitution ought to be complemented by rights-respecting laws and policies.

Tanzania ought to uphold a human rights-based approach when enacting regulations that will cause distress between right holders and duty bearers to ensure equal access to opportunities accorded in both the offline and online world. To ensure digital inclusion, ICT policies in Tanzania need to address the needs of special groups such as women and people with disabilities. Tanzania has a long way to ensuring rights and inclusion in the digital space but a great way to start is to set the right parameters for policy development that foster inclusion in decision making and to ensure that it is people-centered.

¹⁶ The constitution of the United Republic of Tanzania(1977), www.parliament.go.tz/publication/journals



A coastal country in West Africa, Togo shares its borders with Ghana, Benin and Burkina Faso and is home to approximately 7.8 million people. Poverty and inequality remain quite high, especially in rural areas where 69% of households were living below the poverty line in 2015.¹ Togo's Human Capital Index (HCI) remains at a low 0.41.²

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN TOGO

The ruling party, the Union for the Republic (UNIR), has been at the forefront of politics for several years. It currently holds 59 out of 91 seats in the National Assembly following the 2018 general elections. The presidential elections, held on February 22 2020, re-elected Faure Gnassingbé as Head of the country. Faure Gnassingbé is entering his fourth five-year term since he was first elected in 2005. For the first time in 32 years, Togo held local elections in June 2019 to elect its municipal councilors. UNIR won the majority of seats (878 seats out of 1,490 seats).

According to Hootsuite and We are social,³ in January 2020 there were 1.71 million internet users in Togo. The number of internet users in Togo increased by 124,000 (+7.8%) between 2019 and 2020. Internet penetration in Togo was 21% in January 2020. There are five Internet service providers⁴ (ISPs) in the country, including two mobile phone operators (Togocom and Atlantic Telecom). Due to network coverage gaps, there is a large gap between the quality of connectivity in urban areas and rural areas. According to GSMA, the penetration rate for mobile broadband is 36%.⁵



1.71 Million
Internet users in Togo

1. It should be noted that the poverty has decreased from 61,7% to 53,5% between 2006 et 2017.

2. <https://www.banquemondiale.org/fr/country/togo/overview>

3. <https://datareportal.com/reports/digital-2020-togo>

4. Il s'agit de Café Informatique, Togocom, Teolis, GVA Togo (Groupe Vivendi Africa) et Atlantic Telecom Togo

5. <https://www.mobileconnectivityindex.com/#year=2019&zonesocode=TGO&analysisView=TGO>

The cost of internet connectivity, considered to be among the highest in the West African sub-region, is generally the subject of challenges by users and has been the subject of boycotts, organised by consumers, of internet services. For example, for Togocom mobile phone subscribers, the cost of 2 GB with a validity of 30 days is FCFA 5,000 (approximately USD 9.02). It is important to note that on November 16 2020 the Regulatory Authority for Electronic Communications and Posts (ARCEP) put the two mobile telephone operators on notice for their excessively high communication costs which could bode well for the cost of connectivity.⁶

Apart from the high costs associated with internet use, users are dissatisfied with the period of validity allocated to the consumption of mobile data. In the market, competition is relatively low and Internet services are not very varied from one provider to another. The bipolarization of the mobile phone market has an impact on the cost and variety of services, compared to the countries of the Francophone West African sub-region. For example, some fibre optic subscribers complain, not only about the quality of the internet, but also about the quality of the supply and the technical support that is generally only operational during hours of service.

DIGITAL RIGHTS AND THE HUMAN RIGHTS APPROACH

In Togo, digital rights still remain a new reality and the concept is not necessarily assimilated to that of human rights in general. There is a huge lack of knowledge by citizens of their rights. Moreover, the education system does not promote the acquisition of basic technological skills, which means that the population as a whole seems to ignore its digital rights. Even if in recent years there has been a strong interest on the part of the legislator on digital issues. The displayed interest does not seem to be that of protecting the citizen, but rather to adapt the policies of the State to the global digital framework. It is evident that the important prerogatives of the State lead it to take decisions on data protection which are often not popular.



6. L'ARCEP met en demeure Togocel et Moov pour pratiques de différenciation tarifaire, <https://www.republiquetogolaise.com/telecoms/1611-4849-l-arcep-met-en-demeure-togocel-et-moov-pour-pratiques-de-differenciation-tarifaire>

The news from Togo remains marked by the internet shutdowns that occurred on the evening of Election Day (February 22 2020) that had significant economic consequences.⁷ According to a study by the Open Observatory Network Interference (OONI), Togo cut off access to some internet services during the elections.⁸ The results of the tests conducted during the election period showed that instant messaging applications such as WhatsApp, Facebook Messenger and Telegram were blocked for the two mobile phone operators: Togocom and Atlantique Telecom (widely used by citizens for their internet access) while the three apps were accessible on the Canalbox network of Vivendi Africa Togo Group, one of the three fixed-mode internet service providers, showing that the blocking varied according to the modes of internet access.

It is very likely that this approach reflects the fact that the intention of the authorities in shutting down the internet was to drastically reduce access for the segment of the population believed to be most sensitive to political protest, young people, without running the risk of completely cutting the country from the internet. In 2020, however, the Togolese state was condemned by the ECOWAS Court of Justice for the widespread cuts that occurred in 2017 in the context of political demonstrations.⁹ On the issue of digital rights, initiatives are being taken within civil society. A bill sponsored by an organization, Afrotribune, aims to promote digital rights and freedoms. In 2020, the eighth edition of the Internet Governance Forum was organized and focused on the accessibility and cost of internet connectivity.¹⁰

Organized every year, this forum opens the debate on government sector policy and is attended by all internet stakeholders. Most recently, news has been marked by allegations of cyber-espionage of political and religious leaders by the State.¹¹ The government is yet to take a position on the issue.

INTERNET LEGAL FRAMEWORK

The legal framework of the internet is gradually taking shape in Togo. Over the past two years, there has been a strong interest in digital activities among legislators. In 2018, the Togolese Parliament passed a law on cybersecurity and against cybercrime. A year later, the Personal Data Act came into being. This is the law, dated October 29 2019, on the protection of personal data. These laws regulate the freedoms of citizens online and repress cyber-reprehensible acts such as hate speech, the promotion of child pornography, the dissemination of fake news (infox), attacks on human dignity, etc.

The legal framework for biometric identification data was set by the recent law on the identification of natural persons in Togo (e-ID Togo),¹² voted by MEPs on September 3 2020. This law promises mechanisms to regulate the management of citizens' biometric data; it is therefore the second law that regulates personal data.

According to a study by the Open Observatory Network Interference, Togo cut off access to some internet services during the elections



7. <https://jurigeek.law.blog/2020/09/13/pourquoi-coupe-t-on-internet/>

8. OONI uses a free program to detect censor, surveillance and manipulation of the traffic on internet

9. <https://www.agenceecofin.com/gestion-publique/0107-78064-le-togo-condamne-par-la-cour-de-justice-de-la-cedeao-pour-les-coupures-dinternet-de-2017>

10. <https://www.techenafrique.com/2020/10/togo-le-forum-national-sur-la-gouvernance-internet-cest-du-15-au-16-octobre/>

11. How did Togo use the Israeli program Pegasus to spy on religious catholics and opponents, https://www.lemonde.fr/afrique/article/2020/08/03/au-togo-un-espion-dans-les-smartphones_6048023_3212.html

12. The Togo e-ID project is supported by the World Bank through the West Africa Unique Identification for Regional Integration and Inclusion (WURI) program. This program aims to provide government-recognized unique identification credentials to all individuals in participating countries, regardless of their nationality, legal status or place of residence. The program involves Côte d'Ivoire, Guinea, Benin, Burkina Faso, Niger and Togo.



“

On the issue of digital rights, initiatives are being taken within civil society. A bill sponsored by an organization, Afrotribune, aims to promote digital rights and freedoms.

It should be noted that the drafting of laws and policies is not the subject of much communication in order to allow citizens to take a position and to take possession of the contents of the various laws. Togo signed the African Union Convention on Cybersecurity and Protection of Personal Data¹³ (Malabo Convention) on April 2 2019 without ratifying it to date.

At the sub-regional level, in the ECOWAS legal ecosystem, there is the Additional Act A/SA.1/01/10 on the protection of personal data, of which Togo is a party. It should be noted that Togolese laws still comply with the legal framework of international commitments.

IMPACT OF COVID-19 ON DIGITAL RIGHTS AND INCLUSION

On the issue of COVID-19, starting March 2020, the actions that had to be taken by the State led to the serious consideration of the Internet as a new option for governance and crisis management. A few key points can be observed, including the government's inauguration of a digital financial assistance program for those hard hit by the pandemic. This program, called Novissi, made it clear that a comprehensive and more inclusive identification program of the population would avoid inequalities in a context where the use of electoral data led to the exclusion of abstentionists.¹⁴

13. <https://www.internetsociety.tg/internet-et-securite-des-donnees-a-caractere-personnel-queles-solutions-pour-lafrique/>

14. The government preferred to rely on the electoral database, which was considered more inclusive and complete than the identity card database, even though there were a significant number of abstainers in protest at the way the electoral census was organized.

In addition, the pandemic highlighted the low digital literacy of citizens in rural areas. The elderly and the less educated seem to be left out. In addition, the increased use of the internet during the pandemic for professional activities has given a new light to the question of the cost of telephone communication and Internet access.

Moreover, this led to the public taking interest in the security of data that was used to track travellers.¹⁵ It should be noted that the freedom of expression online that seemed to be significantly improved¹⁶ due to capacity (especially for

journalists) to express themselves on any topic on social media without being worried, unless publishing false information, is experiencing a regression with recent internet cuts¹⁷ and the difficulty for some online media to broadcast freely without risking disruption of their services.

Because of its strong links to violent extremism, fake news is subject to greater surveillance on social media, both at the security force and citizen level. Initiatives (such as Togocheck)¹⁸ are being implemented to materialize citizen watch.

CONCLUSION AND RECOMMENDATIONS



It should be noted that every year, significant progress is being made on issues surrounding the Internet, but much remains to be done. Internet governance has become one of the reflections of the level of democracy and good governance.

For the promotion of internet rights in Togo, it is important that:

- Efforts are made in terms of accessibility, cost and connectivity, but also quality and coverage of the network;
- Internet service providers should be encouraged to place the interests of internet users at the heart of their concerns by offering quality services and by paying attention at all times to their feedback (complaints or suggestions for improvements);
- Citizens should be encouraged to know their digital rights and the government must stop considering the Internet as a means of sanctioning people's expression. In this context, the adoption of a law on digital rights and freedoms would be appropriate;
- Finally, a more open governance of the Internet, including all stakeholders, still needs to be strengthened.

15. For example, the TogoSafe application is mandatorily downloaded by travelers landing at the Gnassingbé Eyadema International Airport and is monitored to ensure compliance with the mandatory quarantine.

16. It should be noted, however, that the 2020 World Press Freedom Index by Reporter Without Borders ranked Togo 71st out of 181 countries. The country had occupied the 76th place in 2019. It was reported that on the day the presidential election results were declared, the Supreme Court of Justice ordered the blocking of the opposition coalition's websites, <https://rsf.org/fr/ranking/2019#>

17. AD216: La liberté d'expression au Togo serait-elle mise en quarantaine en période de crise?

<http://afrobarometer.org/fr/publications/ad216-la-liberte-dexpression-au-togo-serait-elle-mise-en-quarantaine-en-periode-de>

18. <https://www.togocheck.com/>



Case Study: Togo Safe application's data grab

Compiled by Seyram Adiakpo

The TogoSafe application was conceived by the Togolese Ministry of Posts and Digital Economy in the context of COVID-19, to track and follow travelers in-country. The app was compulsory for all travellers arriving in Togo. Besides the compulsory downloading of the application, the traveler is required to sign up to the corresponding government website. However, due to several factors, the application presents issues relating to digital rights and freedoms' violations.

