AFRICAN DECLARATION
ON INTERNET RIGHTS AND FREEDOMS

The impact of COVID-19 on digital rights in Africa

AFRICAN DECLARATION ON INTERNET RIGHTS AND FREEDOMS

The impact of COVID-19 on digital rights in Africa

COORDINATION TEAM
Koliwe Majama (APC)
Janny Montinat (APC)
Avani Singh (ALT Advisory)

SELECTION TEAM
Izak Minaar (South African National Editors' Forum)
Ashnah Kalemera (Collaboration on International ICT Policy in East and Southern Africa)
Hlengiwe Dube (University of Pretoria, Centre for Human Rights)
Lori Nordstrom (APC)

EDITORIAL TEAM
Izak Minaar (South African National Editors' Forum)
Avani Singh (ALT Advisory)
Veronica Ferrari (APC)

COPY EDITING AND PROOFREADING
Lori Nordstrom (APC)

PUBLICATION PRODUCTION AND SUPPORT
Cathy Chen (APC)

GRAPHIC DESIGN
Andrea Estefanía

Published by the African Declaration on Internet Rights and Freedoms Coalition
https://africaninternetrights.org
November 2020

ISBN 978-92-95113-35-0
APC-202011-CIPP-R-EN-DIGITAL-325

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

This publication is a compilation of 19 articles by African researchers, academics, journalists and human and digital rights activists on the impact of the COVID-19 pandemic on digital rights in Africa.

The articles were commissioned by the African Declaration on Internet Rights and Freedoms (AfDec) Coalition as part of its project on "Securing human rights online in Africa through a strong and active 'African Declaration on Internet Rights and Freedoms' network".[1] The AfDec Coalition is a pan-African initiative which promotes human rights standards and principles of openness in internet policy formulation and implementation on the continent, guided by the 13 principles established in the African Declaration on Internet Rights and Freedoms.[2]

At the time that the papers were commissioned, in June 2020, African states had either invoked existing policies or adopted new policies for prevention of spread, containment and treatment of the virus that had an impact on the enjoyment of digital rights. For example, most governments employed the use of contact tracing applications to track and trace citizens' movements and put in place measures criminalising free speech when it contained false information about the pandemic. These two examples had the potential to be abused, particularly the latter, which was used to silence journalists and government critics.

The pandemic also moved most citizens' communication, education, work, trade and access to basic services from physical interactions to primilary online interactions. However, the continent is still largely made up of informal economies, has a low internet penetration rate of 28.2%[3] (far below the global average of around 53%), and has seen an increase in reports of digital rights violations resulting from repressive cyberlaws, making the efforts to address the pandemic inadequate and inequitable.

These articles offer reflective analyses on government efforts to curb the COVID-19 pandemic from the perspective of the AfDec principles, with a focus on a number of the principles including privacy and personal data protection, gender equality, freedom of expression, internet access and affordability, and the right to development and access to knowledge. The articles trace trends in access to the internet by the general populace and marginal communities;

1 https://www.apc.org/en/project/securing-human-rights-online-africa-through-strong-and-active-african-declaration-internet

2 https://africaninternetrights.org/en/declaration

3 ITU. (2019). *Measuring digital development: Facts and figures 2019.* https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

affordability of accessing the internet; online learning initiatives; contact tracing and the handling of health data for official reports and aid; media freedom; and freedom of expression.

The articles offer recommendations for national and regional-level advocacy in response to emerging violations of online rights that will remain relevant even after the COVID-19 pandemic. Policy advocacy is one of the AfDec Coalition's key strategic areas, aimed at contributing to the Coalition's long-term goal of achieving national and regional internet-related policy frameworks that promote and respect human rights across Africa.

PRIVACY AND PERSONAL DATA PROTECTION

Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions

Author: Tomiwa Ilori

INTRODUCTION

Data protection in Africa can still be described to be in its nascent stage. Most African states do not have a data protection law. Countries on the continent are divided along the lines of countries with a data protection law, countries with fragmented frameworks, and countries without any semblance of a law. Out of the 55 states on the continent, only 28 countries have a data protection law, of which 15 have set up data protection authorities (DPAs) to enforce the law.[1]

The focus of this paper is two-fold. The first objective is to consider the status of data protection in Africa, while the second objective focuses on the impact of public emergencies like the COVID-19 pandemic on data protection in Africa. This is done by considering both international and national contexts on data protection in Africa. The countries being focused on are: Nigeria, Senegal, Uganda, Kenya, Morocco, Tunisia, South Africa and Mauritius. The choice of national contexts is premised on language and differences in legal systems across each of Africa's sub-regions.

The paper finds that the status of data protection in Africa is inadequate. This inadequacy is due to many reasons such as dependence of DPAs, financial constraints, lack of institutional capacity and others. These defects are further exacerbated by the COVID-19 pandemic, thereby increasing calls for privacy reforms in Africa. In order to correct these effects while also planning for future dynamics like the COVID-19 pandemic, solutions such as legislative reforms, fiscal viability and multistakeholder partnerships are proffered.

1 Dahir, A. L. (2018, 8 May). Africa isn't ready to protect its citizens personal data even as EU champions digital privacy. *Quartz*. https://qz.com/africa/1271756/africa-isnt-ready-to-protect-its-citizens-personal-data-even-as-eu-champions-digital-privacy; a repository of data protection laws in Africa is available at: https://dataprotection.africa

REGIONAL FRAMEWORK AND INSTRUMENTS

AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION (MALABO CONVENTION) 2014

The Malabo Convention sets a strong intention for the protection of personal data and ensuring cybersecurity in Africa.[2] The Convention seeks to establish a credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, and promotion of cybersecurity, e-governance and combating cybercrime.[3]

The Convention provides fair information principles, legal basis, and rights of data subjects recognised under other international instruments.[4] It also mandates member states to set up independent data protection authorities.[5] The Malabo Convention provides a personal data protection framework which African countries may potentially transpose into their national legislation for it to have the full force of the law, and encourages African countries to recognise the need for protecting personal data.[6] The Convention will come into effect 30 days after the 15th ratification by a member state.[7] Currently, it has been signed by 14 member states, ratified by five, and deposited to the African Union Commission by six out of 55 members states.[8]

AFRICAN DECLARATION ON INTERNET RIGHTS AND FREEDOMS

Though not a binding instrument, the African Declaration on Internet Rights and Freedoms has become a regional resource in terms of its policy direction and influence in Africa. The African Declaration emphasises the responsibility of African states to respect, protect and fulfil human rights online for all people.[9] It comprises 13 principles that aim to engender the promotion of fundamental rights of Africans on the internet. The eighth principle provides for privacy and data protection.

---

2 https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf; unlike the EU's General Data Protection Regulation (GDPR), which can be transposed nationally, the lawmaking process in Africa is different, which means Africa-wide instruments do not automatically take effect when in force.

3 Ibid.

4 Articles 13, 16-19.

5 Article 11.

6 Deloitte. (2017). *Privacy is Paramount: Personal Data Protection in Africa.* https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

7 Article 36

8 Status of adoption of the Malabo Convention as of 28 June 2019: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

9 https://africaninternetrights.org/wp-content/uploads/2015/11/African-Declaration-English-FINAL.pdf

The African Declaration restates that everyone has the right to privacy online, including the right to the protection of their personal data. The right extends to anonymous communication on the internet, and the use of appropriate technologies to ensure the security and anonymity of such communication. However, the right does not exist without restrictions, which must be subject to limitations provided by law, be recognised under international human rights law, and be necessary and proportionate in pursuance of a legitimate aim. The processing of personal data must be done with respect to the principles of data processing established under relevant data protection law.

The ninth principle of security, stability and resilience of the internet impacts data protection. Confidentiality and integrity are principles recognised under data protection laws. The Declaration extends to protection against unlawful surveillance, monitoring, unlawful interception of communication by both state and non-state actors and any measure that can undermine security and trust on the internet.

SADC MODEL LAW ON DATA PROTECTION, 2010

The Southern African Development Community (SADC) developed the model law in 2010 and adopted it in 2013 to promote the protection of human rights in member states. Its preamble acknowledges that the safeguarding of data protection rights aids the preservation of other rights like freedom of expression, movement and association. The model law mandates member states to create an independent data protection authority while also providing for its core mandates and duties and powers to impose sanctions.[10] The law establishes principles of data processing which include data minimisation, accuracy, storage limitations, lawfulness and fairness, purpose limitation and accountability.[11]

It also creates an obligation to notify the supervisory authority when there is a data breach without undue delay and to ensure the rights of data subjects.[12]

ECOWAS SUPPLEMENTARY ACT A/SA.1/01/10 ON PERSONAL DATA PROTECTION, 2010

The Economic Community of West African States (ECOWAS) Act gives member states direction on what should be provided for in their national data protection laws, while also urging member states to enact data protection laws without prejudice to the interest of the state.[13] The Act demands the setting up of an independent data protection authority by member states. Also, the Act creates

10 Articles 5, 3(5) and 9 of the SADC Model Law on Data Protection.

11 Articles 11, 12, 13 and 30 of the SADC Model Law on Data Protection.

12 Article 25 and Part 7 of the SADC Model Law on Data Protection. The data processor is expected to notify the data controller.

13 The ECOWAS member states are Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo. https://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf

Above: A woman raises the black power fist with the South African flag while wearing a facemask. Source: Thema Hadebe

a high threshold for protection of special categories of data like genetic data and health research, data relating to offences, sentences or security measures,biometric data, and data processed for public interest reasons.[14] It additionally sets out the guiding principles on processing of personal data.

The Act was signed by 13 countries. According to Greenleaf and Georges, this is the only binding regional data protection agreement yet in force in Africa. In addition, once this framework is completed, it may be enforced by the ECOWAS Court of Justice.[15]

EAC LEGAL FRAMEWORK FOR CYBERLAWS, 2008

The East African Community (EAC) Framework is divided into two parts. The first addresses thematic issues like electronic transactions and electronic signatures, cybercrime, data protection and privacy and consumer protection.[16] The second part addresses intellectual property, competition, e-taxation and information security. Framework I commenced in 2007 and was completed in 2008 and approved in 2010. Framework II started in 2010 and was completed in 2011, and approved in 2013. The implementation is still ongoing. Out of the five countries that are member states, only Kenya and Uganda have a proper data protection act. Rwanda has a splintered framework, while Burundi and Tanzania do not have adequate data protection law.[17]

14 Article 12 of the ECOWAS Supplementary Act on Personal Data Protection.

15 Greenleaf, G., & Georges, M. (2014). African regional privacy instruments: Their effects on harmonization. 132 Privacy Laws and Business International Report 19-21. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566724

16 http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y

17 The three countries have a data protection bill at different stages.

Above: A man's temperature is being measured with a thermometer gun while wearing a facemask. Source: Themba Hadebe

DECLARATION OF PRINCIPLES ON FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION IN AFRICA

Perhaps a more direct and binding instrument, the Declaration of Principles on Freedom of Expression and Access to Information in Africa is sourced from the African Charter on Human and Peoples' Rights (ACHPR). The ACHPR is the most primary human rights instrument in Africa, which all African countries are party to and obligated to abide by. Article 9 of the Charter provides for the right to freedom of expression and access to information, which has in turn produced more guidelines on both rights in the digital age.

Since the ACHPR does not provide for the right to privacy, and given the gaps that could be created by such a lacuna, especially in the digital age, the Declaration of Principles, together with the other above-mentioned instruments, further links Africa's most fundamental law on human rights to privacy rights. Principle 40 of the Declaration provides for the protection of people's personal information. Principles 41 and 42 address privacy and communication surveillance and establish the legal framework for the protection of personal information in Africa.

Principle 40 provides that there shall be no indiscriminate storage or sharing of a person's personal information. Sub-section 2 requires that communication surveillance shall only be authorised by law and such law must comply with international human rights law. The last part of the Principle mandates that such law must ensure prior authorisation by a judicial authority, due process, period of use, notification, transparency and an independent oversight mechanism.

Principle 41 focuses on the general scope of what a data protection legislation must protect. The provisions lay out how personal information must be handled, the rights of data subjects, notification, online harms, legal redress and oversight mechanisms.[18]

18 https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf

DATA PROTECTION LANDSCAPE IN AFRICA

The continent is divided along the line of countries with a framework, an insufficient framework, and no framework. In some instances, a country like Botswana has a data protection law but the law is yet to take effect, or yet to set up a data protection authority, or a combination of both. The divergent framework creates a fractured terrain for data protection and enforcement of the law across the continent.

However, the protection of the right is as good as the strength of the law. A good number of data protection laws in Africa are considered weak. As will be further discussed below, many countries like Nigeria, Senegal, Kenya and others do not have some key principles of data protection provided for in their respective framework.

This becomes even more evident with concerns around cross-border transfer of data. Most African countries' data protection law mandates the transfer of data to third party states only when the state is considered to have adequate data protection law to protect the rights of individuals. This would be a challenge as the continent looks to closer integration on trade through the African Continental Free Trade Agreement (AfCFTA).

In evaluating the strengths of the laws under focus, there would be recourse to international best practices and standards established under notable international instruments like the Modernised Convention 108+ of the Council of Europe, the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data,[19] the Asia-Pacific Economic Cooperation Privacy Framework,[20] the European Union General Data Protection Regulation (GDPR), the United Nations Guidelines Concerning Computerized Personal Data Files, and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).[21] Although there are common trends in the data protection laws, there are principles that differ significantly from country to country.

19 https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflow-sofpersonaldata.htm

20 https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

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

Table 1.

Key data protection issues	Senegal	Nigeria	Kenya	Uganda	Morocco	Tunisia	South Africa	Mauritius
Legislation (Status)	[23] ✓ (Enforced)	[24] ✓ (Enforced)	[25] ✓ (Not yet enforced)	[26] ✓ (Not yet enforced)	[27] ✓ (Enforced)	[28] ✓ (Enforced)	[29] ✓ (Partially enforced)	[30] ✓ (Enforced)
Rights of data subjects	✓	✓	✓	✓	✓	✓	✓	✓
Data protection principles	✓	✓	✓	✓	[31] ✓	✓	✓	✓
Legal basis for processing	✓	✓	✓	✓	✓	✓	✓	✓
Data security	✓	✓	✓	✓	✓	✓	✓	✓
Data breach notification	×	[32] ×	✓	✓	×	×	✓	✓
Cross-border data flow	✓	✓	✓	✓	[33] ✓	[34] ✓	[35] ✓	✓
Registration with supervisory authority	✓	×	✓	×	[36] ✓	✓	×	✓
Data protection impact assessment	×	[37] ×	✓	×	×	×	✓	✓
Privacy by design and default	×	×	✓	×	×	×	×	×
Appointment of data protection officer/information officer [38]	×	✓	✓	✓	×	×	×	✓
Supervisory authority	[39] ✓	[40] ✓	[41] ✓	[42] ✓	[43] ✓	[44] ✓	[45] ✓	[46] ✓
Remedies, enforcement and sanctions	✓	✓	✓	✓	✓	✓	✓	✓

As may be gleaned from Table 1, while all of the countries have data protection laws, in some the laws are not yet in force. Kenya and Uganda fall into this category. Also, while some are in force, they are not fully enforced. South Africa is an example of such a country.

Some countries do not provide for notification of breaches in their laws, and this includes Senegal, Nigeria, Morocco and Tunisia. Also, though not in force, only Kenya provides for privacy by design in its data protection framework. In addition to this, Senegal, Nigeria, Uganda, Morocco and Tunisia's laws do not provide for data protection impact assessment. These national contexts present a snapshot of the inadequacy of the data protection framework in Africa.

22 Law No. 2008-12.

23 Nigeria Data Protection Regulation.

24 Data Protection Act 2019.

CHALLENGES OF DATA PROTECTION IN AFRICA

In our assessment of the laws, it could be seen that even in the countries that have enacted a data protection law, the law is inadequate in protecting rights and other key data protection principles due to the challenges highlighted below.

DEPENDENCE OF DATA PROTECTION AUTHORITIES

The absence of full independence to discharge their duties limits the capability for enforcement. Our findings revealed that the constitution of some supervisory authorities is contrary to recognised international standards.[46]

As an example, the Nigerian data protection supervisory authority is an agency of the government, with members of the executive arm of the government constituting its governing board. This is contrary to articles 11(1)(b) and 11(1)(6) of the Malabo Convention,[47] which states that membership of the data-protection authority shall be incompatible with membership of government.[48]

---

25 Data Protection Act 2019.

26 Law No. 09-08 and Decree No. 2-09-165.

27 Organic Act No. 2004-63. The law is limited in application to private organisations. There is no obligation on public organisations.

28 Protection of Personal Information Act 2013.

29 Data Protection Act 2017.

30 Does not include data minimisation principle.

31 This was not addressed in the Regulation, but is mentioned in the Data Protection Draft Implementation Framework that is yet to be adopted.

32 Needs authorisation of the National Data Protection Commission (CNDP).

33 Needs authorisation of the CNDP.

34 Needs approval of the information regulator.

35 Prior to processing data, the National Authority for Protection of Personal Data (INPDP) must be notified.

36 This was not addressed in the Regulation, but mentioned in the Data Protection Draft Implementation Framework that is yet to be adopted.

37 The South Africa Protection of Personal Information Act refers to it as an information officer.

38 Commission of Personal Data (CDP).

39 National Information Technology Development Agency (NITDA).

40 Not yet set up. A data protection commissioner is yet to be appointed.

41 Not yet set up. It will be domiciled within the National Information Technology Authority (NITA). Its independence has been questioned.

42 Data Protection National Commission (CNDP).

43 National Authority for Protection of Personal Data (INPDP).

44 Information regulator.

45 Office of the Data Protection Commissioner.

46 In Uganda, though yet to be set up, the Office of the Privacy Commissioner is domiciled inside another government agency. The situation is the same in Kenya.

47 Nigeria is yet to sign and ratify the Convention.

48 See also Article 14(2) and 16 of ECOWAS Supplementary Act on Personal Data Protection, Article 16(5) of the Council of Europe Modernised Convention 108 and Article 52 of the EU General Data Protection Regulation.

In Mauritius, the DPA is materially and institutionally dependent on the Prime Minister's Office and is unable to administer fines to offenders. Similarly, in Ghana, the governing body of the DPA may receive ministerial directives on policy matters. The lack of independence would limit the effectiveness of the regulator.[49]

There are no immediately available best standard structures that ensure the independence of DPAs in Africa. What may, however, serve for introspection with respect to ensuring independence for DPAs in Africa will be what Senegal is currently seeking to do, which is legal reform to address the gaps identified since the law was passed in 2008.[50] While the proposed law does not address all of the problems identified in this section, it identifies the need to ensure more independence for the Commission on Personal Data.

FINANCIAL CONSTRAINTS

Lack of funding to exercise statutory functions will limit the capability of data protection regulators to ensure people's data protection rights. A poorly funded DPA will also lack the requisite resources to employ the best brains, conduct audits, investigate, issue sanctions effectively, and carry out other statutory functions. This could be partly responsible for why some countries have yet to set up their data protection authorities.

INADEQUACY AND LACK OF IMPLEMENTATION OF LAWS

Kenya, Uganda, Botswana, Equatorial Guinea, Seychelles and Madagascar are examples of countries that have passed laws and are yet to set up their DPAs. The absence of the regulator to enforce the law leaves data protection rights unprotected.

Also, there are countries that do not have any law on data protection, or inadequate law. As an example, Nigeria uses a secondary legislation and the president is yet to assent to the Data Protection Bill that was passed in 2019.[51] In contrast, countries like Tanzania, Sudan, Ethiopia, Libya and Djibouti do not have any law. The absence of law does not offer any protection to citizens of such a country. Similarly, such a country will be considered inadequate for transfer of data, which could impact trade and economy.

---

49 In July 2019, NITDA announced the investigation of the Nigeria Immigration Services over exposure of the passport page of a Nigerian citizen through its Twitter account. Almost a year on, it is yet to issue a sanction or go public with the status of the investigation. This Day. (2019,13 July). NITDA investigating banks, telcos, immigration for privacy rights violation. https://www.thisdaylive.com/index.php/2019/07/13/nitda-investigating-banks-telcos-immigration-for-privacy-rights-violations

50 Senegal Digital Strategy (2016-2025). https://www.sec.gouv.sn/sites/default/files/Stratégie%20Sénégal%20Numérique%202016-2025.pdf

51 The subsidiary legislation is weaker, compared to an Act of Parliament.

LACK OF INSTITUTIONAL CAPACITY

Data protection is a nascent development in the larger part of the continent. The regulators are still learning to bite, and would still need to invest in capacity development to function optimally. As an example, one year on after releasing the Nigeria Data Protection Regulation, the National Information and Technology Development Agency (NITDA) – the government agency that released the regulation – is yet to publish its Data Protection Draft Implementation Framework or issue any guide, guideline or guidance. A strong institution with independence and human capacity will aid the enforcement of data protection rights across the continent. According to a report by ID4Africa, DPAs in African jurisdictions currently range from as few as three to as many as 11.[52]

DUPLICATED AUTHORITIES

This is a problem in countries where data collection is done by multiple government authorities and where data protection laws are in sector-specific pockets. In Nigeria, the personal data of citizens is collected by multiple government agencies, and by extension, this makes those agencies regulators in respect of such data. Similarly, government agencies like the Federal Competition and Consumer Protection Commission and the Central Bank of Nigeria could have limited jurisdiction regulating data protection infringement. This, if not properly managed, could create overlaps and confusion.

LEGISLATIVE STANDARDS

The quality of law in some African countries is not in touch with modern reality on data protection. In Tunisia and Morocco, organisations need to submit requests to the regulator to transfer data outside the country. In Tunisia, the approval could take two months, and this could hurt digital trade that needs the mobility of data in real time. Similarly, in 2018, an EU delegation examined the Moroccan law and identified a number of shortcomings, such as the absence of references to biometric data or sexual orientation, no right to data portability, no detailed conditions related to the validity of consent, the lack of requirements to notify the authority of data breaches, the absence of a data minimisation principle, and limits of powers granted to the Moroccan data protection authority, the CNDP.[53]

It can be gleaned from the countries under focus that some do not have modern data protection measures like privacy by design and default, which only appeared in the Kenyan law. Data protection impact assessment is only present in the

52 ID4Africa. (2019). Roundtable of African Data Protection Authorities: Status and response to privacy risks in identity systems. https://www.id4africa.com/2019/files/RADPA2019_Report_Blog_En.pdf

53 Chenaoui, H. (2018, 11 September). Moroccan data protection law: Moving to align with EU data protection? *International Association of Privacy Professionals.* https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection

Kenyan and Mauritius law and absent in the four other countries.[54] Similarly, data breach notification is absent in the laws of Senegal, Tunisia and Morocco. Lastly, accountability from organisations is hampered when there is no legal obligation to appoint a data protection officer; Senegal, Morocco and Tunisia do not have such requirements.

COVID-19 AND DATA PROTECTION IN AFRICA

The outbreak of the novel cononavirus continues to strike the core of the world's existence, spreading along its trail pressured healthcare systems and devastating socioeconomic impacts.

Africa is not spared from the dispersion of the virus; the continent recorded its first case in February in Egypt.[55] On 11 March 2020, the World Health Organization declared COVID-19 a pandemic.[56] In containing, detecting, preventing and combating the virus, governments are imposing urgent measures. In Africa, 45 countries have introduced different legislative measures, and 37 countries have imposed various limitations on human rights.[57] Due to the measures that many countries have had to carry out against the pandemic, it has become necessary to ensure that such measures adhere to human rights protection, most especially, data protection.[58]

Combating the virus implies that the government may deploy a number of measures that could possibly impact on people's fundamental rights, and specifically data protection rights. Of the 18 African countries that had declared states of emergency in response to fighting the pandemic at the time of writing, only seven countries have data protection laws in force.[59] The effect of a state of emergency is the derogation of civil liberties until peace and order is restored. It is, however, not a blanket derogation of all liberties and rights. The enforcement of extreme measures is not grounds for total erosion of fundamental rights or unlimited suppression of rights and freedoms under the garb of public interests.

Protecting these rights becomes more important knowing the penchant of African states for information censorship, surveillance, excessive data retention,

54 Though this is contained in the Data Protection Draft Implementation Framework in Nigeria, the framework is yet to be adopted.

55 WHO. (2020, 25 February). A second COVID-19 case is confirmed in Africa. https://www.afro.who.int/news/second-covid-19-case-confirmed-africa

56 WHO. (2020, 11 March). WHO Director-General's opening remarks at the media briefing on COVID-19. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

57 The governments of Botswana, Sierra Leone and Senegal declared a public health emergency.

58 According to the United Nations, the pandemic is becoming a human rights crisis. United Nations. (2020). COVID-19 and Human Rights: We are all in this together. https://www.un.org/sites/un2.un.org/files/un_policy_brief_on_human_rights_and_covid_23_april_2020.pdf

59 These are Cape Verde, Côte d'Ivoire, Senegal, Botswana, Guinea, Angola and Equatorial Guinea.

interception of communication, and internet shutdowns. There is also fear of normalisation of some of the emergency measures currently adopted. Some of the emerging issues identified by the International Centre for Not-For-Profit Law (ICNL) are the limited oversight on the scope of emergency measures, the impact of emergency measures on vulnerable populations, the use of legislation that regulates freedom of expression and access to information, and the use of digital technologies during and post COVID-19.[60]

ADDRESSING COVID-19 AND THE IMPACT ON HUMAN RIGHTS

The emergency measures adopted by different African countries in combating the pandemic present an opportunity for violation of human rights. The imposition of full or partial restriction of movement and public gatherings impacts on the freedom of movement and association. The use of location-based data impacts on the right to privacy and data protection. Isolation and quarantining of patients impacts on the right to personal liberty. Addressing the public health crisis is one of the acceptable instances for restrictions and conditions where rights can be limited. However, countries like Malawi, Kenya, Nigeria, Zimbabwe and Rwanda have militarised the enforcement of limitations on public gatherings, resulting in killings, brutality and abuse of citizens.[61]

The United Nations (UN) Secretary General, in a recent address, declared the response taken by some countries as a human right crisis.[62] This is borne out of the fear that human rights could be suppressed under the garb of combating the virus. These measures could impact the rights of people when implemented without lawful safeguards. According to UN High Commissioner for Human Rights Michelle Bachelet:

> Emergency measures may well be needed to respond to this public health emergency. But an emergency situation is not a blank check to disregard human rights obligations. Emergency measures should be necessary and proportionate to meet that need. People should be fully informed about the emergency measures and told how long they will remain in effect. The enforcement of emergency measures needs to be applied fairly and humanely.[63]

60 African Government Responses to COVID-19: https://www.icnl.org/post/analysis/african-government-response-to-covid-19

61 There are also reports of suppression of journalists in Zimbabwe and Nigeria using "fake news" and cybercrime laws, respectively, to criminalise information against public officials in the frontline.