On the question of data, the general conditions for utilization remain silent. It is only said that the application is designed to “monitor the user’s movements but not expose their private life”. This brief affirmation is made with no clarification on the way the user’s private life will be protected and the users’ data will be kept from any other use than that mentioned above.

Furthermore, the user has no idea of the exact data collected. The user is only ordered to keep the Bluetooth and GPS services on their devices activated. The user is forced to agree to share their data without knowing which data is being shared, otherwise, they are placed in quarantine within the monitoring structures set up by the State at their own expense.

The government site reads, “People in lockdown must respect the strict rules while keeping the TOGOSafe application activated while awaiting results of the COVID-19 PCR test.” They have to abide by such unexpected control by security agents and health workers at their place of lockdown.

In addition, the application is available on app platforms such as Google Play, App Store and the App Gallery. On the app’s website, it notes that data is not shared with third parties without the third parties being defined. “The state now voluntarily or forcefully offers personal data to these companies,” regrets Anoumou (name changed), a Togolese citizen residing in the United States, whom when passing through Togo was forced to download the app before entering the country.

Four other people contacted as part of the study said they had no choice but to accept. Users are not informed about whether they can access the data collected, oppose it or have it modified or deleted unless they go to the



website of the application, which not everyone has the instinct to do. Users who download the application do not have enough information on the general conditions of use.

In Togo, Law No. 2019-14 of October 29 2019 details the principles relating to the protection of personal data. Under this law, provision is made for the creation of a Personal Data Protection Authority (IPDCP). It also states the existence of the Independent Administrative Authority (AAI) which is responsible for ensuring that the processing of personal data is carried out in accordance with the provisions set out in the law. If the legal framework that protects personal data is absent, it becomes difficult for the traveller to have an open dialogue, resulting in difficulties in having their data modified or erased. They will have to engage the developers of the application, which might result in a lack of transparency.

On the issue of transparency, the management of the TogoSafe app is not open-sourced even though open data would give civil society and academia the opportunity to assess the application. A human rights-based approach has not been taken into account in the management of the TogoSafe application. When it comes to digital rights, the human rights-based approach mainly concerns the legal framework put in place by the State, but also its attitude towards citizens. The human rights-based approach includes the following principles: participation, accountability, non-discrimination and equality, empowerment and legality.

In addition, the application challenges medical confidentiality. The medical data of people who test positive for COVID-19 is shared with the entity that manages the application. This sensitive data is made available to the entity. The purpose of the application must be clearly defined.

The State should make users more aware of the risks of using the application without having to find them on their own. Users should be free to opt out of using an application such as TogoSafe. In addition, the application must be brought into compliance with Law No. 2019-14 on the protection of personal data. All technical choices should be documented and explained by the responsible parties. The technical operation of the application should be completely transparent so that users feel responsible for their choice of whether or not to use the application. Finally, the application protocol and its implementation should be documented, public, and independently audited.



Tunisia is a North African country with a population of 11.7 million.¹ After the ousting of a long time dictatorship regime, Tunisia began a transition to democracy in 2011.

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN TUNISIA

For the past decade, the country has been undertaking ongoing reforms. However, the history of censorship and the slow pace in reforming the legal framework, as well as economic struggles, have challenged the state of freedoms and respect of digital rights.

INTERNET ACCESS

The number of internet subscriptions reached 83.7 per 100 habitants in 2020.² There were 1,318,103 fixed-broadband subscriptions as of August 2020, including around 917,837 wired, 400,205 radio, and 61 satellites.³ The international bandwidth capacity increased from 430 Gbps in 2018 to 810 Gbps in June 2020. As of August 2020, there were over 9 million mobile data subscriptions in the country, consisting of about 405,501 subscriptions to 3G/4G USB keys and 121,005 machine-to-machine communication (M2M) subscriptions, with mobile plans accounting for the remainder.⁴



83.7%

**per 100 habitants
of internet subscriptions**

1. The World Bank, "Tunisia," March 23, 2021, <https://data.worldbank.org/country/tunisia>

2. Ministry of communication technologies and digital economy, "Nombre d'abonnements au réseau Internet /100 habitants", <https://www.mtcen.gov.tn/index.php?id=334&L=656>

3. Instance Nationale des Télécommunications, "Suivis des principaux indicateurs du marché de la data fixe en Tunisie [Monitoring of main indicators regarding the fixed data market]," August 2020, http://www.intt.tn/upload/files/TB3_Data-Fixe%20-08_2020.pdf

4. Instance Nationale des Télécommunications, "Suivis des principaux indicateurs du marché de la data mobile en Tunisie [Monitoring of main indicators regarding the mobile data market]," August 2020, http://www.intt.tn/upload/files/TB4_Data-Mobile%20-08_2020.pdf

For the purpose of providing network coverage in areas with a low population density, the Ministry of Technology, Information and Digital Transformation, after a national call for tender, has contracted the operator Tunisie Telecom for the implementation of broadband coverage in these areas. The project's implementation reached 90% at the start of 2020. It is expected to cover over 47 delegations in 15 governorates and benefit 164 schools, 59 basic health centers and 180,000 inhabitants.⁵

IMPACT OF COVID-19 REGULATIONS ON DIGITAL RIGHTS AND INCLUSION

The COVID-19 pandemic has had an impact on the telecommunications sector in Tunisia. This impact translates into a change in consumer behavior. Tunisia, like most countries in the world, confined its population during the period of the second quarter of 2020. Internet consumption soared as soon as the general health lockdown was announced in March 2020.⁶ According to statistics for the second quarter of 2020 provided by the Tunisian National Telecommunication Authority, the average daily consumption in ADSL, LTE TDD and mobile data offers on smartphones per subscriber is respectively 5.8 GB, 4.5 GB and 521 MB, up 22.7%, 114.93% and 67.5% compared to the second quarter of 2019.⁷ This could be in part explained by employees shifting to working from home, students studying online, and the rise of e-commerce.

In response to the growing connectivity needs and the additional traffic demand in densely populated areas during the quarantine period, telecommunications operators and internet service providers have deployed new resources and offered special plans to increase their bandwidth capacity and avoid an internet blackout risk.⁸

Students were granted free access to educational platforms.⁹ However, in contrast to universities, public schools did not provide online platforms for pupils to pursue their education and take their exams. The Ministry of Education instead broadcast courses on national television. The possibility of nationwide online education in schools could not be fulfilled for many reasons, including the digital divide between households and regions.

A number of initiatives, resulting from joint efforts between the government, civil society organizations and the private sector have been launched since the start of the pandemic in order to bridge the digital divide and provide children from low-income families with laptops and an internet connection. Other initiatives have focused on building resources to update citizens on the spread of the virus, in an effort to ensure citizens' right to access information. For instance, covid-19.tn, an accessible online portal, provides the latest updates and informs citizens about the COVID-19 symptoms.¹⁰ For reference, in March 2016, Tunisia adopted a basic law on the right to access information. The law guarantees access to

5. Ministry of communication technologies and digital economy, "Core list of ICT indicators Country: Tunisia Core indicators on access to, and use of, ICT by households and individuals," June 2020,

https://www.mtcen.gov.tn/index.php?id=119&L=hcdqjoicun&tx_ttnews%5Btt_news%5D=4049&cHash=11d45942db63b2d23cb217987770dd1b

6. Tunisian Press Agency, Le confinement à domicile pendant 14 jours est obligatoire pour tous les arrivants en Tunisie sans exception (Chokri Hamouda), March 13, 2020, <https://www.tap.info.tn/fr/Portail-Soci%C3%A9t%C3%A9/12435492-le-confinement-%C3%A0>

7. Instance Nationale des Télécommunications, "Carnet Trimestriel", August 2020,

[http://www.intt.tn/upload/files/Carnet%20trimestriel%20de%20la%20consommation%20TR2-2020\(3\).pdf](http://www.intt.tn/upload/files/Carnet%20trimestriel%20de%20la%20consommation%20TR2-2020(3).pdf)

8. 'COVID-19 : les opérateurs téléphoniques volent au secours du ministère tunisien de la Santé', <https://thd.tn/covid-19-les-operateurs-telephoniques-volent-au-secours-du-ministere-tunisien-de-la-sante/>

9. 'Arab League launches e-learning site to combat disruption', <https://www.universityworldnews.com/post.php?story=20200318110141904>

10. <https://covid-19.tn>

information held by government bodies including ministries, the presidency, publicly funded NGOs, the parliament, local municipalities, the central bank and constitutional bodies.

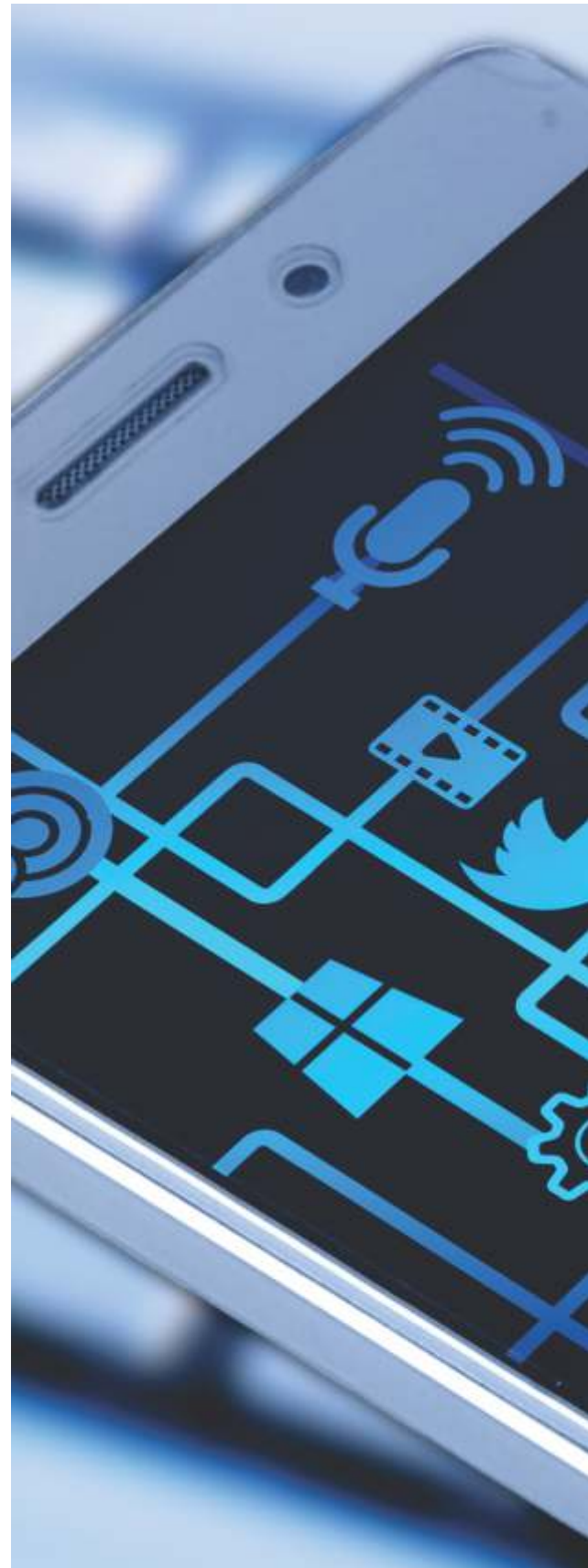
PRIVACY AND SURVEILLANCE

The Ministry of Health launched a free and anonymous online survey aiming to optimize the care of patients by the emergency services by letting users answer 12 quick and easy questions.¹¹ The results were expected to help identify locations requiring intervention, in particular in terms of screening tests.