62 United Nations. (2020). Op. cit.

63 UN High Commissioner for Human Rights. (2020, 9 April). COVID is "a colossal test of leadership" requiring coordinated action. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25785&LangID=E

DATA PROTECTION AND THE RESPONSE TO COVID-19: IMPACT ON THE CONTINENT

In the light of the outbreak, some countries' data protection authorities have issued guidance, guidelines or some other policy direction, clearly laying out a blueprint for both public and private organisations on how to respect the data protection rights of their citizens. In countries with regulators but without guidance, the implication is that recourse will be made to the letters of the extant law to prevent abuse of data protection rights.

In contrast, countries with inadequate or non-existing law risk violations of the freedoms and rights of their citizens. The absence of a data protection law exposes them to gross abuse, indiscriminate surveillance, lack of transparency and accountability with processing of information, violation of their rights without redress, and other real or imminent risk.

Another challenge is the limited oversight of the procedures for processing information and the technology deployed, and exposure of vulnerable groups like refugees and the poor. According to the UN, it is important to factor in vulnerable persons while responding to the pandemic in order to adequately protect rights.[64]

MEASURES TAKEN BY AFRICAN DATA PROTECTION AUTHORITIES ON COVID-19

The data protection authorities in South Africa,[65] Mali,[66] Senegal,[67] Mauritius,[68] Morocco,[69] Tunisia,[70] Burkina Faso[71] and Nigeria[72] have issued guidance or state-

64 Ibid.

65 Information Regulator (South Africa). (2020). Guidance note on the processing of personal information in the management and containment of COVID-19 pandemic in terms of the protection of personal information ACT 4 of 2013 (POPIA). https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf

66 Niang, B. (2020, 1 April). Covid-19: the APDP's warnings on the collection of personal data and the protection of people's privacy. APDP. https://apdp.ml/covid-19-les-mises-en-garde-de-lapdp-sur-la-collecte-de-donnees-personnelles-et-la-protection-de-la-vie-privee-des-personnes

67 Commission de Protection des Données Personnelles. (2020, 24 April). "Press release: The protection of personal data in the context of the COVID-19 pandemic. https://www.cdp.sn/content/communique-sur-la-protection-des-donnees-personnelles-dans-le-contexte-de-la-pandemie-liee

68 Data Protection Office. (2020, 17 April). Guide on data protection for health data and artificial intelligence solutions in the context of the Covid-19 pandemic. http://dataprotection.govmu.org/English/Documents/Guide%20on%20Data%20Protection%20for%20health%20data%20and%20AI.pdf

69 Commission Nationale de Contrôle de Protection des Données à Caractère Personnel. (2020, 22 April). Press release of 04/22/2020. https://www.cndp.ma/fr/presse-et-media/communique-de-presse/668-communique-de-presse-du-22-04-2020.html

70 Instance Nationale de Protection des Données Personnelles. (2020, 27 March). Recommendations of the National Personal Data Protection Office relating to the protection of personal data in the COVID-19 period. https://globalprivacyassembly.org/wp-content/uploads/2020/04/COMMUNIQUE-DE-LINPDP-COVI D-19.pdf

71 Ouedraogo-Bonane, M. (2020, 4 April). Message from the CIL on the coronavirus pandemic (COVID-19). https://globalprivacyassembly.org/wp-content/uploads/2020/04/Message-de-la-CIL-CORRIGEcongo.pdf

72 IT Edge. (2020, 30 March). COVID-19 Data Collection Complies With NDPR, Says NITDA. http://itedgenews.ng/2020/03/30/covid-19-data-collection-complies-with-ndpr-says-nitda/

ments, urging both public and private organisations to be responsible with data processing. There is relative similarity in the approaches by governments – the minimum requirement is that data can only be used during this period according to the safeguards provided by law. Data must be processed lawfully and strictly for the purpose of combating the virus. Also, organisations are required to be accountable by processing personal information of data subjects in a responsible manner during the management of COVID-19 and to keep proper documentation,and take technical and organisational security measures to protect the data.[73] Data should only be stored for the duration of the pandemic, and can only be retained beyond the period for research, statistical or historical purposes.[74] Data can be used for other purposes if it is necessary to prevent a serious and imminent threat to public safety or public health. The Senegalese authority also urged that ethics should play a role.[75]

Health data is categorised as sensitive personal data and the processing prohibited subject to few exceptions. For example, in South Africa, under the recently published Guidance Note on the Processing of Personal Information in the Management and Containment of the COVID-19 Pandemic:

> [M]edical professionals, healthcare institutions or facilities or social services may process special personal information of a data subject, if such processing is necessary for the proper treatment and care of a data subject in the context of covid-19.[76]

On the legal basis for processing, public interest, vital interest, and existence of a legal obligation was a common thread. However, the South African Information Regulator included the legitimate interest of a controller or a third party. South Africa permits electronic communication service providers to provide the government with mobile location-based data of data subjects and the government can use such personal information in the management of the spread of COVID-19.[77] In Nigeria, the NITDA stated that the collection of information being carried out to address the spread of the virus is justifiable on the legal basis of vital interest and public interest, and conforms to the Nigerian data protection framework.[78] The regulator is yet to issue comprehensive guidance on the intersection of data protection and COVID-19.

---

73 The data should be archived or deleted after the pandemic.

74 Mauritius requires this to be documented in a record of processing activities.

75 Commission de Protection des Données Personnelles. (2020, 24 April). Op. cit.

76 Such as vital interest of the patient, public health, existence of legal obligation, etc. See generally Section 4.11.1 of the Guidance Note on the Processing of Personal Information in the Management and Containment of the COVID-19 Pandemic. https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf

77 The guidance allows the use of location data for mass surveillance to manage the spread of the virus, when such data is anonymised or de-identified.

78 IT Edge. (2020, 30 March). Op. cit.

DATA PROTECTION AND COVID-19 RESPONSE

Some of the technological measures deployed in the fight against the COVID-19 pandemic leverage on personal data and could impact on data protection. Under most data protection laws on the continent, health data, biometric data and genetics are considered sensitive personal data, whose processing is usually expressly prohibited, except in limited circumstances.[79] These circumstances include responding to public health crises, and when the data is processed under the vital interest or legitimate interest of a data subject.

In South Africa, telecom location data is being used to aid contact tracing.[80] In Nigeria, it was reported that the country's governors' forum is collaborating with one of the telecommunication companies on measures to combat the virus[81] and the Minister of Communications and Digital Economy was reported to have said that data mining of SIM cards and national biometric bank verification numbers will be used to determine the vulnerable population.[82]

A response without respect for lawful safeguards raises apprehension of excessive and long-term surveillance and its possible normalisation post COVID-19.[83] There is fear of discrimination without an avenue for accountability and the historical lack of transparency from the government.[84] The fear is aggravated with the number of African countries with poor human rights records, where the government is happy to justify the extreme measure of surveillance under the garb of public interest or national security. There is fear the pandemic could be used as a basis for the government to retain data beyond the pandemic and for other purposes including unlawful surveillance and discrimination.[85]

Responding to the crisis is not sufficient grounds to completely suppress the data protection rights of citizens. The discourse is not between public health or

79 Nigeria, Senegal, Burkina Faso, Kenya, Mauritius, etc.

80 Kahla, C. (2020, 26 March). SA government will be tracking mobile phones to curb COVID-19. *The South African.* https://www.thesouthafrican.com/news/government-tracking-mobile-phones-curb-covid-19/

81 Nigeria Communications Week. (2020, 7 April). Governors, MTN Partner to Halt Spread of COVID-19 with Data. https://www.nigeriacommunicationsweek.com.ng/governors-mtn-partner-to-halt-spread-of-covid-19-with-data

82 Adanikin, O. (2020, 24 April). COVID-19: Controversy trails Ministers' decision to mine data of phone users without consent. *International Centre for Investigative Reporting.* https://www.icirnigeria.org/covid-19-controversy-trails-ministers-decision-to-mine-data-of-phone-users-without-consent

83 Wintour, P. (2020, 23 April). Coronavirus pandemic is becoming a human rights crisis, UN warns. *The Guardian.* https://www.theguardian.com/world/2020/apr/23/coronavirus-pandemic-is-becoming-a-human-rights-crisis-un-warns

84 Ebert, I. (2020, 26 March). Commentary: Gathering data through COVID-19 tracking apps can result in discrimination & violations of the right to privacy. *Business and Human Rights Resource Centre.* https://www.business-humanrights.org/en/commentary-gathering-data-through-covid-19-tracking-apps-can-result-in-discrimination-violations-of-the-right-to-privacy

85 The prospective use of "immunity cards" could cause discrimination. Patel, N. V. (2020, 9 April). Why it's too early to start giving out "immunity passports". *MIT Technology Review.* https://www.technologyreview.com/2020/04/09/998974/immunity-passports-cornavirus-antibody-test-outside/

data protection, it is public health *and* data protection. The two extremes are fatal to the effort to combat the epidemic.

The fight against COVID-19 involves the collection and processing of vast amounts of personal data. Data protection laws do not hinder this processing, but require that it be done with appropriate legal bases and taking data protection principles into account. The pandemic is a public health crisis necessitating urgent measures to curb and eradicate it. Nonetheless, upholding data protection is equally crucial for the preservation of human rights before, during and after the pandemic. Governments must take every measure to preserve civic and democratic space and help to build and preserve trust in institutions. Measures

deployed must be non-intrusive, limited in time and purpose, and abide by the strictest protections and international human rights standard.[86]

RECOMMENDATIONS

LEGISLATIVE REFORM

Countries without legislation will need to enact a data protection law to prevent abuse and protect people. Countries with inadequate or old laws will need to modernise their laws to reflect the new norms and trends in international law. An archaic or inadequate law will remain insufficient in protecting people.

The enactment of the GDPR in Europe is quite commendable and there has been a clamour for a similar shift in Africa. Again, online risks are decentralised and ignore the maturity stage of infrastructure. Africa will need to integrate and harmonise its data protection laws to bring countries from the three categories to a common ground. The signing, ratification and transposition of the Malabo Convention or regional instrument should be the minimum requirement for such harmonisation. This has become more important as the continent is looking to integrate through a common market.[87]

COLLABORATION

Countries will need to collaborate on efforts to effectively strengthen the regulatory landscape on the continent. DPAs will need to develop intra-continental and, where necessary, international mechanisms for cooperation to facilitate an effective enforcement landscape and data protection. This could be by way

86 UN Sustainable Development Group. (2020). *Shared Responsibility, Global Solidarity: Responding to the socio-economic impacts of COVID-19.* https://www.un.org/sites/un2.un.org/files/sg_report_socio-economic_impact_of_covid19.pdf

87 As an example, Morocco has not considered any African country adequate for transfer of data. https://www.cndp.ma/images/deliberations/deliberation-n-236-2015-18-12-2015.pdf

of joint investigation, knowledge sharing and capacity building, notification, complaint referral, and other forms of mutually beneficial assistance.[88]

FISCAL VIABILITY

Financial constraints are among the challenges identified in the countries under consideration. While most data protection authorities are funded by the government, the authorities could explore innovative ways to limit financial dependency on an unwilling government. Inward funding through effective management of monies realised from implementing a data protection law could be an effective way of financing a DPA, for example. This model is a multistakeholder approach, wherein DPAs build stronger collaboration with research institutions and share human resources.

ACCEDING TO INTERNATIONAL INSTRUMENTS

More African countries need to accede to more international instruments on data protection and different regional instruments. Accession to these instruments will improve the quality of our laws, and bring them abreast with current reality. Ratifying Convention 108 would also ease a signatory state's consideration for an adequacy decision by the European Commission. The adequacy decision will ease the free flow of data and would facilitate transnational trade. Four African countries (Senegal, Tunisia, Mauritius and Cape Verde) have already ratified the Council of Europe Modernised Convention 108.[89]

Below: A man wears a facemask.
Source: Jandro Saayman

88 There is the Association of Francophone Data Protection Authorities (AFAPDP).

89 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=0MQrfqMP

STRENGTHENING INSTITUTIONS

An independent data protection authority is critical to the success of protecting personal data. A supervisory authority that is not independent may cause conflict of interests, will be ineffective and inefficient in enforcement, and would be subject to compromise from other arms of the government. The constitution and the workings of the DPA should be independent according to best practices and standards enunciated in international instruments.

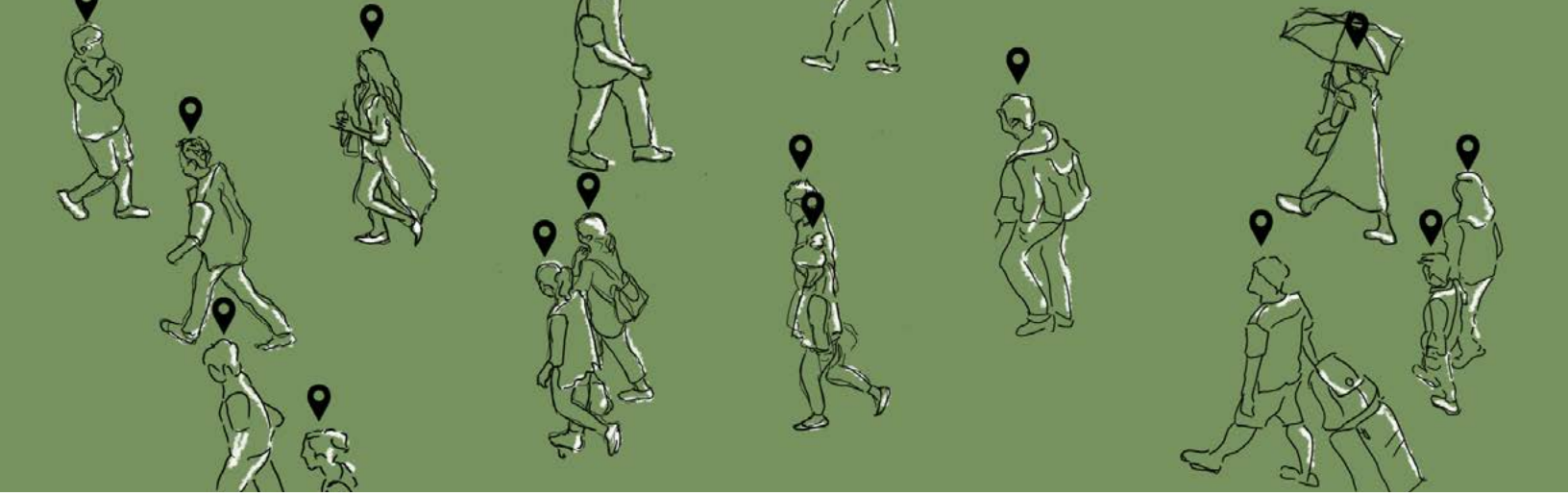
MULTISTAKEHOLDER APPROACH

The development of data protection in Africa is still ongoing. What this suggests is the need to maximise partnerships while also working towards effective implementation of a strong data protection landscape for Africa. Key stakeholders like governments, civil society, the private sector, academia and research and development need to work together. For example, one of the practical ways of implementing such an approach, especially given the current realities, is to establish ad-hoc multistakeholder committees with representatives of each key stakeholder mentioned above.[90] Not only does this ensure a level of transparency, it provides an avenue for accountability on data use and protection.

CONCLUSION

The risks posed by technology are many, especially given our realities. This paper considers these risks given the current status of data protection in Africa. It finds that the framework of protection is inadequate. These inadequacies have been highlighted and recommendations on how best to navigate them have also been proffered. What stands out prominently in the paper is how inadequate the data protection landscape is in Africa and how the fight against the COVID-19 pandemic may exacerbate the existing gaps and put data protection rights in danger. What will be required is a smart mix of ideas, and it is hoped that the issues discussed and solutions proffered will be further explored not only to improve data protection in Africa but also to respond to the current needs for protection during the COVID-19 pandemic.

90 Ilori, T., & Adeboye, A. (2020, 20 April). How to protect Nigerians' personal information while combating COVID-19. *Global Voices.* https://globalvoices.org/2020/04/20 how-to-protect-nigerians-personal-information-while-combating-covid-19



Can the social contract theory justify data rights violations? A review of South Africa's contact tracing regulations

Author: Rumbidzai Matamba and Chenai Chair | Country: South Africa

INTRODUCTION

We are slowly becoming aware of the proliferation of our data by different companies and entities across different sectors due to a data "spillage" as we access the digital conveniences and necessities of the world that we live in today. These companies and entities range from advertising, insurance, banking, and even government sectors. Companies and entities that have a significant influence on our quality of life, how we navigate the world today and how we are treated politically, socially and economically. While acknowledging that a simple search for the price of a laptop will result in being hounded by various laptop manufacturers and vendors, and having, inadvertently, let this become a running joke of the 21st century, we were not prepared for governments to utilise our data without our consent and to not have any legal recourse to this obvious violation of our right to privacy, as it is espoused in different international legal instruments and Principle 9 of the African Declaration of Internet Rights and Freedoms.[1]

The current pandemic has resulted in a need for solutions to "flatten the curve", including lockdowns and digital solutions such as contact tracing. The latter raises questions on the balance of privacy rights with public health data. This essay employs the use of the South African government's contact tracing initiatives in response to the COVID-19 pandemic and some public perceptions on these initiatives to assess whether the social contract theory can be employed as a tool to justify privacy violations for public health.

1 https://africaninternetrights.org/articles

BACKGROUND

As the second largest economy in sub-Saharan Africa,[2] South Africa is aaccess to communication services. Across its nine provinces, the highest percentage of households with access to cellular phones is 96.5% and the lowest is 77.1%.[3] Households with neither cellular phones nor landlines come in at a low 10.3%.[4] Over half of the population – 53% – make use of mobile internet, but the country's high data prices, the lack of internet-enabled devices and low digital literacy rates are barriers to internet use.[5]

African countries have been slow to adopt data protection regulations: only 14 out of the 54 countries on the continent have signed the African Union's Convention on Cyber Security and Personal Data Protection and only 25 countries have passed their own individual data protection laws.[6] South Africa's data protection law, the Protection of Personal Information Act 4 of 2013 (POPIA), is set to commence on 1 July 2020 with a one-year grace period for full compliance by companies.

Be that as it may, South Africa recognises the constitutional right to privacy. However, this right may be infringed where there are larger public interest considerations that outweigh the impact on privacy. Further, the lawful interception and monitoring of communications by law enforcement agencies is dealt with in separate legislation, the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (RICA),[7] although the contact tracing provisions passed have different objectives from RICA.

METHODOLOGY

The main premise this essay seeks to answer is whether an adage of Hobbes' social contract theory, that people are willing to give up certain rights and live according to a moral code if the remainder of their rights are guaranteed, can be used to justify the violation of online privacy rights. To do this, we conducted a desk review of the contact tracing initiatives employed by the South African government and sought public input on the conceivability of this theory through

2 Delport, J. (2020, 24 March). Africa's Top 10 wealthiest countries ranked by GDP. *ITNews*. https://www.itnewsafrica.com/2020/03/africas-top-10-wealthiest-countries-ranked-by-gdp

3 Independent Communications Authority of South Africa. (2019). *ICASA Annual Report 2019*. https://www.icasa.org.za/legislation-and-regulations/icasa-annual-report-2019

4 Ibid.

5 Research ICT Africa. (2018). *After Access: The State of ICT in South Africa*. https://researchictafrica.net/2018/09/10/state-of-ict-in-south-africa

6 Sylla, A., & Ford-Cox, A. (2019, 14 October). Overview of Data Protection Laws in Africa. *Hogan Lovells*. https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2#:~:text=Today%2C%20out%20of%2054%20countries,be%20on%20the%20legislative%20agenda

7 Several provisions in RICA were struck down by the high court in September 2019 after being found to be problematic to the extent the state was using the instrument to spy on citizens. See: amaBhungane. (2020, 19 February). Advocacy release: Concourt to hear amaB's Rica challenge. https://amabhungane.org/advocacy/advocacy-release-concourt-to-hear-amabs-rica-challenge

a short survey. This survey was in the form of a questionnaire, distributed online, in which 25 people responded to questions about whether they are aware of the South African government's contact tracing initiatives, whether they are aware of the POPIA and what their take is on the negotiation between their right to privacy and the need for contact tracing surveillance for the greater good. The survey is not representative of the South African population, nor may results be inferred. As such, we welcome any collaboration for further in-depth research on public perceptions on contact tracing initiatives. However, the survey provides insight relevant for the purposes of this study.

SOUTH AFRICAN COVID-19 RESPONSES AND HUMAN RIGHTS ONLINE

As the national lockdown began, the South African government passed regulations to address, prevent and combat the spread of COVID-19 under the Disaster Management Act 57 of 2002. Regulation 10 of this effort provides for the use by the Director General of Health of one's location and movement data, from their electronic communications service provider, without their informed consent, for inclusion in the South African COVID-19 tracing database.[8] This not only applies to one person, but to everyone that is presumed to have been in contact with them from the period during which the pandemic has been reported and is still active in South Africa, i.e. from March 2020 onwards.[9] Under these regulations, the data collected is used for contact tracing purposes only in response to the COVID-19 pandemic, and the data is to be retained for a period of six weeks after being obtained; thereafter it is to be destroyed.[10] The regulations further include transparency provisions in the form of safeguards to protect the right to privacy and give an oversight role to a retired Constitutional Court judge. The judge, appointed by the Minister of Justice, receives a weekly report stating the names and details of any person traced using the COVID-19 tracing database and provides oversight only on the tracing process. As of 3 April, it has been reported that 1,500 people's data has been shared to be used in the tracing database.[11]

Contact tracing is a supplement to on-the-ground testing and physically warding off COVID-19 through social distancing and constant washing and sanitising of hands. It presents governments with an opportunity to identify people who may have been exposed to COVID-19 and advise them to self-quarantine before they expose other people to the virus. In the survey we conducted as part of our research into public perceptions on contact tracing, 52% of the 25 respondents

8 Department of Cooperative Governance and Traditional Affairs. (2020). Disaster Management Act, 2002: Amendment of Regulations Issued in Terms of Sections 27(2). www.cogta.gov.za/?p=7871

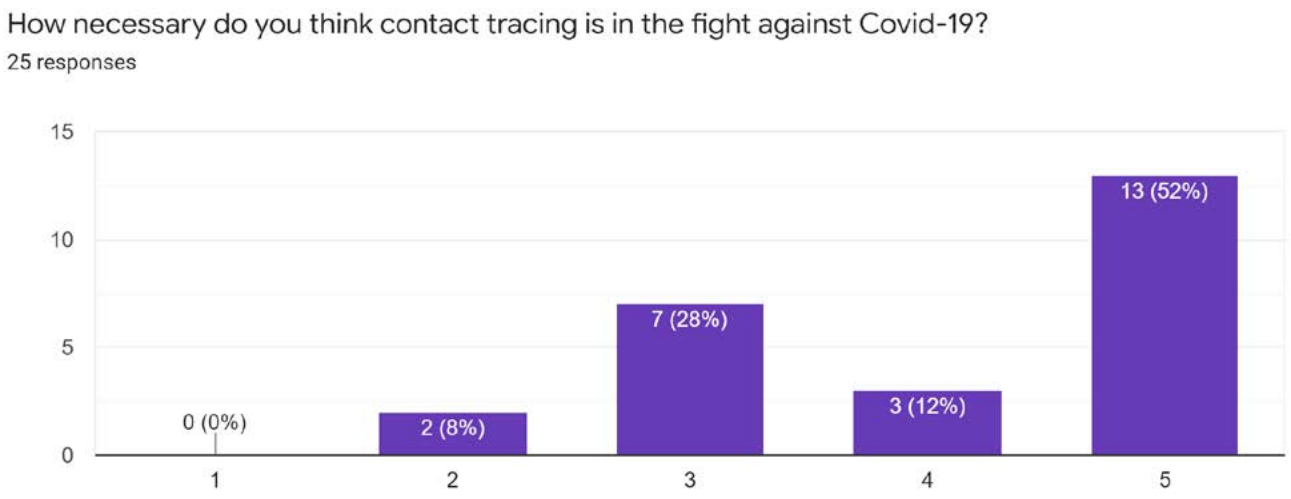
9 Ibid.

10 Ibid.

11 Gershgorn, D. (2020, 9 April). We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World. *OneZero*. https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9

felt contact tracing was necessary but still indicated that they worried about their right to privacy.

And rightfully so, because, as the Amabhungane Centre for Investigative



Above: Contact Tracing against Covid-19
Source: Chenai Chair | Rumbidzai Matamba

Journalism pointed out, the regulations are not entirely error-free.[12] For example, for the purposes of contact tracing, the interception of communications in the ordinary course of events is permitted, but there is no post-spying notification during the process. This means that anyone whose communication data has been intercepted is not alerted to this until six weeks after the national state of emergency has lapsed.[13] This provides ample opportunity for the system to be abused and for this abuse to go unnoticed.[14]

Furthermore, the regulations provide that the tracing database must be stripped of any identifying information, and the de-identified data may only be used for public health research going forward. However, there is no indication on whether the process of de-identifying the data will be monitored and who the responsible party for monitoring it will be. Storing data is also a fraught process – and these databases, filled with detailed personal data, might draw the attention of hackers before it has been de-anonymised.[15] Given several examples where encrypted data has been de-anonymised – for example, US President Donald Trump's location data was recently de-encrypted,[16] and the South African government

12 Hunter, M., & Thakur, C. (2020, 3 April). Advocacy: New Privacy Rules for Covid-19 Tracking a Step in the Right Direction, but.... *amaBhungane*. https://amabhungane.org/advocacy/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but

13 Ibid.

14 Ibid.

15 Wild, S. (2020, 5 May). COVID-19: Geolocation Tracking Fuels Concerns Around Privacy and Data Protection. *Africa Portal*. https://www.africaportal.org/features/covid-19-geolocation-tracking-concerns-privacy-data

16 Thompson, S. A., & Warzel, C. (2019, 20 December). How to Track President Trump. *The New York Times*. https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html

itself has been hacked before[17] – the implications of contact tracing on the right to privacy are dire.