On a more controversial note, in June 2020, the Prime Minister also confirmed the government was tracking citizens' movements anonymously through their SIM cards.¹² The Ministry of Communication and Digital Economy released a statement to clarify that the tracking relied on general data from mobile phones between regions and respected legal requirements for personal data protection, and that the Ministry was in consultation with the National Authority for the Protection of Personal Data (NAPPD). NAPPD released a statement confirming that it had advised the government regarding the deployment of a number of tracking applications. So long as individuals' anonymity is ensured, the program does not violate the legal provisions related to the protection of personal data.¹³

Later on, the Ministry of Health announced the adoption of E7mi,¹⁴ a contact-tracing mobile application that collects users' phone numbers and uses Bluetooth signals and location data to detect and alert users who may have had contact with someone infected with the COVID-19 virus. The download of this mobile application was at no stage mandatory.

However, Access Now, a digital rights organization, stated that even though the National Authority for the Protection of Personal Data confirmed that the application complies with



11. Stop Corona Testez vous, accessed November 2020, <https://covid-19.tn/fr/blog/stop-corona-testez-vous-et-participez-a-la-lutte-contre-le-coronavirus/>

12. Mosaïque FM, "We monitored the respect of health quarantine through Tunisians' phones," June 14, 2020, <https://www.mosaïquefm.net/ar/-/تونس-أخبار-755657/القفحاح-أقينا-إحترام-الحجر-الصحي-عبر-هواتف-التونسيين>

13. Tunisiatv, "Clarification regarding the government's use of an application that monitors citizen movements", June 15, 2020, <http://news.tunisiatv.tn/-/توضيح-8F4c1KjFi#بخصوص-استخدام-الحكومة-لتطبيق-تتبع-تحركات-المواطنين/2020/06/مجمع>

14. 'Tunisia launches virus-tracking app', <https://medicalxpress.com/news/2020-05-tunisia-virus-tracking-app.html>



“

The Ministry of Health launched a free and anonymous online survey aiming to optimize the care of patients by the emergency services by letting users answer quick and easy questions.

Tunisia’s 2004 Data Protection Law, the law “is outdated and does not account for technologies developed since it was written.”¹⁵

The current Data Protection Law is not the only legal text criticized by the digital rights community. The 2014 Constitution that was approved following the 2011 revolution was highly praised for guaranteeing the right to privacy and personal data protection; the right to access information and communication networks; and the right to free expression and freedom of the press.

However, the text contains vague language tasking the state with “protecting the sacred”, which could act as a constitutional restriction on internet freedom.¹⁶

ONLINE FREEDOM OF SPEECH

Legal texts that have been criticized for restricting freedoms remain dangerous in the absence of a constitutional court. So far, two Parliaments have failed in establishing the mandated Constitutional Court to which the defendants can appeal when they face prosecutions under unconstitutional laws.

For instance, Article 86 of the Telecommunications Code states that anyone found guilty of “using public communication networks to insult or disturb others” could spend up to two years in prison and may be fined up to 1000 dinars.¹⁷ Based on that article and others in the Tunisian Penal Code,¹⁸ in November 2020, Wajdi Mahouachi, a blogger, was

15. Access Now, “COVID-19 contact-tracing apps in MENA: a privacy nightmare”, June 18, 2020, <https://www.accessnow.org/covid-19-contact-tracing-apps-in-mena-a-privacy-nightmare/>

16. Constitute Project, “Tunisia’s Constitution of 2014,” August 13, 2019, Translation by UNDP, https://www.constituteproject.org/constitution/Tunisia_2014.pdf

17. Tunisian Telecommunication Code, http://www.legislation.tn/fr/affich-code/Code-des-T%C3%A9l%C3%A9communications__116

18. Tunisian Penal Code, <http://www.legislation.tn/sites/default/files/codes/Peal.pdf>

sentenced to two years in prison by the Tunis First Instance Court for posting a video on Facebook that denounced a Tunis public prosecutor's failure to arrest and open an investigation against an extremist preacher.¹⁹

Between April and May 2020, bloggers Hajer Awadi and Anis Mabrouki were arrested and charged with offences including “insulting a civil servant” and “causing noises and disturbances to the public” under Articles 125 and 316, respectively, of the Penal code. They had both posted videos on Facebook criticizing government corruption and its poor handling of aspects of the health crisis. Mabrouki was acquitted, but Awada and her uncle were both sentenced to a 75-day suspended prison sentence.²⁰

In July 2020, the Court of First Instance in Tunis convicted another blogger of “inciting hatred between religions through hostile means or violence” under Articles 52 and 53 of the Tunisian Press Code, for sharing a Facebook post of a text that imitates verses from the Quran to make fun of

the COVID-19 situation. She was sentenced to six months in jail and ordered to pay a \$700 fine for the post.²¹

Human rights organizations, including Amnesty international and Human Rights Watch, have raised the alarm about these recurring arrests that may lead to more oppression and self-censorship.

MISINFORMATION LAWS

At the start of the coronavirus pandemic in the spring of 2020, a draft law to combat disinformation that had been proposed by a member of Parliament faced a backlash, resulting in its withdrawal one day later. The bill sought to criminalise the “disclosure of any false or questionable speech among users of communication networks and social media platforms, which may be insulting to individuals, groups or institutions.” According to civil society groups, it was seen as a direct threat to freedom of expression and, since it employs vague language, it could be used to silence online activists.²²

CONCLUSION AND RECOMMENDATIONS



The findings presented in this report confirm the ongoing challenges Tunisia faces in ensuring the protection of digital rights. As 2020 marks the tenth anniversary of the uprising that toppled the 23-year-rule of an autocratic president, the Tunisian digital space presents an arena for citizens to express opinions about politics and society and to hold governments accountable. Therefore, it is essential to make further progress in reforming the legal framework as well as deploying more efforts to minimize the digital divide for an open inclusive internet in Tunisia.

19. Human Rights Watch, “Tunisia: Harsh Sentence Against Blogger”, November 24, 2020, <https://www.hrw.org/news/2020/11/24/tunisia-harsh-sentence-against-blogger>

20. Amnesty International, “Criminal Prosecutions of Online Speech”, <https://www.justice.gov/eoir/page/file/1335186/download>

21. Amnesty International, “Tunisia: Blogger Emna Chargui sentenced to six months in prison for social media post”, July 15, 2020, <https://www.amnesty.org/en/latest/news/2020/07/tunisia-blogger-emna-chargui-sentenced-to-six-months-in-prison-for-social-media-post/>

22. Accessnow, “Tunisia’s Parliament on COVID-19: an initiative to fight disinformation or an opportunity to violate fundamental rights?”, April 1, 2020, <https://www.accessnow.org/tunisias-parliament-on-covid-19-an-initiative-to-fight-disinformation-or-an-opportunity-to-violate-fundamental-rights/>



Uganda is a country in east-central Africa with a population of around 46 million. It became an independent country in 1962. Its governmental system is multi-party democracy, and both English and Swahili are official languages.¹

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN UGANDA

The latest figures from the communications regulator, Uganda Communications Commission (UCC), show there were 16.9 million internet subscribers by the end of December 2019, while mobile subscriptions stood at 26.7 million in December 2019.² Despite these impressive figures, a majority of the population remains unconnected, due to high costs and poor infrastructure, including lack of electricity supply, especially in the rural areas. The lack of connection has also been made worse as a sizable number of people who were accessing the internet at their places of work can no longer do so due to the COVID-19 restrictions and closure of workplaces.³

The legal regime governing the digital sphere in Uganda includes the Uganda Communications Act 2013, Anti-Pornography Act 2014, Regulation of Interception of Communications Act 2010, Registration of Person Act 2015, the National Information Technology Authority, Uganda Act (Act No. 4 of 2009) and the Electronic Signatures Act 2011 (Act No. 7 of 2011).

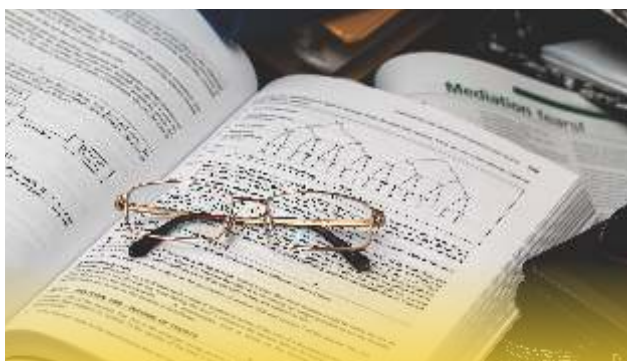


16.9 Million
*Internet subscribers
in December 2019*

1. Britannica, 'Uganda', <https://www.britannica.com/place/Uganda>

2. Daily Monitor, 'Internet subscribers rise to 16.9 million', <https://www.monitor.co.ug/uganda/business/technology/internet-subscribers-rise-to-16-9-million-ucc-report-1892924>

3. Unwanted Witness, 'Internet barriers constrain the work of Uganda HRDs amidst COVID-19 pandemic', <https://www.unwantedwitness.org/internet-barriers-constrain-the-work-of-uganda-hrds-amidst-covid-19-pandemic/>



MONITORING AND TAXATION OF THE MEDIA

On May 30th, 2018, the Parliament of Uganda passed the Excise Duty Amendment Act which ordered users of social media to pay Shs. 200 (\$0.05) each day to access it.⁴ The failure to suspend the implementation of the OTT tax has continued to undermine the efforts to increase access to and affordability of ICTs by a large majority, thus denying a large population access to critical information and citizen participation in democratic processes. Similarly, a 0.5% levy (originally 1%) imposed on all mobile money transactions under the same law continues to lock many out of the digital economy.⁵

In September 2020, UCC ordered all news websites and online broadcasters to register their services by 5 October, 2020. The targeted services are blogs, online television, online radio, online newspapers, internet-based radio and TV stations, streaming radio and TV providers, and video-on-demand providers.⁶

It was not a new regulation but rather the enforcement of a directive issued in March 2018 that punished non-compliance with the risk of being blocked by internet service providers.⁷

One controversial guideline requires providers to ensure “content uniformity” between online and any print or offline versions.⁸ The requirement is ambiguous and stifles the creativity and flexibility of online platforms. At least 48 online data communication and broadcast service providers had registered with the UCC by the end of September. There are fears that these regulations are intended to give the regulator more control over online content producers and policing them. The guidelines further impose an application fee for an annual authorization of UGX 100,000 (approximately USD 27), regardless of size or revenue.⁹

The refusal by the government to suspend the implementation of the Over-The-Top (OTT) tax, despite several appeals from different stakeholders, has continued to undermine the efforts to increase access to and affordability of ICT for a large proportion of the population, thus denying them access to critical information disseminated on social media platforms.¹⁰

***The Parliament of Uganda passed the
Excise Duty Amendment Act which
ordered users of social media to pay
Shs. 200 (\$0.05) each day to access it.***

4. Leadership, 'MPs okay taxes on social media', May 31, 2018,

<https://webcache.googleusercontent.com/search?q=cache:u3ydH5b36F0J:https://leadershipmagazine.org/%3Fp%3D15816+&cd=1&hl=en&ct=clnk&gl=uk>

5. New Vision, 'Mobile money tax reduced to 0.5%', <https://www.newvision.co.ug/news/1486921/mobile-money-tax-reduced-05>

6. Acme, 'UCC's latest directive on online content producer registration arrives with a shadow', <https://acme-ug.org/2020/09/09/op-ed-uccs-latest-directive-on-online-content-producer-registration-arrives-with-a-shadow>

7. Public notice: Registration of online data communication and Broadcast service providers, http://www.ucc.co.ug/wp-content/uploads/2018/03/UCC_ONLINE-DATA-COMMUNICATIONS-SERVICES.pdf

8. Acme, 'UCC's latest directive on online content producer registration arrives with a shadow', <https://acme-ug.org/2020/09/09/op-ed-uccs-latest-directive-on-online-content-producer-registration-arrives-with-a-shadow>

9. Acme, 'UCC's latest directive on online content producer registration arrives with a shadow', <https://acme-ug.org/2020/09/09/op-ed-uccs-latest-directive-on-online-content-producer-registration-arrives-with-a-shadow/>

10. State of Internet Freedom in Africa 2020: Resetting Digital Rights Amidst The COVID-19 Fallout, https://cipesa.org/?wpfb_dl=361 (accessed on 1/12/2020)

COVID-19 AND THE DIGITAL SPACE

The digital space, like everything else, has in 2020 been eclipsed by the COVID-19 pandemic. As of 16 December 2020, Uganda had registered 28,168 cases with 10,005 recoveries and 225 deaths.¹¹

Following the confirmation of the first case of COVID-19 in Uganda on 22 March 2020 the government of Uganda issued a raft of measures to stem infections.¹² They included closing of institutions of learning and places of worship, suspending public gatherings, banning public transport, partially closing markets, a dusk-to-dawn curfew, mandatory wearing of face masks, and closure of the country's borders and international airport to passenger traffic.