The South African government has also approached other technology companies to identify suitable projects that may assist in its efforts against COVID-19. One such project is a partnership with the University of Cape Town to develop a smartphone app to assist the government with tracking people who may have come into contact with anyone who is COVID-19-positive.[18] The app is called Covi-ID and it has a GDPR-based privacy policy. Covi-ID also voluntarily submits to the data protection act (POPIA). The app is voluntary at this stage and requires personal information such as your COVID-19 status and your location. This information is stored on the user's phone using a technology called self-sovereign identity, which is not a centralised government or private sector database.[19] This means that the user has full authority and control over who can access their data, what they can access the data for, and how long they can have access to this data.[20] Additionally, the Department of Health also launched a WhatsApp-based symptom-reporting process which, unfortunately, does not set out any terms and conditions of use, information on who is processing the information, or where else it might be shared.[21]

Left: Covid-19 WhatsApp database Source: bloomberg.com/news/articles/2020-03-25/whatsapp-service-in-south-africa-goes-global-in-who-virus-fight

Although the POPIA is not yet in full force, the Information Regulator whose role is mandated by the act issued a guidance note to clarify the legality of the contact tracing provisions. The guidance note provides for the limitation of the right to privacy when enlisting the use of personal information of data subjects for the purposes of containing the COVID-19 virus.[22] The Information Regulator is of the opinion that these contact tracing initiatives do not violate POPIA provisions and that if anyone tests positive for COVID-19 they have a duty to share this information with the government

17 Kubheka, A. (2020, 18 March). Hackers Hit Government Websites. *IOL*. https://www.iol.co.za/dailynews/news/kwazulu-natal/hackers-hit-government-websites-45122121

18 Norton Rose Fulbright. (2020). *Contact tracing apps: A new world for data privacy.* https://www.nortonrosefulbright.com/en-za/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy

19 Georg, C. (2020, 5 April). Covi-ID: Privacy-Preserving COVID-19 Status Verification. *Medium*. https://medium.com/coviid/covi-id-privacy-preserving-covid-19-status-verification-c11d59ec92f6

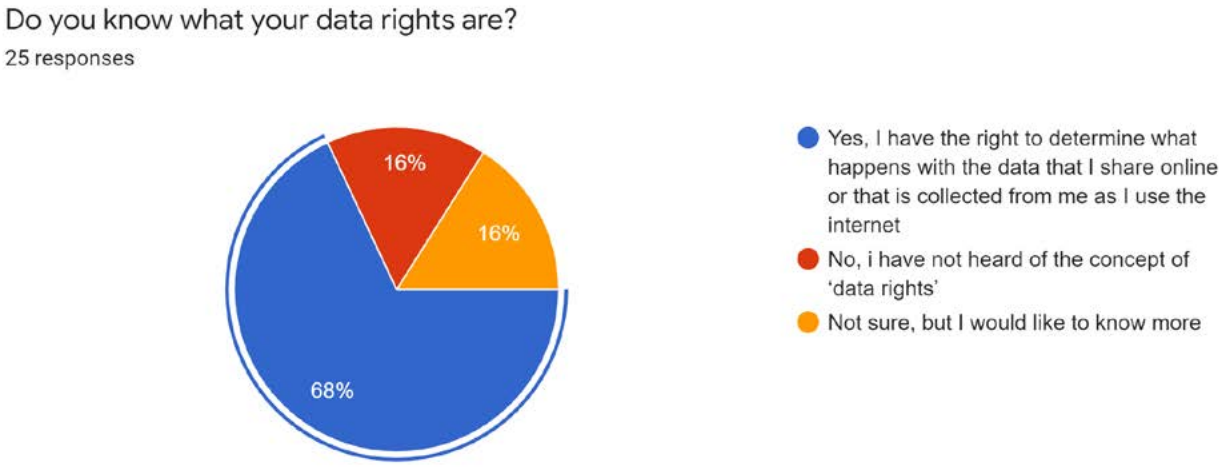
20 Ibid.

21 Norton Rose Fulbright. (2020). Op. cit.

22 Information Regulator (South Africa). (2020, 3 April). Guidance Note on the Processing of Personal Information in the Management and Containment of COVID-19 Pandemic in terms of the Protection of Personal Information Act 4 of 2013 (POPIA). https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf

so that it may act accordingly.[23]

While the Covi-ID app has in-built functions to protect the right to one's privacy, the WhatsApp initiative is lacking in that department, as one is not even aware of who they are sharing their information with. We note, at this point, that our survey results indicated that 32% of our respondents were not aware of their data rights. The ambiguity of the widely used WhatsApp database (it reached about 1.5 million users within the first week of use) highlights the need to have privacy by design, so that even where people are not aware of their rights, they are still protected. It is necessary that the right to privacy online is protected despite data subjects' awareness of this right.
Moreover, these two mobile initiatives also raise accessibility issues because, as noted above, 47% of the South African population does not have access



Above: Data Rights
Source: Chenai Chair | Rumbidzai Matamba

to the internet. Consequently, 47% of the population does not have access to the tech systems employed to mitigate COVID-19 by sharing important information relating to this pandemic. Therefore, the issue is not only the implications of these technologies on privacy rights; it extends to the right to not be discriminated against on the basis of one's socioeconomic status and the right to access to information. Another concern around the acquisition of people's data is "function creep", which is when data is collected for one reason and then used for another.[24] South Africa is not outside the realm of doing this, because it has shown an inclination towards humanitarian abuses, for example, 12 people have been killed by the police and the South African National Defence Forces since March 2020.[25] Critics worry that, while the

23 Ibid.

24 Wild, S. (2020, 5 May). Op. cit.

25 Karrim, A. (2020, 3 April). UPDATE | Lockdown: 3 die allegedly at the hands of the police. *News24*. https://www.news24.com/news24/southafrica/news/lockdown-number-of-deaths-from-police-action-rises-to-8-surpasses-sas-covid-19-casualties-20200403

data will initially be collected to track COVID-19, it will also be put to other uses, such as spying on political rivals, or be sold to companies.[26] Overall, there is no sense of ownership of our data – disembodying the data collected and increasing online rights violations.

A SOCIAL CONTRACT APPROACH TO BALANCING PRIVACY BREACHES FOR PUBLIC HEALTH DATA?

The internet has become an interplay between two tendencies: a necessary means of access and a tool used to constrain liberty and privacy. There are increasing calls for the right to privacy online to be ensured in internet governance.[27] While some contact tracing technologies are lightweight and temporary, others are pervasive and invasive and lean more towards constraining liberty and privacy.[28] For example, Chinese contact tracing technologies are more invasive, as they collect identity and location information as well as one's online payment history, so that they can watch for those who break quarantine rules.[29] South African contact tracing technology, as far as we know, can be classified as less pervasive, as it is only limited to identification and location data. However, as the COVID-19 pandemic rages on, technologists are rushing to build applications and services for contact tracing and the South African government has shown an interest in procuring these private technologies.

While the threat of further privacy violations can be mitigated by the regulations passed by the government, public and private technological companies are notorious for harvesting data, which the contact tracing initiatives have given them free reign over. The threat for further privacy violations does exist, and so the contact tracing initiatives present an opportunity to renegotiate the terms with which we use technology; how governments can regulate technology; and how governments and public or private corporations can cooperate for the trustworthy use of artificial intelligence and technology.[30] If this opportunity is not taken, we might observe a slow surrender of public liberties in the name of using surveillance technologies in the battle against COVID-19 and other potential novel viruses.[31]

---

26 Wild, S. (2020, 5 May). Op. cit.

27 African Declaration on Internet Rights and Freedoms Coalition. (2020). *Position Paper in Response to the Covid-19 Pandemic*. https://africaninternetrights.org/wp-content/uploads/2020/06/AfDec_COVID-19_Position-paper_Eng.pdf

28 O'Neill, P.H., Ryan-Mosley, T., & Johnson, B. (2020, 7 May). A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker

29 Ibid.

30 Louradour, S. (2020, 20 April). How to create a trustworthy COVID-19 tracking technology. *World Economic Forum*. https://www.weforum.org/agenda/2020/04/covid-19-coronavirus-tracking-technology

31 Ibid.

The social contract theory put forward by Hobbes in political philosophy posits that citizens give up a portion of their rights and live by a moral code for a guarantee of their remaining rights.[32] The South African constitution is a manifestation of the social contract theory, as it indoctrinates certain guaranteed rights in exchange for our rights to be self-serving and self-governing. Every society that has established norms has also established mechanisms to enforce those norms.[33] While contact tracing is a necessary tool in addressing COVID-19, these surveillance technologies can also be a very powerful tool of social control.[34] This is why societies tend to impose limits on the ability of authorities to place individuals under surveillance against their will or without their knowledge.[35]

The idea of a social contract to justify the violation of online rights stems from the realisation that increased ownership of our personal data does not guarantee us protection.[36] While we all have the right to, ordinarily, consent to the use of our data, the existence of this right has not protected us from national surveillance to address the current pandemic. The issue is not about how we can personally own our individual data and shut out others from accessing it, because our individual data on its own is not very useful, but when combined with other data it shapes societies and its impact varies across socioeconomic status, gender, ethnicity and religion.[37] For example, algorithms work by collecting vast amounts of data from numerous sources to create patterns and predict behaviour. That is why many of the problems around unfair uses of data cannot be solved by controlling who has access to it.[38]

The solution in the form of the social contract theory involves controlling not who has access to data, but how data is used morally, i.e. the use of data for our convenience and not to harm us. This is why the social contract theory works as justification for the violation of privacy rights online: the reassurance that what we give up as a collective is in exchange for the betterment of our navigation in the modern world, and during this pandemic, to protect and promote our right to good health.
The graph above indicates some willingness to renegotiate rights, and we are of the opinion that if we have more transparent systems in place, the public would be more comfortable with an exchange of the proportions brought about by the

32 Ginsberg, R. (1974). Kant and Hobbes on the Social Contract. *The Southwestern Journal of Philosophy*, *5*(1), 115-119.

33 K. N. C. (2019, 13 December). Surveillance is a fact of life, so make privacy a human right: Interview with Lawrence Capello. *The Economist*. https://www.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right

34 Ibid.

35 Ibid.

36 Tisne, M. (2018, 14 December). It's Time for a Bill of Data Rights. *MIT Technology Review*. https://www.technologyreview.com/2018/12/14/138615/its-time-for-a-bill-of-data-rights

37 Tisne, M. (2018, 14 December). Op. cit. and Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*. https://doi.org/10.1177%2F2053951717736335

38 Ibid.

Above: Contact Tracing and Privacy Rights
Source: Chenai Chair | Rumbidzai Matamba

contact tracing initiatives on the right to privacy. Much like how we exchanged the right to be self-governing for the rule of law.

This social contract would work in conjunction with government regulations because tech companies cannot be left to devise their own ethics. The idea is to have a balance of power that regulates this exchange, much like how the executive, judiciary and legislature operate to facilitate and protect the guarantees contained in the South African constitution. If we can achieve this, data rights cease to just be about privacy, but also encompass the right to securing a space for individual freedom and agency while participating in modern society without discrimination or fear of who is collecting your data and what it will be used for.[39]

CONCLUSION

Using South African contact tracing initiatives – their shortfalls and justifications – this essay drew on the social contract theory to assess whether it could be used to justify negotiating privacy rights for purposes of assuring public health. The conclusion is that the idea of a social contract, whereby one trades off certain rights for a guarantee of their remaining rights, is viable as illustrated through the trade-off of some data rights for contact tracing for the purposes of responding to a public health crisis. This gives us some insight into how we can justify the sometimes unavoidable use of our data without our consent, and the protections that must be put in place to justify the violations. Continuous research is needed to assess where the public stands with this trade-off on privacy for public health to ensure justification for the social contract theory approach.
While a new moral code is possible, a comprehensive solution between the public, public and private tech companies and the South African government is needed. It is highly recommended that the Director General of Health take a more

39 Tisne, M. (2018, 14 December). Op. cit. and Taylor, L. (2017). Op. cit.

decentralised approach when collecting the data for contact tracing and storing it for future use. This will mitigate the privacy concerns raised above. Therefore, one branch has to be tasked solely with collecting the data, another branch with de-identifying the data, and, perhaps, the information regulator overseeing these processes to limit privacy violations. It also requires transparency with the public and awareness raising of the process in play. A new social contract must be created, based on trust and cooperation and taking on a multistakeholder approach. For this, governments across the world must provide appropriate regulatory frameworks, which ensure that technologies are designed for use in ways that are compatible with, and for the advancement of, democracy.

Data protection in the age of technology-based disease surveillance

Author: Amanda Manyame | Country: South Africa

INTRODUCTION

Principle 8 of the African Declaration on Internet Rights and Freedoms[1] provides for the right to online privacy, including the protection of every person's personal data. Such a right and such protection have become necessary because of the uses of personal data and data in general. It used to be that a person's personal space was limited. However, emerging technologies have allowed for entities to make use of data and personal data in a manner that provides strategic advantages. This has been particularly true in the health sector and during the COVID-19 pandemic, during which technology-based surveillance has been used to curb the spread of the virus.

The most popular measure being adopted by countries to curb the spread of COVID-19 has been the use of personal and health data to trace and predict the spread of the disease. This is being done by making use of technology-based disease surveillance which has resulted in the over-disclosure of personal and health data about persons infected with COVID-19 and those they have come in contact with. This approach has resulted in the mass collection of personal data and the limitation of the right to privacy of individuals. It is, however, generally accepted that human rights may be limited, if such limitation is reasonable and proportional to the reason for the limitation.[2] This was reiterated in the United Nations Policy Brief titled "COVID-19 and Human Rights: We are all in this together".[3] It has also been generally accepted that the use of technology

1 https://africaninternetrights.org

2 Article 29 of the United Nations Declaration on Human Rights, 1948; Article 4 of the International Covenant on Civil and Political Rights, 1966; Section 36 of the Constitution of South Africa, 1996.

3 United Nations. (2020). *COVID-19 and Human Rights: We are all in this together.* https://www.un.org/sites/un2.un.org/files/un_policy_brief_on_human_rights_and_covid_23_april_2020.pdf

in response to COVID-19 must adhere to the principles of processing personal data, which include transparency, accountability, confidentiality and security.

Without data protection regulations or COVID-19 regulations that provide for these principles and enforcement thereof, the personal and health databases that are being created may be susceptible to abuse – and more so in instances where there is not adequate regulation of the destiny of these databases after the COVID-19 pandemic. This is the predicament that South Africa faces, with the recent announcement that the provisions in the 2013 Protection of Personal Information Act (POPIA) for the processing of personal data are only effective from 1 July 2020, with a 12-month grace period for compliance.[4]

Accordingly, this paper explores the adequacy of the COVID-19 regulations enacted in South Africa as they pertain to protection of the personal and health data being collected in an attempt to curb the spread of COVID-19.

THE IMPORTANCE OF YOUR DATA

In South Africa the right to privacy is protected in section 14 of the country's constitution.[5] Even before the codification of the right, it was recognised as forming part of a person's right to dignity. This is so because a person's privacy is closely associated to their right to dignity. However, over the years, the way in which the right to privacy is protected has evolved to not just provide for protection within a person's private space, but to include general protection of information about a person. This is so because of emerging technologies that make use of personal data in nearly every transaction[6] and in decision making to obtain a competitive edge.[7] Data has, thus, been termed the new oil.

It therefore comes as no surprise that personal and health data has been successfully used to predict the spread of contagious diseases such as severe acute respiratory syndrome (SARS), Middle East respiratory syndrome (MERS) and now COVID-19. Personal and health data is collected and combined into what is referred to as data sets. Quantitative analysis software, making use of artificial intelligence, machine learning and algorithmic computation, is used to, among other things, make predictions and conclusions from the data sets. This is known as big data analytics. Predictions drawn from making use of big data analysis are accurate, resulting in its use during pandemics to stop the spread of viruses like the one that causes COVID-19.

4 Presidency of the Republic of South Africa. (2020, 22 June). 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,-2013

5 https://www.justice.gov.za/legislation/constitution/index.html

6 Tene, O. (2011). Privacy: The new generations. *International Data Privacy Law, 1*(1), 15-27. https://doi.org/10.1093/idpl/ipq003

7 Brynjolfsson, E., Hitt, L., & Kim, H. (2011). Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance? *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486

However, because of the potential of these personal data sets, they are vulnerable and susceptible to cyberattacks, abuse and misuse, sometimes by the very entities that are responsible for these data sets. Consequently, to ensure that the personal data is used for its intended purpose, protected from abuse and with the data subject's privacy protected, meaningful accountability and consistent enforcement mechanisms have been developed in the form of data protection laws.

In South Africa, the POPIA data protection legislation was enacted for such a purpose. In terms of POPIA, public and private organisations that process personal data are required to do so in a lawful, accountable and transparent manner. Unfortunately, the relevant provisions of POPIA only came into effect on 1 July 2020, as announced by the Presidency on 21 June 2020.[8] This was after a national state of disaster had been declared and technology-based disease surveillance measures had been implemented. Furthermore, organisations processing personal data have 12 months from 1 July 2020 to comply with the collection, processing and storage provisions in POPIA. Consequently, a question arises of how personal data collected for the purposes of curbing COVID-19 will be protected for the duration of and after the national state of disaster.

CONTACT TRACING: THE MASS COLLECTION OF PERSONAL DATA DURING COVID-19

In South Africa, the commonly used measures to curb the spread of COVID-19 have been by way of collecting personal and health data and tracking and tracing the spread of the virus. The methods of collection that have been used to date include testing of individuals, identifying those that have contracted the virus, and gathering information about places these individuals have been to and people they have come in contact with.

This has been made possible by the declaration of a national state of disaster in terms of section 27 of the Disaster Management Act, 2002 (DMA).[9] The DMA provides for management policies that focus on reducing the risk of disasters like the COVID-19 pandemic. In terms of section 8(1) of the DMA, the National Disaster Management Centre was set up. The National Centre is empowered, in terms of section 18(1) of the DMA, to request information that is reasonably required by it for the purposes of providing it with adequate information on all aspects of COVID-19 so as to allow it to curb its spread. A requestee may not fail to comply with an information request from the National Centre. A failure to furnish the National Centre with the requested information may be reported to the Minister (a cabinet member designated by the president to administer the act), who must take the necessary steps to ensure compliance. Accordingly, the provision does not allow for failure to provide the information requested.

8 Presidency of the Republic of South Africa. (2020, 22 June). Op. cit.

9 http://www.cogta.gov.za/cgta_2016/wp-content/uploads/2016/06/DISASTER-MANAGEMENT-ACT.pdf

In addition, the DMA empowers the relevant authorities to issue regulations and directions to deal with a national disaster. Consequently, the Disaster Management Regulations, 2020[10] were issued, in terms of which the Electronic Communications, Postal and Broadcasting Directions, 2020 (Electronic Communications Directions)[11] were issued. The latter provided for tracking and tracing of persons. In terms of Direction 8.1, electronic communication network service licensees and electronic communication service licensees, as well as the internet and digital sector in general, are required to provide location-based services in collaboration with the relevant authorities identified to support designated departments to assist and combat the spread of COVID-19. Moreover, Direction 8.2 requires the South African Post Office to avail its national address system to assist the relevant authorities to track and trace individuals that have been infected or come in direct contact with infected persons. The South African Post Office's database may be correlated with other sources from the government or the private sector.

Although the Electronic Communications Directions do not provide for penalties for failure to comply with them, section 60(1) of the DMA provides that it is an offence to fail to comply with a request made by the National Disaster Management Centre in terms of section 18(1). Section 60(2) further provides that if convicted, the accused will be liable for a fine or imprisonment not exceeding six months or both.

In addition, sections 7 and 8 of the Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002 (RICA)[12] provide that state agencies are permitted to surveil citizens without an interception direction where the aim is to prevent serious bodily harm or determine a location during an emergency. An emergency is not defined in RICA. Furthermore, section 8(3) provides that telecommunication service providers must determine the location of the sender of a communication and furnish the details to law enforcement. Failure to comply with requests in terms of RICA also constitute an offence for which the telecommunications service provider or their employees will be liable for a fine or imprisonment. Accordingly, in its efforts to collect information necessary to inform its strategies to curb COVID-19, the National Disaster Management Centre may make requests for information in terms of RICA.

As the infection rate in South Africa rose, the Department of Co-operative Governance and Traditional Affairs (Department of Co-operative Governance) issued amended regulations so as to provide for contact tracing. According to Regulation 11H(2) of the Department of Co-operative Governance Regulations,[13] the National Department of Health is required to develop and maintain a database

10 https://www.gov.za/sites/default/files/gcis_document/202004/43258rg11098gon480s.pdf

11 https://www.gov.za/sites/default/files/gcis_document/202003/43164gon-417.pdf

12 https://www.justice.gov.za/legislation/acts/2002-070.pdf

13 https://www.gov.za/sites/default/files/gcis_document/202004/43199rg11078-gon446.pdf

to enable the tracing of "persons who are known or reasonably suspected to have come into contact with any person known or reasonably suspected to have contracted COVID-19." Regulation 11H(3) further provides for the information that should be included in the tracing database, which includes the individual's name, identity numbers and residential and other addresses where the individual could be located, and cellular phone numbers of all persons who have been tested for COVID-19, the COVID-19 test results of all such persons, as well as the details of the known or suspected contacts of any person who tested positive for COVID-19.

Moreover, Regulations 11H(6) and (7) require that when testing for COVID-19, the person testing is required to obtain as much information as is available at the time of testing and submit it to the Director General: Health, for inclusion into the tracing database. This information includes the above-mentioned information as well as a copy of the passport, driver's licence or identity book of the person tested. In addition, Regulation 11H(10) provides that the Director General: Health may in writing and without prior consent direct electronic communication service providers to provide it with the location or movements of any person known or reasonably suspected to have contracted COVID-19 and the location or movements of any person known or reasonably suspected to have come into contact with a person who has tested positive for COVID-19, during the period 5 March 2020 to the date on which the national state of disaster lapses or is terminated.

To feed the contact tracing database with the required information to combat COVID-19, personal and health data is being collected from security checkpoints between provinces where citizens are tested for COVID-19, and from workplaces where employers are required in terms of the Disaster Management Act: COVID-19 Occupational Health and Safety Measures in Workplaces, 2020[14] to provide a safe environment in workplaces, which has included reporting any cases of COVID-19 or suspected cases.

Hospitals and medical facilities that have any cases of COVID-19 are required to furnish this information to the Director General: Health. Also, the provincial Health Department in Gauteng added a COVID-19 feature to the Mpilo app,[15] allowing individuals to not only access information on COVID-19, but to self-check symptoms and provide location information to emergency medical services, if needed.

As can be seen from the regulatory measures stated above, there has been an unprecedented collection of personal and health data which will result in

14 https://www.gov.za/sites/default/files/gcis_document/202004/43257gon479.pdf

15 Molelekwa, T. (2019, 21 October). Mpilo app: Will using technology improve Gauteng's healthcare? *Health-e News*. https://health-e.org.za/2019/10/21/mpilo-app-will-using-technology-improve-gautengs-healthcare

the South African government possessing large data sets, during and after the pandemic and the national state of disaster.

To provide for the protection of this personal data, the Department of Co-operative Governance Regulations provides that the data forming part of the COVID-19 database is confidential and may not be disclosed without authorisation, unless the disclosure is necessary for fighting the spread of COVID-19. Also, this personal data is to be collected for a specific duration and is to be de-identified – only if it will be used for research, studying or teaching purposes – or deleted within six weeks of the termination or lapsing of the national state of disaster. In this way, the Department of Co-operative Governance Regulations ensures that the database is protected after the pandemic and national state of disaster.

However, the Regulations do not adequately address the illegal and biased exploitation of personal data. Such large data sets are susceptible to data breaches, as was the case with the Life Healthcare Group data breach that occurred on 9 June 2020.[16]

The Department of Co-operative Governance Regulations do not provide security measures that should be taken by the National Disaster Management Centre or the Health Department so as to ensure the protection of the tracing database. These security measures are provided for in POPIA, which organisations still have 12 months to comply with. Notwithstanding, the Information Regulator issued a guidance note[17] encouraging proactive compliance with POPIA.

Additionally, the Department of Co-operative Governance Regulations provide for oversight of the contact tracing, by requiring the appointment of a designated judge. However, the designated judge is merely required to receive weekly reports from the Director General: Health setting out the location information obtained from the electronic communications service providers. Although the designated judge is empowered to provide for further steps to ensure that the right to privacy is protected, she is yet to exercise this power. Consequently, there are no security measures to provide for security and protection against data breaches, maladministration, or misuse of the database.

The limitation on any human right is permissible only when it is necessary, reasonable and in pursuance of a legitimate aim. As this is this case in South Africa at the moment, it is arguable that the limitation placed on the right to privacy is reasonable and justifiable in terms of section 36 of the constitution, as well as in terms of international norms. It is, however, unsettling that the

16 Eyewitness News. (2020, 9 June). Life Healthcare Group hacked amid COVID-19 fight. *Eyewitness News*. https://ewn.co.za/2020/06/09/life-healthcare-group-hacked-amid-covid-19-fight

17 https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf

necessary safeguards and security measures that are provided for by data protection laws were not incorporated in the Department of Co-operative Governance Regulations or any other regulations.

Furthermore, data protection regulations establish that de-identified data is not personal data because it does not belong to an identifiable individual. It would therefore be prudent, in the fight against COVID-19, to regulate the processing of de-identified data after the national state of disaster has been terminated. It is important to regulate the processing of de-identified data because of the way that data in the information age can be used, going beyond the standard uses of aggregated data, presenting a higher possibility of the data being re-identified. This, therefore, calls for additional scrutiny of the requirement to de-identify the database. Moreover, there is a need to scrutinise the methods of aggregating data and third-party handling of aggregated data to minimise threats of de-identified data being misused.

Mass collection of personal data and surveillance of citizens interfere with and violate the right to privacy, unless if it for a justifiable reason. Nonetheless, organisations, including states, should frequently and regularly evaluate the context for the intended use of data and the purpose for which it is collected, created, stored, used, processed, disclosed or disseminated. The reason for the collection may be justified, reasonable and proportionate to the intended use, but measures have to be put in place to ensure that the right to privacy is protected, even when its enjoyment is limited. It should also be recognised that for the enjoyment of their right to privacy, individuals must be protected from unlawful surveillance by other individuals, private entities or institutions, including in their place of work or study and when using public internet access points.

That said, failing to make provision for the security of the contact tracing database, as well as addressing the potential of de-identified data being re-identified, is concerning.

CONCLUSION

Principle 8 of the African Declaration provides that the right to privacy includes the right to protection of personal data while online.

Furthermore, Principle 41 of the African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019[18] (ACHPR Declaration) states that laws providing for targeted surveillance of citizens' communications should also provide for adequate safeguards protecting the right to privacy. In addition, Principle 42 establishes

18 https://www.achpr.org/public/Document/file/English/Declaration of Principles on Freedom of Expression_ENG_2019.pdf

provisions that should be included in legal frameworks that provide for the protection of personal data, including mechanisms that ensure transparency, accountability, confidentiality and security.

As a result of COVID-19, states, South Africa included, have been collecting large amounts of personal data by making use of various methods, from physical collection of the data to the use of technology-based disease surveillance measures. The provisions of the ACHPR Declaration should be kept in mind because Principle 43 requires states to adopt, among other things, legislative measures to give effect to the ACHPR Declaration. According to Principle 43(3), states should provide detailed records of the measures implemented to comply with the ACHPR Declaration.

While the benefits of such mass collection and processing of data cannot be ignored, it is clear that international, regional and national data protection frameworks require transparent, accountable, confidential and secure methods of processing personal and health data to be used, so as to safeguard the right to privacy. With POPIA provisions coming into effect after the promulgation of the DMA Regulations, special provision should have been made for the transparent, accountable and secure processing of personal and health data during and after the national state of disaster.