The measures, while well intentioned, have infringed the principles that protect digital rights namely: internet access and affordability; freedom of expression and right to information; privacy and data protection; and marginalized groups and groups at risk.

Some private players, such as telecom giants MTN Uganda and Airtel Uganda, rolled out packages to mitigate access to online services,¹³ 'work from home' data bundles, zero-rating information from the Ministry of Health website, and free text messaging services to keep the public online.¹⁴ The two companies also offered free mobile money service transactions as a way of minimizing the

physical exchange of paper money to prevent COVID-19 infections. However, these offers were for a very limited time, as the charges were reinstated on 26 May 2020.¹⁵

COVID-19 AND EDUCATION

A key challenge arising out of the lockdown was the continuation of learning for students. The Ministry of Education introduced distance learning for primary and secondary level through radio and television, as well as providing self-study materials to parents. There has, however, been a lack of clarity with regard to e-learning.

A request by Uganda Christian University to conduct online examinations was rejected first by the Ministry and then by Parliament, even after the university authorities showed evidence that the students had been prepared to do the exams online, even before the lockdown.¹⁶

A similar request by the Law Development Centre to conduct online examinations was also blocked by the Ministry of Education and Sports.¹⁷ In July, the government ordered schools to stop conducting their own online teaching and charging parents fees for the service "because both actions are irregular".¹⁸ The directive, however, did not affect international schools which do not follow the national curriculum.

11. <https://www.worldometers.info/coronavirus/country/uganda/> (accessed 16 December 2020)

12. New Vision, 'COVID-19: Uganda entering more dangerous phase – Museveni', <https://www.newvision.co.ug/news/1521333/covid-19-uganda-entering-dangerous-phase-museveni>, New Vision, 'Uganda confirms coronavirus', <https://www.newvision.co.ug/news/1516875/uganda-confirms-coronavirus>

13. https://twitter.com/Airtel_Ug/status/1242050107727654912?s=20

14. Dignited, 'COVID-19: MTN Uganda Introduces Work From Home Data Bundle', <https://www.dignited.com/59266/mtn-work-from-home-data-bundles-uganda>

15. NilePost, 'Airtel, MTN reinstate charges on sending mobile money', Airtel, MTN reinstate charges on sending mobile money - Nile Post

16. Chimp Reports, 'UCU complies with government, suspends online Easter semester exams', <https://chimpreports.com/ucu-complies-with-govt-suspends-online-easter-semester-exams>

17. The Independent, 'Ministry of Education suspends LDC's online classes', <https://www.independent.co.ug/ministry-of-education-suspends-lDCs-online-classes>

18. Daily Monitor, 'Stop charge for online lessons, govt tells schools', <https://www.monitor.co.ug/uganda/news/national/stop-charge-for-online-lessons-govt-tells-schools-1896058>

FREEDOM OF SPEECH IN 2020

As early as February 2020, the Ministry of Health moved to dispel rumours of reported confirmed cases of COVID-19, even before one was confirmed in Uganda. In response to this and other incidents of misinformation, the Uganda Communications Commission (UCC) issued an advisory warning to the public against spreading COVID-19 related false information. UCC warned that suspects would be prosecuted for offending the Computer Misuse Act 2011, the Data Protection and Privacy Act 2019 and Section 171 of the Penal Code Act Cap 120.¹⁹

In March 2020, UCC wrote to three media houses, NTV, Spark TV, and BBS TV, demanding that they provide a reason why regulatory sanctions should not be taken against them. The three were accused of broadcasting content that had the potential “to confuse, divert and mislead unsuspecting members of the public against complying with the guidelines issued by the relevant Government authorities on the COVID-19.”²⁰

In April, a prominent church leader, Pastor Augustine Yiga of Revival Church Kawaala, and Adam Obec who worked with Kampala Capital City Authority, were arrested and charged. Obec was accused of circulating information on social media claiming that Uganda had recorded its first COVID-19 death in Koboko district, an act that, it was claimed, triggered fear and panic among the general public and inhibited Uganda’s efforts to combat the coronavirus.²¹ Pastor Augustine Yiga was charged with uttering false information and spreading harmful propaganda in relation to COVID-19.²²

In October, UCC revealed that they had installed a fact checker facility on their website for any member of the public who wants to verify information about anything before sharing it. They also warned that under the Computer Misuse Act 2011, once you forward anything using your phone, you legally become an author and creator of that content and liable to prosecution.²³



19. Uganda Communications Commission Blog, 'Public advisory notice on circulation of fake information', <https://uccinfo.blog/2020/03/22/public-advisory-notice-on-circulation-of-fake-information/>

20. UCC calls out 3 TV stations on COVID-19; <https://uccinfo.blog/2020/03/29/ucc-calls-out-3-tv-stations-on-covid-19>

21. PML Daily, 'KCCA staff arrested over spreading fake news on coronavirus', <https://www.pmldaily.com/news/2020/04/covid-19-crisis-kcca-staff-arrested-over-spreading-fake-news-on-coronavirus.html>

22. New Vision, 'Pastor Yiga could spend seven years in prison', <https://www.newvision.co.ug/news/1517283/pastor-yiga-spend-seven-prison>

23. <https://www.newvision.co.ug/news/1528471/ugandans-spreading-fake-news-prosecuted-ucc>, (accessed on 1/12/2020)



UCC revealed that they had installed a fact checker facility on their website for any member of the public who wants to verify information about anything before sharing it.

COVID-19, PRIVACY AND DATA PROTECTION

As one of the measures to combat COVID-19, the government passed several statutory instruments that would aid in the identification, isolation, and containment of the spread of COVID-19 in the country. These included the Public Health (Control of COVID-19) Rules, 2020 under the Public Health Act Cap.281, which gave powers to a medical officer or a health inspector to enter any premises in order to search for any cases of COVID-19 or inquire whether there are, or have been, any cases of COVID-19 on the premises.²⁴ Additionally, section 5 of the rules empowers the medical officer to identify and order the quarantine or isolation of all contacts of suspected COVID-19 patients.

However, as the number of cases rose and the government redoubled its efforts to reach out to ensure testing of people returning from coronavirus hotspots abroad, there were reports of Ugandans using online platforms, mainly Facebook and WhatsApp, to share personal contact details of the suspected returnees, with threats of further

exposure should they fail to report for testing.²⁵

The Ministry of Health was reported to have been in possession of the details of all passengers who had entered the country in the second and third week of March, which details the ministry was using to trace them. In Jinja, a couple was forced to seek protection from the district authorities after the community where they were living threatened to evict them from their home where they were self-isolating.²⁶

Although the measures taken by the Ministry to trace all the returnees from places like Dubai, and their contacts, were well-intentioned, as were efforts by vigilant citizens to call out the returnees to voluntarily avail themselves for testing, the situation resulted in the unintentional exposure of individual personal details that put them at risk, contrary to the Privacy and Data Protection Act 2019.

24. Section 6(1) of the Public Health (Control of COVID-19) Rules of 2020, <https://ulii.org/ug/legislation/statutory-instrument/2020/52>

25. Daily Monitor, 'Coronavirus: Uganda hunts', <https://www.monitor.co.ug/uganda/news/national/coronavirus-uganda-hunts-500-dubai-returnees-1882602>

26. Daily Monitor, 'COVID-19: Dubai returnee, wife quarantined at Jinja Hospital after residents threaten with eviction', <https://www.monitor.co.ug/uganda/news/national/covid-19-dubai-returnee-wife-quarantined-at-jinja-hospital-after-residents-threaten-with-eviction-1882196>

DIGITAL EXCLUSION

Even before the COVID-19 pandemic, women, persons with disabilities, the elderly and those in rural communities were already facing digital exclusion and the resultant violations of their information rights.²⁷ The exclusion has been exacerbated by the COVID-19 pandemic and has manifested in keeping the marginalized out of e-learning, remote working, and access to information. Many women and people with disabilities in Uganda remain offline due to the high cost of gadgets, a social media tax, poor connectivity, the high cost of data, and poor digital skills.²⁸

A report by Women of Uganda Network (WOUGNET), notes that even the few women that make it on to the internet have become victims of a new form of gender-based violence commonly referred to as “technology-assisted violence against women and girls”. A WOUGNET survey indicates that in the three months of March, April and May 2020, 50% of women had either faced tech-assisted violence, or heard of an incident either from a friend or through social media, radio or TV, while others were not sure.²⁹

CONCLUSION AND RECOMMENDATIONS



There are already barriers to the digital realm in Uganda, both due to high prices and to monitoring and control of the media. The COVID-19 crisis threatens to make the situation worse, as well as increase the digital divide facing women and minorities. The following recommendations are aimed at preventing this scenario:

- The government should establish mechanisms to stem misinformation and disinformation. This is best achieved through collaboration with key stakeholders and not through the stifling of free expression.
- The government should not turn the COVID-19 pandemic into an instrument that stifles freedom of expression and the expansion and enjoyment of digital rights.
- The government should work closely with platforms and internet businesses to provide affordable quality gadgets and reliable internet services to ensure wide access to and enjoyment of digital rights.
- Academia and research organizations should explore the impact of government COVID-19 measures on fundamental human rights.
- Civil society and rights organizations should continue advocating for the decriminalization of free expression and speaking out against the implementation of measures that undermine free speech.
- Civil society and rights organizations should also create awareness and empower ordinary citizens with the skills and tools to identify hate speech, as well as mis/disinformation.

27. World Bank, 'Africa's young people speak out about ending digital exclusion in their countries', <https://blogs.worldbank.org/youth-transforming-africa/africas-young-people-speak-out-about-ending-digital-exclusion>

28. African Internet Right, 'Women face internet access challenge during the COVID-19 pandemic in Uganda', https://africaninternetrights.org/sites/default/files/Peace_Oliver_o.pdf

29. WOUGNET, 'Submission on domestic violence in the context of COVID-19', <https://wougnet.org/assets/portal/wougnetwebsite/publications/2020-11-16/report.pdf>



Zambia is a landlocked country at the crossroads of Central, Southern and East Africa.

In 2020, Zambia's population stood at 17.9 million.¹ Hailed as one of the fastest growing economies in Africa, with a GDP of \$23 billion.²

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN ZAMBIA

Zambia's economic performance continued to dwindle due to declining copper prices, energy shortages, fiscal deficits that can be attributed to the country's severe debt crisis, and more recently economic pressures caused by the COVID-19 pandemic.