To minimise the negative impact on data privacy, what is needed is data protection regulations that instil transparency, accountability, confidentiality and security into the ways in which the personal data is being used to curb the spread of COVID-19. Moreover, the principles of transparency, accountability, confidentiality and security should apply after the national state of disaster has been terminated. This is imperative because de-identified data can be re-identified, thereby leaving data subjects vulnerable to data privacy violations. There is also a need to provide for the protection of de-identified data to ensure that in its anonymised format, the right to privacy is still being protected.

Finally, there are benefits in disease surveillance for the government and its citizens of South Africa. The aggregation of the personal and health data is not only beneficial for curbing the spread of COVID-19, but it can lead to very deep insights that could prevent future health pandemics or improve health systems generally. As beneficial as it is, there is also potential of abuse of databases like South Africa's contact tracing database.

RESOURCE

For more information, see "Health and Medical Privacy", a presentation delivered during the 2012 Stanford Law Review Symposium co-sponsored by the Stanford Center for Internet and Society, at https://www.youtube.com/embed/ntL4WMGkiXo?feature=oembed

Surveillance numérique pour combattre la COVID-19 : Le droit à la vie privée et le droit à l'information en péril au Sénégal

Auteur : Ndiaga Gueye | Pays : Sénégal

INTRODUCTION

Pour lutter contre la COVID-19 de nombreux pays ont recours aux technologies numériques de surveillance des populations.

En effet, suite à la progression exponentielle du nombre de personnes porteuses de cette maladie, ayant comme conséquence une crise sanitaire mondiale, un nombre de plus en plus important de pays dans le monde prend des mesures liées aux technologies digitales pour mettre sous surveillance leur propre population en vue de stopper la propagation du virus.

Pour atteindre cet objectif, selon le contexte propre à chaque pays, des moyens juridiques et des modalités techniques variées sont mises en œuvre, soit pour vérifier le respect des mesures de quarantaine de certaines personnes infectées ne nécessitant pas de soins intensifs, soit pour découvrir le trajet de personnes ayant été en contact avec une personne diagnostiquée positive au coronavirus.

Parmi les technologies de surveillance numérique utilisée actuellement dans plusieurs pays dans le monde, il y a le « contact tracing » appelé aussi « back-tracking » ou traçage numérique.

Pour mieux comprendre cette technologie du traçage numérique, une présentation en sera faite dans un premier temps mais aussi les dispositions juridiques sur lesquelles peuvent s'appuyer les autorités sénégalaises pour justifier son utilisation pour retracer les cas contacts des personnes infectées à la COVID-19. Dans un second temps, une analyse de l'impact de l'utilisation du traçage numérique sur le droit à la vie privée et le droit à la protection des données à caractère personnel sera effectuée tout en relevant l'opacité gouvernementale sur cette question.

Enfin, dans une troisième partie, des recommandations sont formulées afin d'assurer une réponse du gouvernement du Sénégal à la COVID-19 en utilisant la surveillance numérique dans le respect des droits humains en ligne et hors ligne.

TRAÇAGE NUMÉRIQUE

Le traçage numérique consiste à collecter et traiter les données des appels téléphoniques et de géolocalisation des téléphones mobiles pour retracer les mouvements des individus testés positifs à la COVID-19.

Lorsque qu'une personne se déplace dans le cadre de ses activités quotidiennes, le signal émis par son téléphone mobile passe d'une antenne-relais à une autre. En s'appuyant sur le bordage de ce terminal les opérateurs sont en mesure de visualiser et suivre les déplacements de leurs clients.

Ainsi donc, pour repérer les personnes susceptibles d'avoir été exposées à un porteur du virus, les opérateurs de téléphonie mobile utilisent en effet des informations collectées grâce aux données personnelles de leurs clients et à la géolocalisation de leurs téléphones portables. Ils sont ainsi tracés et mis sous surveillance au quotidien.

Aussi, il est possible, non seulement d'identifier les personnes qui doivent être mises en quarantaine de toute urgence, car elles ont été en contact avec des individus porteurs du virus, mais aussi de détecter les zones à risque dans un pays où le virus pourrait se propager.

CADRE LÉGAL DE SURVEILLANCE NUMÉRIQUE

Pour utiliser un tel dispositif de traçage numérique au Sénégal, le ministère de la Santé transmet les informations sur les personnes testées positives au ministère de l'Intérieur qui s'appuie sur les opérateurs de téléphonie mobile pour identifier et localiser tous les cas suspects.

Les fondements juridiques ne font pas défaut au Sénégal pour justifier la mise en œuvre d'une telle stratégie numérique d'identification des personnes ayant été au contact de personnes infectées.

L'article 1er de la loi n° 2016-33 du 14 décembre 2016[1] relative aux Services de renseignement, votée dans le cadre de la lutte antiterroriste, dispose :

Les services de renseignement ont pour mission commune la recherche, le recueil, l'exploitation et la mise à la disposition des autorités de décision des renseignements relatifs aux menaces contre la sécurité et les intérêts fondamentaux de

1 http://www.jo.gouv.sn/spip.php?article10999

la Nation. Les besoins spécifiques et les priorités en matière de renseignement sont précisés dans un plan national de renseignement.

Cette disposition permet au gouvernement du Sénégal de surveiller la population pour notamment faire face aux menaces contre la sécurité et les intérêts fondamentaux de la Nation en mettant en œuvre l'article 10 de la loi sur le renseignement :

Les services spéciaux de renseignement peuvent, lorsqu'ils disposent d'indices relatifs à l'une des menaces prévues à l'article 2 et en l'absence de tout autre moyen, recourir à des procédés techniques, intrusifs, de surveillance ou de localisation pour recueillir les renseignements utiles à la neutralisation de la menace.

Même si une crise sanitaire n'est pas mentionnée explicitement, une menace contre les intérêts fondamentaux de la Nation peut justifier aux yeux du gouvernement du Sénégal le recours aux dispositifs techniques prévus par la disposition ci-dessus.

Cette disposition qui autorise la surveillance, est renforcée par l'article 90-11 et suivants de la loi n° 2016-30 du 08 novembre 2016 portant Code de procédure pénale[2] qui autorise le juge d'instruction ou l'officier de police judiciaire sur délégation judiciaire ou sur autorisation et sous le contrôle du procureur de la République à adresser des réquisitions aux opérateurs de télécommunications et aux fournisseurs de service ou de réseaux de télécommunications aux fins de communication de toutes informations utiles à l'enquête.

L'article 20 de la loi n°2018-28 du 12 décembre 2018 portant Code des Communications électroniques[3] va également dans le sens d'une légalisation de la surveillance numérique :

Conformément aux dispositions des articles 90-11 et suivants du code de procédure pénale, les opérateurs et fournisseurs de services sur demande des autorités judiciaires :

- Communiquent les données informatiques spécifiées en leur possession ou leur contrôle qui sont stockées dans un système informatique ou un support de stockage informatique ;

- Communiquent les données en leur possession ou sous leur contrôle relatives à leurs abonnés ;

2 https://www.sec.gouv.sn/sites/default/files/loisetdecrets/Loi%20n%C2%B0%202016-30%20du%2008%20novembre%202016%20modifiant%20la%20Loi%20n%C2%B0%2065-61%20du%2021%20juillet%201965%20portant%20Code%20de%20proc%C3%A8dure%20p%C3%A9nale.pdf

3 http://www.numerique.gouv.sn/mediatheque/documentation/loi-n%C2%B02018-28-du-12-d%C3%A9cembre-2018-portant-code-des-communications

- Répondent aux réquisitions aux fins de communication de toutes informations utiles à la manifestation de la vérité stockées dans le ou les systèmes informatiques qu'ils administrent.

Les opérateurs de communications électroniques et les fournisseurs de services ou de réseaux de communications électroniques sont tenus de mettre les informations requises à la disposition des autorités susmentionnées.

Cette collecte de données personnelles par la mise en œuvre de ce cadre légal serait de surcroît conforme à la loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel.[4]

En effet, les données de santé que révélerait une telle surveillance numérique des populations peuvent bien être traitées, d'abord pour le motif suivant : « le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou est effectué par une autorité publique ou est assigné par une autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées », article 41, alinéa 9. Ensuite, elles doivent être « nécessaires à la promotion et à la protection de la santé publique y compris le dépistage », article 43, alinéa 5. Et enfin, « lorsqu'il est nécessaire aux fins de médecine préventive, de diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit de son parent ou lorsque les services de santé agissent dans l'intérêt de la personne concernée. Les données sont traitées sous la surveillance d'un professionnel des soins de santé qui est soumis au secret professionnel », article 43, alinéa 8.

Ainsi donc, tous les éléments juridiques sont déjà mis en place pour permettre au gouvernement du Sénégal d'user de ces pouvoirs de surveillance pour identifier les personnes ayant été en contact avec les personnes porteuses du virus.

OPACITÉ GOUVERNEMENTALE

Toutefois, l'Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) n'a, à ce jour, aucune information officielle du gouvernement du Sénégal permettant d'affirmer l'utilisation de ces pouvoirs démesurés de surveillance des populations, conférés par l'Assemblée nationale depuis 2016, dans le cadre de la lutte contre la COVID-19.

Néanmoins, depuis le début de l'épidémie au Sénégal le 02 mars 2020, les autorités du ministère de la Santé communiquent sur le nombre de cas contacts qu'elles sont en train de suivre.

4 https://www.cdp.sn/content/loi-n%C2%B0-2008-12-du-25-janvier-2008-portant-sur-la-protection-des-donn%C3%A9es-%C3%A0-caract%C3%A8re

Aussi, l'annonce par le ministère de la Santé du Sénégal du nombre de cas contacts suivis, qui étaient de 1875 au 15 avril 2020[5], révèle que la stratégie du traçage numérique a été adoptée par les autorités, en sus, du suivi de contacts traditionnel basé sur l'interrogatoire de la personne infectée.

Pour procéder au traçage numérique, le ministère de la Santé du Sénégal transmet d'abord, la liste contenant les informations sur les personnes testées positives au ministère de l'Intérieur du Sénégal, à savoir, nom et prénom, numéro de téléphone mobile et adresse du domicile, ensuite ce dernier s'appuie sur les opérateurs de téléphonie mobile pour leur identification et leur localisation.

Aussi, se pose la question de la mise en place d'un tel dispositif de collecte et de traitement des données personnelles de géolocalisation à des fins de santé publique sans risquer un impact disproportionné sur les droits humains en ligne, en particulier, sur le droit à la vie privée et la protection des données à caractère personnel.

La Commission de Protection des Données Personnelles (CDP), qui est l'autorité au Sénégal en charge de l'application de la loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel, a publié un communiqué le 24 avril 2020 dans lequel elle rappelle que : « la situation actuelle d'urgence sanitaire, la protection des libertés individuelles et des droits fondamentaux, notamment la vie privée demeure applicable, et ne peut être suspendue. Cependant, des mesures dérogatoires respectueuses de la loi 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel ou d'autres dispositions législatives ou règlementaires applicables peuvent être envisagées ».

Dans son communiqué, la CDP n'a en fait que rappeler la légalité de la surveillance numérique au Sénégal. Elle n'a, à aucun moment, donné des informations sur les dispositifs et les techniques d'identification et de suivi des personnes infectées mises en œuvre par le gouvernement du Sénégal sur lesquelles elle a été consultée par les autorités.

La CDP a tout au plus souligné « que les solutions les moins intrusives pour la vie privée des personnes doivent toujours être privilégiées. Aussi, la Commission préconise que la dimension éthique soit systématiquement prise en charge par tous les acteurs engagés dans le processus de lutte contre le Covid-19 ».

Cette opacité gouvernementale sur les systèmes de surveillance numérique utilisés doit nous pousser à être particulièrement vigilants pour limiter le potentiel intrusif de ces dispositifs pour préserver l'équilibre entre les droits individuels et l'intérêt général.

5 https://twitter.com/MinisteredelaS1/status/1250535918324387845

Le manque de transparence du gouvernement du Sénégal sur les dispositifs techniques d'identification et de suivi des personnes infectées constitue une atteinte au droit à l'information, un des 13 principes de la Déclaration africaine des droits et libertés de l'internet[6].

Le principe 4 de la Déclaration africaine des droits et libertés de l'internet relatif au droit à l'information stipule :

> Tout individu a le droit d'accéder à l'information sur l'internet. L'internet doit être disponible de façon continue pour faciliter la libre circulation de l'information. Toute information, y compris celle générée par des activités de recherche scientifique et sociale, produite avec le soutien des fonds publics, doit être gratuitement accessible à tous.

En outre, il met en péril le droit à la vie privée et à la protection des données à caractère personnel de la Déclaration Africaine.

En effet, le principe 8 dispose :

> Toute personne a droit à la vie privée en ligne, notamment le droit de contrôler la façon dont ses données personnelles sont collectées, utilisées, divulguées, conservées et éliminées. Toute personne a le droit de
>
> communiquer anonymement sur l'Internet, et d'utiliser la technologie appropriée pour assurer une communication sécurisée, privée et anonyme. Le droit à la vie privée sur internet ne peut être soumis à aucune restriction, sauf celles prévues par la loi, pour un objectif légitime, qui sont nécessaires et proportionnées dans une société démocratique, conformément aux normes internationales en matière de droits de l'homme.

Les données collectées et traitées par l'utilisation de ces technologies de surveillance numérique sont des données de santé classées comme des données sensibles. Leur traitement est en principe interdit par la loi sur la protection des données personnelles au Sénégal.

Cependant, leur utilisation peut être légale pour motifs d'intérêt public avec le consentement des personnes concernées.

Répondre à cette double exigence légale est difficile dans le contexte africain, notamment au Sénégal en raison du manque de culture numérique de la population. En effet, le taux d'analphabétisme est élevé (55%)[7].