While the political climate remains relatively stable, the August 2021 elections are widely viewed as a decider and true test on the country's political situation judging from protest action and social media outbursts witnessed during the year about youth unemployment, high commodity and energy prices, load shedding, fluctuating foreign currency rates and high foreign debt coupled with defaults on repayments. Zambia's credit rating was downgraded after the government missed an interest payment and announced a suspension of debt service to external creditors.³

ICT SECTOR

Considerable investments have gone into upgrading the country's ICT infrastructure, including erecting about 1000 communication towers. The year 2020 saw a 25.7% increase in the number of communication



1000
Communication
Towers Erected

1. Zambia Statistics Agency, <https://www.zamstats.gov.zm/> [Accessed 23 November 2020]

2. World Bank: Zambia Country Data, <https://data.worldbank.org/country/ZM>

3. "Zambia Economic Outlook", Focus Economics, 17 November 2020, <https://bit.ly/2JgMgkL>

sites between June 2019 and June 2020.⁴ Zambia continues to maintain three mobile network providers and 17 internet service providers,⁵ although a call for issuance of a fourth mobile operator was made following the cancellation of Vodacom's license. In the third quarter of 2020, internet penetration stood at 57% accounting for over 10 222 million internet users, indicating a 2% decline from the 59% (representing 10 289 million users) recorded in the third quarter of 2019.⁶ This decline can be attributed to the depreciation of the Kwacha and inflationary pressure which led to the general increase in the cost of goods and services, leaving people with less disposable income that could be used to access internet services. Interestingly, mobile network subscriptions stood at 18,619 million, representing a 104% mobile penetration rate, indicating that there are more registered SIM cards than the total population.⁷ This could be because most individuals may own more than one mobile phone and utilise up to three SIM cards. Mobile money transactions increased by 89% from the number of transactions recorded in the first half of 2019.⁸

LOCAL AND REGIONAL POLICY DEVELOPMENTS

In terms of the ICT legal and policy environment, the Information and Communication Technologies Act of 2009, the Electronic Communications and Transactions Act of 2009, and the outdated National ICT Policy of 2006 continue to govern the use of telecommunications in the country.

While there is no clear indication regarding the drafting of a new National ICT Policy, in August

2020 the Minister in charge of Transport and Communications confirmed that four ICT Bills had been drafted and were undergoing harmonisation at the Ministry of Justice, namely: Cybersecurity and Cybercrimes Bill, Data Protection Bill, Electronic Commerce, and Transactions Bill and E-Government Bill. In June 2020, Parliament through the Committee on Media, Information and Communication Technologies adopted a committee report to enhance e-governance across all government operations.⁹ In the same month, the Ministry of Transport and Communications alongside the regulator, Zambia Information and Communication Technology Authority (ZICTA), launched the National Child Online Protection Strategy¹⁰ aimed at providing children with the necessary safeguards against online vulnerabilities.

In June 2020, Cabinet passed a resolution to approve the African Union Convention on Cybersecurity and Personal Data Protection which is a welcome step that will ensure harmonisation of the new cyber laws and regional cooperation on matters of cybersecurity, cybercrime, and data protection.

NETWORK DISRUPTIONS

In February 2020, residents of Southern Province, an opposition stronghold reported an internet blackout that affected all three mobile services. The blackout brought business to a standstill in the severely affected towns of Monze and Livingstone and it is unknown how long it lasted or what could have caused it, however, the ICT regulator, ZICTA, attributed the disruption to a technical fault.¹¹

4. ZICTA: ICT Sector 2020 Mid-Year Market Performance, 10 September 2020, <https://bit.ly/3698kXv>

5. ZICTA Statistics Portal: Operator Statistics, <https://bit.ly/37akYFa>

6. ZICTA Reports: Quarter 3, 2020, <http://onlinesystems.zicta.zm:8585/statsfinal/>

7. ZICTA Reports: Quarter 3, 2020, <http://onlinesystems.zicta.zm:8585/statsfinal/>

8. ZICTA: ICT Sector 2020 Mid-Year Market Performance, 10 September 2020, <https://bit.ly/3698kXv>

9. "Parliament adopts committee report to enhance e-governance", News Diggers, 26 June 2020, <https://bit.ly/2JhBb38>

10. ZICTA: National COP Strategy, <https://bit.ly/3l8xny5>

11. "Southern Province in internet blackout", News Diggers, 21 February 2020, <https://bit.ly/3gGme5p>, "Southern Province In Internet Network Shut Down", *Zambian Observer*, 20 February 2020, <https://bit.ly/2YNmLwh>



THREATS TO DIGITAL RIGHTS AND DIGITAL ACTIVISM

Despite a lack of comprehensive data protection laws, in December 2019 the Zambian government resumed the Lusaka Safe City project and approved a proposal by Huawei Technologies to turn Lusaka into a Smart City by mounting 24 hour CCTV cameras across the city including public markets and bus stops.¹²

Further, cautionary statements by government officials on the use of the internet and social media persisted. In February 2020, the Minister of Transport and Communications warned against alleged social media abuse by the public¹³ and in June 2020, Chief Government Spokesperson announced that the government “will not tolerate anyone using any social media platform to insult the President or any citizen.”¹⁴

In June 2020, a group of 13 activists staged a protest on the outskirts of Lusaka, after being denied a permit to peacefully march

To protect the lives of the protesters and avoid causing damage to public property, the activists opted to protest at a secret location in the bush and live-streamed the event across their social media pages, holding placards and taking turns to give moving speeches. The live streams attracted almost half a million viewers.¹⁵ Meanwhile, riot police armed in full body armor were deployed all over Lusaka and fruitlessly searched for the venue of the protest in order to dispel protesters and enforce COVID-19 restrictions. One of the activists popularly known as ‘Pilato’ said, “There are these physical streets and social media streets. I think this had more influence than if we’d gone to the physical streets.”

In March 2020, a 15-year-old male juvenile¹⁶ was arrested on charges for the defamation of the president, alongside several other Facebook page admins.¹⁷ The juvenile, who was charged with three counts of libel, operated under the pseudonym ‘ZOOM’ and allegedly published defamatory posts about the president and three others. In another incident, a famous photographer was charged with four counts of criminal libel after he allegedly aired derogatory remarks against several government officials on his Facebook page.¹⁸ In June 2020,¹⁹ an online editor of online newspapers - Zambia Reports and Eagle One - was arrested for publishing and widely circulating criminal libellous material against the Home Affairs Minister. In November 2020, a man of Kitwe was arrested for insulting the ruling Patriotic Front (PF) government and its leaders in a video that went viral on social media.²⁰

12. “Huawei to plant 24 Hour cameras across Lusaka”, 7 December 2019, <https://bit.ly/368Nesm>

13. “Stop social media abuse- Kafwaya”, News Diggers, 24 February 2020, <https://bit.ly/34qAtJ7>

14. Social media Abusers warned”, Ministry of Information and Broadcasting Services - Zambia Facebook Page, 22 June 2020, <https://bit.ly/3l5UpH8>

15. “Zambian Youth Outsmart Police”, Lusaka Times, 22 June 2020, <https://bit.ly/2Yt5OHZ>

16. “ZOOM Arrested For The Offence Of Defamation Of The President”, Zambia Reports, 12 March 2020, <https://bit.ly/3hlfjsS>

17. “ZICTA and Police Arrest Admins for Zed Hule, Zambia Watch and others Admins for a WhatsApp group”, Mwebantu, 11 March 2020, <https://bit.ly/2V5hYUS>

18. “POLICE ARREST CHELLAH TUKUTA FOR CRIMINAL LIBEL”, Zambia Reports, 18 June 2020, <https://bit.ly/32F9WGD>

19. “Police arrest Zambia Reports editor for criminal libel”, Mwebantu, 25 June 2020, <https://bit.ly/3qekSFh>

20. “Tulefwaya, ukuchinja, ubuteko”, man arrested in Kitwe for insulting the PF Government and its leaders”, Mwebantu, 24 November 2020, <https://bit.ly/2VmbLnL>



“

In December 2019 the Zambian government approved a proposal by Huawei Technologies to turn Lusaka into a Smart City by mounting 24 hour CCTV cameras across the city.

DIGITAL RIGHTS AND INCLUSION IN THE WAKE OF COVID-19 REGULATIONS

Zambia recorded its first two cases of COVID-19 on 18th March 2020 and it is one of the few countries in the region that did not close its borders. The rise in positive cases led to a closure of schools, private and public services, amenities, and non-essential workers were sent to work from home. The unprecedented COVID-19 pandemic saw many Zambians migrating their day-to-day activities to digital platforms for communication, financial transactions, schooling, meetings, entertainment etc. This move forced many citizens to utilise existing digital literacy skills and to develop new ones in order to cope with the disruption.

Unfortunately, with the increased use of the internet and digital services came the rise in cybercrimes such as online fraud, impersonation and mobile money scams.²¹ This reinforced the need for increased user digital security awareness and

consumer protection initiatives. Several mobile network providers zero-rated some browsing services and transaction fees, and increased daily transaction limits to enable free flow of funds and ease remote payments of bills and essentials.²²

The country's digital preparedness was tested as most institutions of learning battled to cope with delivering online lessons and lectures to learners. Students and learners could not access e-learning facilities due to prohibitive costs, lack of access and ownership of gadgets, unavailability and lack of adequate e-learning platforms in some institutions and limited digital literacy skills for both teachers and learners. Further, the pandemic exposed a severe lack of access to digital infrastructure and e-learning platforms for people living with disabilities and lack of digital literacy skills, infrastructure and connectivity for people living in rural areas.

21. ZICTA: ICT Sector 2020 Mid-Year Market Performance, 10 September 2020, <https://bit.ly/3698kXv>

22. "Airtel Zambia scraps transaction fees for money transfers", Telecompaper, 26 March 2020, <https://bit.ly/3ldztgr>

While no significant movement restrictions were imposed in the country, the media were allowed to adequately cover the live COVID-19 briefing sessions and utilised various digital platforms to keep the nation informed. In addition, the Ministry of Health live-streamed the bulletins on their social media pages. However, no media personnel were allowed inside the COVID-19 isolation facilities.

In April 2020, a popular private TV channel, Prime TV, had its license canceled by the Independent Broadcasting Authority (IBA) over a COVID-19 advert dispute. The TV channel allegedly refused to

air COVID-19 adverts for free.²³ Activists described this as an attack on access to information as Prime TV is widely viewed as a balanced and objective media house that provides an alternative to the state-owned ZNBC TV. The Law Association of Zambia described the cancellation of Prime TV's license as illegal and that "it was done prematurely without following the correct channels of the law".

As of November 2020, Zambia had recorded 17,553 total cumulative positive cases of COVID-19, 16,779 recoveries, and 357 deaths.²⁴

CONCLUSION AND RECOMMENDATIONS



There is an urgent need to enact updated ICT laws that will provide cybersecurity, provide protection against cybercrime and ensure data protection and privacy. In addition, if the SMART City project comes into effect, there will be a need to provide strict measures on the protection of data that is captured as well as ensuring that the technology is not used to spy on unsuspecting citizens, human rights defenders, activists, etc. Furthermore, there is a need to ratify the African Union Convention on Cybersecurity and Personal Data Protection to provide a regional framework for combating cybercrimes as well as to ratify an international convention such as the Budapest Convention on Cybercrime, to provide a framework for international cooperation.

Furthermore, there is a need to continue investing in digital infrastructure, skills development, and literacy programs to capacitate users with the know-how on utilizing ICTs in their day to day lives as well as consumer protection and digital security skills for online safety. There is a need to update the National ICT Policy to capture new national ICT aspirations and goals as well as provide a broadband plan which must provide strategies that enhance access and connectivity for under served groups such as people living with disabilities, in rural areas, women, girls, etc.

Zambia Digital Rights and Inclusion Report 2020 Lastly, ahead of the highly contested August 2021 elections, the government of Zambia must commit to keeping the internet on and to not harass online users, but rather to promote online platforms as spaces for communication, access to information, and civic engagement.

23. "Zambia cancels license of private TV channel over COVID-19 ad dispute", International Press Institute, 14 April 2020, <https://bit.ly/2HGeDIC>

24. Zambia National Public Health Institute: Zambia COVID-19 Dashboard, <https://bit.ly/39hr3Ch>



Case Study: COVID-19 and the need for data privacy and protection regulations in Zambia

Compiled by Bulanda Nkhowani

Zambia recorded its first two cases of COVID-19 in March 2020 and was one of the few countries in the region that partially kept its borders open. While most countries battled to find ways to understand, mitigate and stop the spread of the novel coronavirus, Zambian health professionals quickly took to a tried and tested method to prepare, surveil and respond to the looming threat. The Ministry of Health (MoH), through the Zambia National Public Health Institute (ZNPHI), implemented a multi-sectoral emergency response approach to fight COVID-19, an approach that had previously been used to fight reoccurring cholera outbreaks in the country. This involved activating the National Public Health Emergency Operations Centre (PHEOC) located at the ZNPHI and using a multi-sectoral Incident Management System (IMS) approach, supplemented by a dedicated call centre to coordinate efforts.

“It all started with a slight tickle in my throat upon returning from a trip to a neighbouring country for business. At that time COVID-19 had just hit Zambia and there was a general panic across the country. I called the toll-free line where the person from the call centre enquired about my symptoms. They also took down my names, phone number, physical address, occupation, next of kin and information about where I had physically been to in the last few days as well as whom I had interacted with. The person appeared to be typing and capturing my responses on the other end, they ended by promising that I would receive help from a response team that had been dispatched to assist me and that I stay put within my house. I was very lucky to have contracted the virus at a time when response teams were very fast in responding. In no time they arrived at my premises. Sadly, I tested positive for the virus, although I was not exhibiting severe symptoms, I was admitted to the COVID-19 isolation ward,” said Mutale, one of the earliest COVID-19 survivors.

Tamara’s case on the other hand was different, “After experiencing high fever and a dry cough, I visited the nearest health facility to test for COVID-19. My suspicions were right, I tested positive for the virus. I was led to a room where a medical professional manually took down my personal identifying details and those that would be used to trace any individuals that I had been in contact with. I read a lot about data rights so naturally, I was concerned about how my



information would be stored, used and for how long it would be kept seeing as the medical professional was now entering it onto a paper that could easily be lost. Also, my consent was not sought when acquiring this data, however, when I enquired as to what it would be used for, I was assured that it was safe and that it would be used only for purposes of contact tracing and reporting. I was later advised to self-isolate at home for a period of 14 days. In those days I got phone calls from my case manager enquiring how I was faring on a daily basis until the end of my quarantine period. I am not sure what became of my personal information,” she said.

Zambia, like many countries in sub-Saharan Africa, uses a mostly manual contact tracing approach aided slightly by mobile phones and computers to monitor, locate and contact existing and potential COVID-19 patients. While no contact tracing apps exist, all relevant COVID-19 data are captured into a national public health database which then raises concerns on the safety and security of personal health data that is captured, especially for public health emergencies. Other systems and networks exist, for example a network that acts as a communications hub for all emergency field agents involved in the front-line fight against COVID-19.

Amid this data collection and uncertainty on the personnel and protocols involved in accessing the database or principles governing data sharing or third party involvement in the development, supply and management of the database, Zambia continues to lack data protection and privacy laws. Similarly, in 2017, Zambia rolled out an e-health system to deliver digital health solutions, further raising questions on the capacity of public health data handlers to adhere to data protection and privacy ethics.

It is clear that data is key to solving current and future public health threats. The urgent need for enactment of human rights-respecting data protection and privacy regulation, that safeguard personal data and privacy of citizens like Mutale and Tamara, is also more apparent. This need includes frameworks that oversee implementation of best practice policies on the capture, storage, management, transfer or retention of data on information systems. Furthermore, there is a strong need to build the capacity of health professionals and third parties’ obligations when handling sensitive data. Citizen awareness is also critical in ensuring that the correct policies and protocols are implemented and that individuals’ rights are not infringed upon.



Zimbabwe is a country in Southern Africa under the new rule of President Emmerson Mnangagwa following the ousting of the late former president Robert Gabriel Mugabe in 2017.

INTRODUCTION

DIGITAL RIGHTS AND INCLUSION IN ZIMBABWE

In terms of the Constitution of Zimbabwe, 2013 section 3(c), Zimbabwe is founded on values and principles of fundamental human rights and freedoms. Digital rights are fundamental human rights enabling the enjoyment of life with dignity. These human rights are outlined in the Universal Declaration of Human Rights, the International Covenant for Civil and Political Rights (ICCPR), the International Covenant on Economic Social and Cultural Rights (ICESCR) and the African Charter on Human and People's Rights.

On 27 June 2014, the African Union Convention on Cyber Security and Personal Data Protection¹ was adopted by the African Union and to date, Zimbabwe is not a signatory. The legal framework on data protection and cyber security remains piecemeal. In 2020, Zimbabwe gazetted the Cyber Security and Data Protection Bill which has not yet come into effect and does not sufficiently protect digital rights. The state of digital rights and inclusion in Zimbabwe increasingly became a concern in 2020 due to the events which howed a departure from human rights standards.



Cyber Security and Data Protection Bill not yet in effect

1. See <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf>



IMPACT OF COVID-19 REGULATIONS

In response to the COVID-19 pandemic, the government of Zimbabwe enacted Statutory Instrument (S.I.) 83 of 2020² which provides in section 14 that any person who communicates falsehoods shall be liable for prosecution under section 31 of the Criminal Law Code³ (“Publishing or communicating false statements prejudicial to the State”) and liable to a penalty or up to twenty years imprisonment. Section 14 abolishes criminal defamation provisions and expands the scope of the already problematic Section 31 of the Criminal Law (Codification and Reform) Act Chapter 9:23 (the Criminal Law Code) which provides numerous restrictions on freedom of expression and presents penalties of up to 20 years imprisonment. The offence of criminal defamation was abolished in Zimbabwe following a finding of unconstitutionality by the Constitutional Court in the Madanhire case.⁴

During the COVID-19 lockdown period from 30 March to September 2020,

informal traders comprising largely youths and women lost their source of income. Amidst high inflation rates and an ailing economy, the government embarked on allocating COVID-19 relief to low-income families. Vendors Initiative for Socio-Economic Transformation (VISET), an organisation with 68 000 members told PIN that a few VISET members received this allocation. The government approached VISET and asked for a list of those in need. Relief was going to be allocated to those registered on OneWallet, a mobile money transfer platform that operates on a NetOne cell phone line. This was problematic as most members were registered on other mobile money platforms such as Ecocash, a service provided by Econet.

Subsequently, the Finance Minister reportedly made a statement that the government would make use of a sophisticated algorithm to allocate COVID-19 relief grants to affected groups of low income earning households. Marginalized groups were left out from the relief. There were no consultations with the community and no explanation of the privacy policy employed in the use of algorithms in allocating COVID-19 relief.⁵

ENJOYMENT OF FREEDOM OF EXPRESSION, ASSEMBLY AND ASSOCIATION IN 2020

During the lockdown which commenced on 30 March 2020, the Zimbabwe Human Rights NGO Forum documented 20 cases of journalists whose media freedoms were violated as at 29 October 2020.⁶ Moses Sigauke, a nurse at Sally Mugabe Central Hospital went on trial in July 2020 following an arrest and charged with incitement as

2. Statutory Instrument (S.I.) 83 of 2020 <https://zimlil.org/zw/subleg-consol/S.I.%2083%20of%202020%20Public%20Health%20%28COVID-19%20Prevention%2C%20Containment.pdf>

3. Criminal Law (Codification and Reform) Act Chapter 9:23, <https://zimlil.org/zw/legislation/act/2004/23>

4. See Madanhire & Anor v The Attorney General 2014 (1) ZLR 719 (CC)

5. Mthuli Ncube & His “Sophisticated Algorithms” For Corona Relief Funds – Another Privacy Disaster Looming?, TechZim, <https://www.techzim.co.zw/2020/04/mthuli-ncube-his-sophisticated-algorithms-for-corona-relief-funds-another-privacy-disaster-looming/>

6. The Zimbabwean, Zimbabwe COVID-19 Lockdown Weekly Monitoring Report 23-29 October 2020 – Days 206-213

<https://www.thezimbabwean.co/2020/11/zimbabwe-COVID-19-lockdown-weekly-monitoring-report-23-29-october-2020-days-206-213>

defined in section 187 of the Criminal Law Code. He was acquitted from allegations of abusing Facebook to mobilise and incite medical practitioners to stage protests against the government. Hopewell Chin'ono and Jacob Ngarivhume were arrested on 20 June 2020 for whistle blowing on corruption and allegedly, for planning demonstrations against corruption on the 31st of July 2020, respectively, following expressions made online.

The Constitution under section 61 (5)(a) and (b) states that incitement of violence and hate speech do not form part of freedom of expression and freedom of the media. However, hate speech was propagated in the course of 2020. A noteworthy event is that of the Archbishop Robert Ndlovu, whose attack, marred with tribal connotations, was condemned globally following a letter by the Zimbabwe Catholic Bishops' Conference calling for urgent resolution to the country's economic and political challenges. The *#ZimbabweanLivesMatter* hashtag was trending in August 2020 following global condemnation of human rights violations in Zimbabwe and among other things, hate speech on Archbishop Ndlovu⁷ whom the Zimbabwe Information Minister Monica Mtsvanga accused of being evil. Zimbabweans came together under the hashtag which was followed by the deployment of a South African delegation to engage on the human rights situation in Zimbabwe.⁸

In April 2020, Lovemore Zvokusekwa appeared before Harare Magistrates Court after he was arrested and charged with communicating falsehoods as defined in section 31(a)(i) of the

Criminal Law Code. In summing up challenging digital rights issues in 2020, POTRAZ mentioned to Paradigm Initiative (PIN) that misinformation was a major issue faced in 2020. There is need for citizens to be responsible through fact checking before sending communications and making use of platforms like Zimfact to sift fact from fiction.⁹ Nevertheless, while there is a need to curb misinformation, regulations must conform to human rights standards. The use of online propaganda by the group commonly known as Varakashi, Zanu-PF's (the ruling party) "online warriors", continued in 2020 and this onslaught has been seen over the years manifesting in the form of criticisms, hate speech, gender-based attacks, harassment and peddling of false news online using fake accounts in political and dissenting discourse.¹⁰

On 5 July 2020, the Freedom of Information Bill which sought to repeal the Access to Information and Protection of Privacy Act¹¹ was gazetted. Contrary to what the name suggests, the new law focuses on access to information and not freedom of expression. The Cyber Security and Data Protection Bill¹² (the Bill) was gazetted on 15 May 2020. Its purpose is to consolidate cyber related offences and provide for data protection with due regard to the declaration of rights under Chapter 4 of the Constitution and the public and national interest.

Incitement of violence and hate speech do not form part of freedom of expression and freedom of the media.



THE CONSTITUTION UNDER SECTION 61 (5) (A) & (B)

7. See <https://twitter.com/davidcoltart/status/1294981558013763586?lang=en>

8. <https://elmmagazine.eu/adult-education-and-democracy/social-media-creates-new-space-for-activism-in-zimbabwe/>

9. See Zimfact on <https://zimfact.org/about-us/>

10. See <https://theconversation.com/a-vicious-online-propaganda-war-that-includes-fake-news-is-being-waged-in-zimbabwe-99402> and <https://www.africafex.org/digital-rights/cybersecurity-and-data-protection-bill-entrenches-surveillance>

11. Veritas, BILL WATCH 40-2019 The Freedom of Information Bill, <http://www.veritaszim.net/node/3618>

12. Cyber Security and Data Protection Bill, 2019, http://veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf



“

There is need for citizens to be responsible through fact checking before sending communications and making use of platforms like Zimfact to sift fact from fiction.

It seeks to establish a cyber security centre and a data protection authority, to which roles are designated to the POTRAZ. Furthermore, the Bill provides for investigation and collection of evidence of cybercrime and unauthorised data collection and breaches, and to provide for admissibility of electronic evidence for such offences. This enhances the conduct of trials in the digital age.

The Bill also creates a technology driven business environment and encourages technological development and the lawful use of technology.

The Bill, however, has its flaws such as the criminalization of falsehoods in section 164C which attracts a penalty of up to 5 years imprisonment.

Apart from this Bill, the Criminal Law code has been largely relied upon by the Zimbabwe Republic Police to follow through on surveillance on human rights defenders with arbitrary arrests. The notorious provisions of section 22 of the code have been used to criminalise free speech. The Interceptions of Communications Act, 2007 has been also used for targeted surveillance on human rights defenders inconsistent with regional and international privacy standards. The government proposed crafting a new law termed the Patriotic Bill which will criminalise campaigning against the country through private correspondence with foreign governments and harming national interests.¹³ Such law if drafted and passed shall have adverse effects on freedom of expression, media freedoms, association and privacy rights among others.

13. <https://www.sundaymail.co.zw/new-law-to-criminalise-unpatriotic-acts>

PRIVACY, DIGITAL ID AND SURVEILLANCE

Privacy is aptly protected by section 57 of the Constitution. In July 2020, the High Court granted an order in favour of MISA Zimbabwe interdicting Econet Wireless Zimbabwe and others from implementing a police warrant seeking information on the mobile phone operator's transactions.¹⁴ This order had the effect of defending the right to privacy of Econet users. The use of biometric technology has in the past attracted distrust from some members of the population following the 2018 elections. Currently, the Department of the Registrar General issues biometric national identity documents through a process that collects fingerprints and the iris. While this has digitised the process of documenting citizens, the concern lies in the possible abuse of data by third parties in the absence of adequate data protection laws that safeguard privacy.¹⁵

In February 2020, the government gave an ultimatum to civil servants who were not complying with the compulsory biometric registration introduced in 2019 for civil servants or they would risk being struck off the payroll at the end of the month.¹⁶ The Interception of Communications Act remains a tool for breaching privacy against human rights defenders through surveillance. The Act extends to intercepting communications through phone calls, emails and fax. In June 2020, a detailed account was given by the government on the movement of opposition activists aligned to the Movement for Democratic Change (MDC), Joana Mamombe, Cecilia Chimberi and Netsai Marova following a reported abduction.¹⁷ This account of the event by the government was aimed at casting aspersions on the abductions. The government reportedly made use of CCTV footage from a supermarket, cell phone tracking and pictures to disprove the allegations of an abduction.¹⁸ This account of the event by the government was aimed at casting aspersions on the abductions. The government reportedly made use of CCTV footage from a supermarket, cell phone tracking and pictures to disprove the allegations of an abduction. The account of their movements on the day of the



14. MISAZim, Court Grants Order in Favour of MISA Against ECONET Search Warrant

15. Engine Room, Digital ID in Zimbabwe: A case study, [https://digitalid.theengineroom.org/assets/pdfs/\[English\]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf](https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf)

16. See <https://www.zimeye.net/2020/02/11/government-gives-civil-servants-ultimatum-to-comply-with-biometric-registration/> Digital ID in Zimbabwe: A case study, [https://digitalid.theengineroom.org/assets/pdfs/\[English\]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf](https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf), See <https://twitter.com/zifmstereo/status/1268467649123622912?lang=en> Herald, MDC-A abduction claims under scrutiny <https://www.herald.co.zw/mdc-a-abduction-claims-under-scrutiny/> See <https://www.zimeye.net/2020/02>

17. See <https://twitter.com/zifmstereo/status/1268467649123622912?lang=en>

18. Herald, MDC-A abduction claims under scrutiny <https://www.herald.co.zw/mdc-a-abduction-claims-under-scrutiny/>

alleged abductions was evidence of surveillance which civil society actors, political actors and other human rights defenders are exposed to in breach of their privacy rights.

INTERNET ACCESS

According to POTRAZ, the internet penetration stood at 59,9% at the end of the third quarter in 2020,¹⁹ a drop from the 60,6% recorded in the 2019 fourth quarter report. This internet penetration rate is at great variance with the 27% internet penetration rate recorded by the International Telecommunication Union at the end of 2019. In light of the growing need for internet access, especially during the COVID-19 pandemic, there is a need for an increase in internet penetration.

According to the *African Declaration on Internet Rights and Freedoms*, the cutting off or slowing down of access to the internet, or parts of the internet, for whole populations or segments of the public, should not be permitted on any grounds, including public order or national security grounds.²⁰ Zimbabwe experienced erratic and slow internet access on 30 and 31 July 2020 ahead of planned protests which were meant to occur on 31 July 2020.²¹ NetBlocks documented the incident as a slowing down or throttling of connectivity speeds on both days on TelOne network.²² The disruption lasted approximately 5 hours on the 30th and 14 hours on the 31st of July.²³ This was in clear violation of internet freedom.

The cost of data in Zimbabwe was high for low-

income households and vulnerable communities following the COVID-19 pandemic which called for lockdowns and retrenchment of many from the job market. Zimbabwean data costs are not the highest in the Southern African region,²⁴ however, considering the high cost of living in Zimbabwe, marginalized communities cannot afford an average of about US\$4 for access to 1GB mobile prepaid broadband. The need for internet access was more pronounced in the advent of the COVID-19 pandemic which first struck Zimbabwe in March 2020.²⁵ According to a statement by MISA-Zimbabwe on 14 April 2020,²⁶ the cost of mobile data in Zimbabwe remains prohibitive, discriminates and infringes on citizens' rights to access to information as provided for by the Constitution and the African Declaration on Internet Rights and Freedoms. The internet penetration rate is even lower in rural areas and the digital divide needs to be bridged by digital infrastructure that enables internet access.²⁷

THE EXTENT OF DIGITAL EXCLUSION AND ITS IMPACT ON HUMAN RIGHTS

While the exact extent of the digital divide is not readily ascertainable, Afrobarometer survey data from 2017 and 2018 shows that a majority of Zimbabwean households didn't have mobile phones with internet access, computers, or reliable electricity supply. Cell-phone service was available in almost all urban zones as of 2017, but 15% of rural areas did not have coverage. 43% of cell-phone

19. POSTAL AND TELECOMMUNICATIONS REGULATORY AUTHORITY OF ZIMBABWE (POTRAZ), ABRIDGED POSTAL & TELECOMMUNICATIONS SECTOR PERFORMANCE REPORT, <https://t3n9sm.c2.acecdn.net/wp-content/uploads/2020/12/Abridged-Sector-Performance-report-3rd-Q-2020.pdf>. See also, <https://t3n9sm.c2.acecdn.net/wp-content/uploads/2020/03/Abridged-Sector-Performance-report-4th-Q-2019.pdf>

20. See African Declaration on Internet Rights and Freedoms, <https://africaninternetrights.org/en/principles/2>

21. Jeffrey Moyo and Patrick Kingsley, Zimbabwe Locks Down Capital, Thwarting Planned Protests, <https://www.nytimes.com/2020/07/31/world/africa/zimbabwe-coronavirus-protest.html>

22. NetBlocks, <https://netblocks.org/reports/zimbabwe-internet-disruption-limits-coverage-of-protests-7yNV70yq>

23. NetBlocks, <https://netblocks.org/reports/zimbabwe-internet-disruption-limits-coverage-of-protests-7yNV70yq>

24. See https://researchictafrica.net/ramp_indices_portal/

25. Idah Mhetu, Zimbabwe Records First Confirmed Case of Coronavirus, Minister Appeals for Public Calm <https://allafrica.com/stories/202003210054.html>

26. <https://www.africafex.org/country-highlights/misa-zimbabwe-calls-for-reduction-in-cost-of-data>

27. See <https://freedomhouse.org/country/zimbabwe/freedom-net/2020>

owners and only 28% in rural areas said their phones had access to the internet.²⁸ Digital exclusion is widening the inequality gap in Zimbabwe through the absence of adequate access to digital technology and connectivity to the internet that enhances access to education and jobs among other rights. While private schools migrated to online platforms, rural communities were left behind. Community Youth Development Trust (CYDT) mentioned to PIN that digital infrastructure remained a challenge for many considering the limited resources that are necessary to enable the use of data, systems and processes.

Principle 37 of the African Declaration of Principles on Freedom of Expression and Access to Information mandates States to facilitate the rights to freedom of expression and access to information online and the means necessary to exercise these rights. The internet should be accessible and affordable without discrimination. The Amalgamated Rural Teachers Union of Zimbabwe mentioned three critical barriers to digital inclusion - the cost of data which was too high for ordinary citizens, minimal availability of devices for accessing the internet and limited digital literacy in rural communities. The Ministry of Primary and Secondary Education launched a program to offer online classes via radio which was a welcome step in bridging the digital divide. However, the gap remains due to unavailability of devices and limited coverage.²⁹

The lack of access to smart phones and other forms of technology was a barrier to accessing critical information on the COVID-19 pandemic in 2020, basic health care and also affected access to

information relevant for the enjoyment of human rights such as information on service delivery, development and proposed amendments to the Constitution. With adequate access to digital tools, communities would be more empowered to engage with national processes.

DIGITAL EXCLUSION

According to the Decades of Struggle and Hope: A Zimbabwean Youth Compendium 2019 report published by Youth Empowerment and Transformation Trust, 42% of youth owned a smartphone and 14% had access to them. In the findings of the report, the prominence of internet use for social networking was corroborated by participants in all urban and some rural focus group discussions who reported using the internet to access Facebook, Twitter, WhatsApp, Instagram, Skype, YouTube, Tinder and Telegram.³⁰ This did not improve in 2020. Access to digital technologies for women and girls is critical for women empowerment and remains a gap which needs to be breached in Zimbabwe.

Women, who form the majority in the informal sector, were grossly affected by the lockdown in 2020 which saw the informal sector grounded from trading meaningfully for the greater part of the year. While a considerable number of urban women have access to smartphones, access to the internet is out of reach for many, especially in the rural areas. Bridging the digital divide for women improves their access to information which is critical in accessing basic human rights such as maternal health care and education.

28. AfroBarometer, Limited Internet access in Zimbabwe a major hurdle for remote learning during pandemic, http://afrobarometer.org/sites/default/files/publications/D%C3%A9p%C3%Aches/ab_r7_dispatchno371_hurdles_for_remote_learning_during_pandemic_in_zimbabwe.pdf

29. The Herald, Zimbabwe: Bridging the Digital Divide in Education <https://allafrica.com/stories/202006090417.html>

30. YETT, Decades of Struggle and Hope: A Zimbabwean Youth Compendium 2019 Report <https://bit.ly/2MII8jw>

DIGITAL INFRASTRUCTURE

In 2018, the Ministry of ICT partnered with POTRAZ and established more than 200 Community Information Centers (CICs). These CICs provide access to computers, the internet and other digital technologies that enable people to gather information, create, learn and communicate with others while they develop essential digital skills. This was initiated to reduce the digital divide. While these CICs are useful and a step in the right direction, they lack adequate funding and their reach is limited. There is a need for more sustainable solutions which ensure better resourcing of CICs, capacitating rural schools, clinics and other community-based centers to have the necessary broadband access and digital technologies for bridging the digital divide.

CONCLUSION AND RECOMMENDATIONS



The government must promote an enabling environment for digital rights and inclusion by amending or repealing repressive and archaic policies and laws. There is a need for an effective data protection law. The Cyber Security and Data Protection Bill must adequately safeguard privacy and provide penalties that fall within the bounds of proportionality. COVID-19 must not be used as an excuse to stifle dissent. Freedom of expression must be liberated through cessation of arbitrary arrests and unlawful detention meted out to media practitioners and activists. Unwarranted charges against media practitioners and activists must be dropped in the promotion of digital rights. It is incumbent on the government and telecommunications companies to ensure data protection and access to the internet which is unhampered by disruptions.

The government must work with a broad spectrum of stakeholders to ensure a sustainable digital infrastructure. There is a need for consultative and awareness raising multi-sectoral processes before introducing any technology that collects data from data subjects. The engagements must be all inclusive reaching among others, civil society actors, technologists, media practitioners, persons with disabilities, women, children and the youth. The government must be transparent ensuring that policies are implemented with due consideration for human rights. Telecommunications companies must provide transparency reports that clearly outline their conduct of business which should adhere to human rights standards. Civil society organisations must continue to engage with the government and telecommunications companies for an enabling environment for digital rights and inclusion.



Case Study: COVID-19 Case No.15: A Zimbabwean victim of misinformation

Compiled by Thobekile Matimbe and Everson Mushava

A Bulawayo lady who tested positive for COVID-19 at the inception of the recording of cases in Zimbabwe was subjected to brutal attacks online. This followed a release by the government, in the Chronicle newspaper, that the patient – Case No. 15 – was violating COVID-19 regulation by escaping from quarantine, and posing a health risk to the community. Unfortunately, as a result of this, Case No.15 got to hear the news of her status through social media, leaving her victimised. The system of disclosure of information was flawed and had no regard for the protection of personal information of patients. For purposes of preserving the identity of Case No. 15, this case study refers to her as X.

On April 16 2020, the Chronicle newspaper ran an article on X expressing concern that she was Case No. 15 yet gallivanting across the city of Bulawayo, spreading COVID-19 in blatant disregard for isolation as required of positive patients. The headline was titled, “Beware of this patient! COVID-19 positive woman gallivants around town.” The article gave an exposition of X disclosing that Case No. 15 was a health worker breaching COVID-19 guidelines after a positive test result. It portrayed her as a reckless individual.

Information gathered revealed that X was screened for COVID-19 on April 12, 2020, using a thermometer and turned out to have a high temperature. She was then tested for COVID-19 by a Rapid Response Team which advised her to wait for 48 hours to access her results. On the night of April 14 2020, X then received messages on her cell-phone from colleagues who were checking if she was alright. She discovered a COVID-19 update report released by the government which was describing her as Case No. 15 amongst the new messages on her phone.

“I checked my inbox and came across the daily update from the Ministry of Health and Child Care and immediately realised that Case No. 15 was referring to me as had a number of my colleagues. I resolved to await official communication from the Rapid Response Team who only came through to my residence on Tuesday, the 15th, at 1430hrs.”



That was her first encounter with her results. The government, through the Rapid Response Task Force, failed to reveal X's results to her before disclosing them publicly. Her colleagues were able to also gather from the description in the report that X was positive of COVID-19. X was appalled by having to find out of her COVID-19 status through social media.

As if this were not enough, X was even more shocked when the Chronicle released the article on April 16, 2020.

"[Imagine] my shock when in the wee hours of the morning on Thursday the 16th of April, 2020, I received a link to the publication by the Chronicle accusing Case Number 15 of recklessly endangering the lives of residents by defying self-isolation. Social media has since been awash with the news which begs me to ask whether there is another Case Number 15 or is this just a case of unethical journalism," expressed X.

The newspaper article in the Chronicle is no longer accessible at the time of writing this story. Through the article, the government peddled false news about X. The false news found its way on various online platforms such as WhatsApp and Facebook. The government later clarified that X was not guilty of the allegations made against her through an article in the Chronicle on April 18, 2020, titled "COVID-19 defaulting patient taken to Thorngrove." This new version in the Chronicle disclosed that there was a mix up as Case No. 15 was not the individual who had breached COVID-19 isolation procedures as revealed by health officials.

There is a need for the government to ensure that safeguards are in place for adequate privacy and personal data protections.



Case Study: Protecting the privacy of Zimbabwean COVID-19 patients

Compiled by Thobekile Matimbe and Everson Mushava

Zimbabwe recorded its first COVID-19 case on March 21 2020 amidst an unprepared healthcare system. Slowly, the numbers of COVID-19 recorded cases started growing. Amidst these cases was the misfortune that befell Saul Sakudya, a Harare businessman.

Sakudya was the third recorded case of COVID-19 since the outbreak started in March 2020 in Zimbabwe.

According to Sakudya, he presented the tell-tale symptoms of coughing and feeling dizzy after his return from a trip to Dubai on March 19 2020. He consulted with medical practitioners but his situation did not improve. Sakudya resolved to visit Wilkins Infectious Hospital (Wilkins) which was the only designated hospital handling cases of COVID-19 at the time. His 21-year-old son drove him to Wilkins and Sakudya was tested for COVID-19 but did not immediately access his test results.

“I was told that my results would come out in five hours and if they didn't, it would mean that I had tested negative,” said Sakudya.

He went home to wait for his results, anxiously. It was only on the third day that Sakudya received a call that he had tested positive. According to Everson Mashava, a journalist who conducted the interview with Sakudya, the Ministry of Health permanent secretary, Ms. Agnes Mahomva, confirmed to The Standard newspaper at the time that COVID-19 test results were indeed meant to be delivered within five or seven hours.

The delay in receiving an update on his results caused much anxiety. The Ministry of Health officials then took samples for testing of Sakudya's wife and son as they were his caregivers, as well as his 10-year-old daughter. This was part of the contact tracing response to COVID-19 by the taskforce handling the disease.

In the meantime, Sakudya was placed in quarantine at Beatrice Infectious Diseases Hospital in Harare. He suffered from stigmatisation at the hospital as



COVID-19 was a new and terrifying phenomenon to the medical personnel at the hospital. The medical personnel at the time had no adequate personal protective equipment and as such were fearing for their lives. In this chaos, Sakudya opted to go back home to quarantine in a more conducive environment for his recovery.

What was even more disconcerting was that before his family received their test results, social media users had received information that two of his family members had tested positive of COVID-19. Apparently, the government published the new cases before revealing the results to the patients in violation of their right to accessing information.

“It was saddening that results came after announcements were made and were already circulating on social media. That is not good,” expressed Sakudya in a state of dismay. “We received several calls from relatives, friends and neighbours who told us that social media was awash with news that three family members have tested positive to the virus. This was before the Ministry of Health officials came with the results. It was very traumatizing for my wife and son to learn of their health status on social media.” True to the results circulating online, Sakudya’s wife and son tested positive, while their 10-year-old daughter tested negative.

Sakudya’s wife mentioned that she was a victim of social media bullying. “It was a painful experience. Firstly, I was described as a small house, a home wrecker, and then, my COVID-19 results going viral without me knowing them,” she said.

Sakudya’s 21 year old son also expressed concern at the “apparent disregard for confidentiality of the family’s health status.” He mentioned that his family suffered stigmatisation as a result of the positive results.

The Sakudya family experienced trauma both through the delayed disclosure of COVID-19 results and the failure to exercise due caution in the release of the results in March 2020. There were clearly no effective data protection measures in place to ensure a level of care taken in informing the patients of their results. Such measures would, for example, provide for the publication of updates of new COVID-19 cases after the individuals concerned were notified of their results. Furthermore, there was a need to put measures in place to protect the privacy of the patients who tested positive for COVID-19.

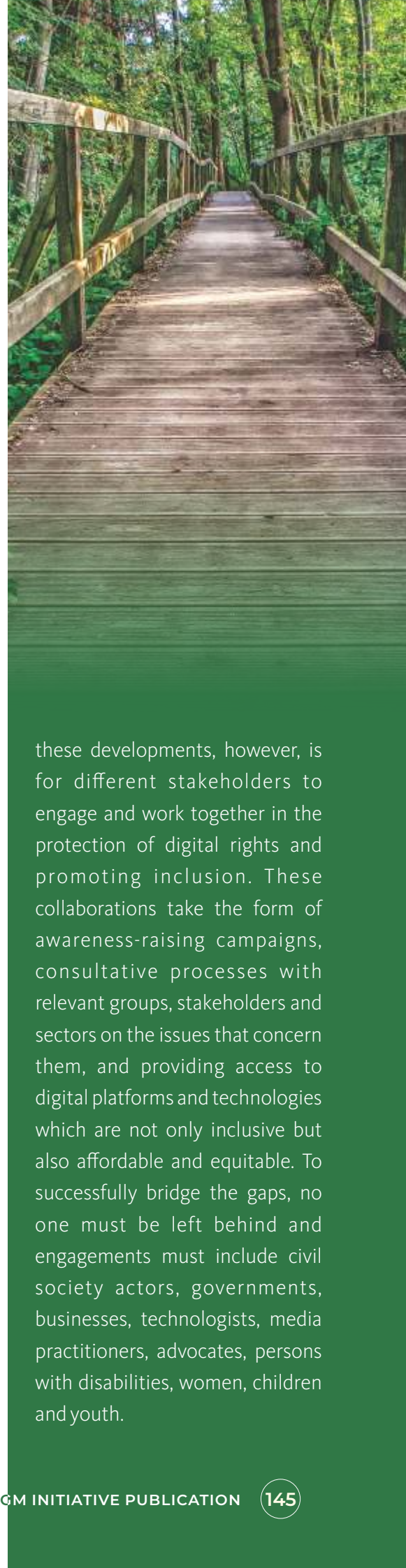
CONCLUSION

The digital ecosystem in Africa continues to be marked by violations. This report has captured the state of digital rights in 20 countries, with censorship and disruptions being reported throughout 2020. The recommendations from the country reports show a resounding consensus on calls for efforts that will guarantee human rights, develop infrastructure and promote meaningful and affordable access. Legislative and policy frameworks on data protection and privacy, as well as cyber laws, must comply with ratified regional and international standards, mainly the African Charter on Human and Peoples' Rights (the Charter) and the International Covenant on Civil and Political Rights which provide in articles 9 and 19 respectively for freedom of expression, opinion and access to information. Additionally, it is important for outstanding African states to ratify the African Union Convention on Cybersecurity and Personal Data Protection to bring it into force and provide a regional framework for combating cybercrimes while countries without data protection laws must prioritise enacting these laws. It is also paramount that countries which still criminalise defamation and false news, repeal such laws and focus on alternative means to curb misinformation such as through civil claims.

Due to the pandemic, the issues of affordability and meaningful access have never been more urgent. This report highlights numerous populations that are being left behind as a result of the evident lack of inclusive digital opportunities required to narrow the digital divide. The African Commission on Human and Peoples' Rights' Declaration on Principles of Freedom of Expression and Access to Information lays down principles for promoting and fulfilling article 9 of the Charter which African states must refer to in ensuring compliance. A common thread of poor digital infrastructure is highlighted across the countries covered, indicating that attention must be given to building resilience against future crises by focusing on improving access for everyone in place of decisions that violate the rights of African citizens and preclude inclusion.

The potential and impact of engagement and collaboration were demonstrated in this report by noteworthy milestones in Ghana, Botswana, Malawi and Kenya. Of equal importance to celebrating

these developments, however, is for different stakeholders to engage and work together in the protection of digital rights and promoting inclusion. These collaborations take the form of awareness-raising campaigns, consultative processes with relevant groups, stakeholders and sectors on the issues that concern them, and providing access to digital platforms and technologies which are not only inclusive but also affordable and equitable. To successfully bridge the gaps, no one must be left behind and engagements must include civil society actors, governments, businesses, technologists, media practitioners, advocates, persons with disabilities, women, children and youth.





DIGITAL RIGHTS AND INCLUSION IN AFRICA

A PARADIGM INITIATIVE PUBLICATION

Published by Paradigm Initiative

374 Bomo Way, Yaba, Lagos, Nigeria

Email: media@paradigmhq.org

www.paradigmhq.org

Published in April 2021

Report produced by Paradigm Initiative

Design & Layout by Luce Concepts

This publication maybe reproduced for non-commercial use in any form provided due credit is given to the publishers, and the work is presented without any distortion.

Copyright © 2021 Paradigm Initiative



Creative Commons Attribution 4.0 International (CC BY 4.0)



Paradigm Initiative

374 Bomo Way, Yaba, Lagos, Nigeria

Email: media@paradigmhq.org

www.paradigmhq.org



@ParadigmHQ