6 https://africaninternetrights.org/fr/declaration

7 www.ansd.sn/ressources/RGPHAE-2013/ressources/doc/pdf/3.pdf

Left: Sénégal et la Surveillance numérique
Source: ASUTIC

Par conséquent, il est sûr et évident que les citoyens ne seront pas en mesure de comprendre les principes de fonctionnement de ces technologies et les conséquences de leur utilisation sur leurs données personnelles et leur vie privée. Ainsi, ils ne pourront pas donner un consentement éclairé.

De plus, rien dans l'utilisation de ces technologies ne garantit l'anonymat, il y a donc toujours une possibilité d'être identifié. La non-protection des données personnelles des personnes permet de connaître la personne infectée par la COVID-19.

Ce sera une violation du droit à la vie privée, ce qui pourrait être une source de stigmatisation ou même de discrimination sociale. C'est un danger pour la cohésion sociale.

Le niveau de vigilance doit être élevé car le gouvernement du Sénégal n'informe jamais la population quant à la façon dont il utilise concrètement ce cadre légal de surveillance, une totale opacité est entretenue.

Par conséquent, il nous faut être très attentif à l'utilisation de ces dispositifs de dépistage afin d'éviter le risque d'entrer dans une nouvelle ère de surveillance numérique invasive des Sénégalais.

Le gouvernement du Sénégal doit s'engager à faire immédiatement la transparence sur toutes les mesures de surveillance numérique de la population mises en œuvre ou qu'il compte mettre en œuvre pour lutter contre la propagation de la COVID-19.
Ainsi, elles seraient dûment examinées par les citoyens pour limiter les risques d'abus qui découleraient des pouvoirs exorbitants que lui confère ce cadre légal en attendant que les lois votées depuis 2016 au Sénégal, attentatoires aux droits numériques[8], soient battues en brèche.

8 https://droitsnumeriques.sn/etat-des-lieux

Dans les principes fondamentaux de la société de l'information au Sénégal, celui de sécurité vise à garantir les droits fondamentaux des personnes et les droits sur les biens :

> Le principe de sécurité vise à établir la confiance de l'ensemble des acteurs dans l'organisation et le fonctionnement des infrastructures et des systèmes de la société de l'information. Il garantit les droits fondamentaux des personnes et les droits sur les biens et sauvegarde l'ordre public ainsi que les valeurs fondamentales de la société de l'information dans un environnement transparent et prévisible qui reflète la situation réelle du pays.
>
> La sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives.
>
> L'État a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre public, à la protection des personnes et des biens.
>
> Il associe à la politique de sécurité dans la société de l'information, les collectivités locales, les acteurs du secteur public comme privé et les organisations de la société civile, confrontés aux manifestations de la cybercriminalité sous toutes ses formes[9].

En d'autres termes, il ne peut être mis en place au Sénégal au nom de la sécurité un dispositif numérique qui remette en cause le respect du droit à la vie privée y compris la confidentialité des communications et la protection de leurs droits et libertés à l'égard de tout traitement de données à caractère personnel

Sur le fondement de cette exigence légale, ASUTIC, a procédé à la signature de la déclaration conjointe de la société civile[10], qui rappelle aux gouvernements

que le recours aux technologies de surveillance numérique pour combattre la pandémie doit se faire dans le respect des droits humains.

RECOMMANDATIONS

Au regard de tout ce qui précède, ASUTIC formule les recommandations suivantes au gouvernement du Sénégal dans l'utilisation de la surveillance numérique pour lutter contre la propagation de la COVID-19 dans le pays :

---

9 Article 6 de la Loi n° 2008-10 du 25 janvier 2008 portant loi d'orientation sur la Société de l'Information. http://www.jo.gouv.sn/spip.php?article6661

10 https://www.hrw.org/fr/news/2020/04/02/covid-19-declaration-conjointe-de-la-societe-civile

- Faire la transparence sur toutes les mesures de surveillance numérique de la population mises en œuvre ou qu'il compte mettre en œuvre pour lutter contre la propagation de la COVID-19, par le respect du droit à l'information consacré par la constitution du Sénégal;

- De se garder de penser que le numérique est la solution principale à la propagation du virus ;

- Recourir aux technologies de surveillance numérique dans le respect des droits humains, en particulier, le droit à la vie privée et à la protection des données à caractère personnel ;

- S'inspirer dans la lutte contre la COVID-19 du succès de pays démocratiques plutôt que de faire du copier-coller de mesures en provenance de pays totalitaires ayant des sociétés complètement différentes de la nôtre;

- D'associer à la politique de sécurité sanitaire de lutte contre la COVID-19 dans la société de l'information, les organisations de la société civile.

Privacy and the pandemic: An African response

Author: Gabriella Razzano

INTRODUCTION

COVID-19 has led to a surge of efforts by both state and private actors to manage the pandemic itself, and the consequences of it, with the aid of technology. Yet privacy has immediately been cast as a required trade-off in the efforts to combat the disease. Key examples of this are being seen in the introduction of contact tracing and related surveillance interventions, worldwide. These technologies are underpinned by the personal data of citizens. The jurisprudential tools that arise from human rights discourse (such as limitations tests) provide a powerful tool for ensuring human-centred concerns are forwarded within rapidly emerging contexts, and give a particular focus for interpreting the African experience. Looking to South Africa as an example, human rights frameworks will be used to demonstrate how both privacy and access to information can serve to provide the nuance needed in assessing contact tracing, locally.

BACKGROUND

From the early stages of the global pandemic, human rights activists have tracked contact tracing and related initiatives with the objective of monitoring for potential, and exacted, human rights abuses.[1] Digitalisation in response to disasters has of course in recent years increased substantially; this extends from big data and its analysis, to the use of technology to refine and improve processes such as contact tracing.[2]

Contact tracing is being promoted for the fight against COVID-19 for specific reasons. Vaccines will take significant time to develop and, until a vaccine is

1 Privacy International. (2020). Tracking the Global Response to COVID-19. https://privacyinternational.org/examples/tracking-global-response-covid-19

2 McDonald, S. (2016). *Ebola: A Big Data Disaster.* Centre for Internet and Society. https://cis-india.org/papers/ebola-a-big-data-disaster

widely available, the only "available infection prevention approaches are case isolation, contact tracing and quarantine, physical distancing, decontamination, and hygiene measures."[3] This is why technological solutions to contact tracing have been given such high priority.

A quantitative epidemiological study noted that, given the infectiousness of SARS-CoV-2, and with the sample data demonstrating the high level of transmission by *pre-symptomatic* patients, manual contact tracing is not sufficiently fast enough, and thus automated contact tracing should be preferred.[4] Yet, there are places that have been successful in combatting the disease without a focus on technology and with low costs. The state of Kerala in India and Vietnam, both of which also have pre-existing strong public health care systems, combatted COVID-19 successfully with a strong focus on primary health care.[5]

CONTACT TRACING TECHNOLOGIES

Often the discussions on human rights are obfuscated by the inclusion of technology – which is why attention should be paid to differentiating the types of technologies, and the purposes to which they are employed. Contact tracing focuses on tracking down those who have been exposed to a patient with COVID-19 as a method of prioritising testing and tracking the spread of the disease, which can be done both manually and/or aided by technology.[6]

States were the first to promote mobile applications with centralised data options for contact tracing. The Singapore government launched a voluntary application called TraceTogether, but it had an uptake of only 20% within the population.[7] That failure is significant, because the same study which advocated for automated contact tracing also noted that for such systems to have any efficacy, they would have to be adopted by a minimum of 65% of the relevant population.[8] Members of the public mainly stated a fear of state surveillance as being the reason for failing to download the application.[9] South Korea was

3 Ferretti, L., et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science, 368*(6491). https://doi.org/10.1126/science.abb6936

4 Ibid.

5 The Economist. (2020, 9 May). Vietnam and the Indian state of Kerala curbed covid-19 on the cheap. https://www.economist.com/asia/2020/05/09/vietnam-and-the-indian-state-of-kerala-curbed-covid-19-on-the-cheap

6 van Dyk, J. (2020, 26 March). Can you pause a pandemic? Inside the race to stop the spread of COVID-19 in South Africa. *Bhekisisa*. https://bhekisisa.org/features/2020-03-26-can-you-pause-a-pandemic-inside-the-race-to-stop-the-spread-of-covid19-in-south-africa

7 Criddle, C., & Kelion, L. (2020, 7 May). Coronavirus contact-tracing: World split between two types of app. *BBC*. https://www.bbc.com/news/technology-52355028

8 Ferretti, L., et al. (2020).Op. cit.

9 Sim, D., & Lim, K. (2020, 18 May). Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app? *South China Morning Post*. https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether

famously more successful in collecting mobile data centrally for contact tracing, but also had surveillance technologies directly in use.

Privacy concerns abound in solutions that centralise data at one point due to vulnerability and accountability. In terms of efficacy too, the reliance by African states on mobile technologies that require internet access presents a serious inhibition to efficacy where smartphone prevalence is not universal, and where data costs are prohibitive to constant online presence.[10] And there are other digital inequality risks: geolocation data from cellphone towers is less accurate in rural areas.[11] Particularly in the context of mobile phone data, there are ways to gain access to that data without a mobile application. States might approach telecommunication service providers directly for the data they hold on clients, which include geolocation points and call detail records.[12]

An alternative mobile phone solution, significantly driven by the private sector, are "peer-to-peer" solutions with decentralised data that focus strongly on Bluetooth. In such solutions, the data stays on a person's mobile device. Google and Apple collaborated to develop a shared contact tracing application programming interface (API), which means applications can be developed and made available to people through their mobile app stores. However, their protocols require the application developed to be decentralised, i.e. holding the data on the phone.[13] Many governments are seeking to amend their solutions to comply with this protocol (as availability through the store could improve voluntary uptake by citizens), though there are concerns that the designs may not adapt well.[14] This decentralisation is meant as a nod to privacy, though commentators have noted that the device manufacturers themselves do not have perfect privacy track records.[15]

HUMAN RIGHTS AND CONTACT TRACING

HUMAN RIGHTS LIMITATIONS

The principles of legality and proportionality have long had reference in international human rights law for understanding justifiable limitations of rights.

10 Gillwald, A., & Mothobi, O. (2019). *After Access 2018: A demand-side view of mobile Internet from 10 African countries*. Research ICT Africa. https://www.africaportal.org/documents/19044/2019_After-Access_Africa-Comparative-report.pdf

11 McDonald, S. (2016). Op. cit.

12 Oliver, N., et al. (2020). Mobile phone data and COVID-19: Missing an opportunity? *ArXiv:2003.12347*. https://arxiv.org/abs/2003.12347

13 Criddle, C., & Kelion, L. (2020, 7 May). Op. cit.

14 Ibid.

15 Kaye, D. (2020). *Disease pandemics and the freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/44/49&Lang=E; Mansell, R. (2020, 23 April). Coronavirus contact tracing apps – a proportionate response? *Media@LSE*. https://blogs.lse.ac.uk/medialse/2020/04/23/coronavirus-contact-tracing-apps-a-proportionate-response

Proportionality has been interpreted to include necessity and reasonableness,[16] though often it is referred to as a separate test for limitations.[17] These tests help challenge a false dichotomy that arises in much commentary, which pits privacy as competing against public health, and thus public health requiring "privacy trade-offs".[18] Human rights principles are designed specifically to consider the balance between "competing" interests, and a recognition that rights (whether to health or privacy) are not absolute.

These principles have already been used to assess specific contact tracing initiatives worldwide.[19] France's data protection watchdog, in considering the introduction of a voluntary contact tracing application called "StopCovid", considered many aspects of the application to be problematic. In particular, it held that "the invasion of privacy will be admissible in the present case only if [...] the Government can rely on sufficient evidence to have reasonable assurance that such a measure will be useful in managing the crisis."[20]

In other words, it considered the reasonableness, while also considering whether the measures were proportional to their intended purpose. Vitally, too, it highlights the importance of evidence (and sufficiency of evidence) for an inquiry into necessity.[21] The Israeli Supreme Court held that its version of contact tracing was not properly authorised by law.[22] While it doesn't appear as if there has been any direct litigation on contact tracing technologies in Africa, in a recent South African judgement, *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2019] ZAGPPHC 384, it was held that mass surveillance being performed in the country was unconstitutional because of the lack of express empowering legislation to do.

THE RIGHT TO PRIVACY

The right to privacy is at the forefront of conversations on contact tracing. In Africa, personal privacy was not prioritised previously as a rights area given

16 Cianciardo, J. (2009). The Principle of Proportionality: Its Dimensions and Limits. *ExpressO*. https://works.bepress.com/juan_cianciardo/1

17 Mansell, R. (2020, 23 April). Op. cit.

18 Servick, K. (2020, 22 March). Cellphone tracking could help stem the spread of coronavirus. Is privacy the price? *AAAS*. https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price

19 Renieris, E. M. (2020, 18 May). The Dangers of Blockchain-Enabled "Immunity Passports" for COVID-19. Medium. https://medium.com/berkman-klein-center/the-dangers-of-blockchain-enabled-immunity-passports-for-covid-19-5ff84cacb290

20 CNIL. (2020). Deliberation N°. 2020-046 of April 24, 2020 delivering an opinion on a proposed mobile application called "StopCovid". https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_april_24_2020_delivering_an_opinion_on_a_proposed_mobile_application_called_stopcovid.pdf

21 Renieris, E. M. (2020, 18 May). Op. cit.

22 Or-Hof, D., & Perelman-Farhi, R. (2020, 1 May). Striking the right balance: Government contact tracing powers and the right to privacy. *IAPP*. https://iapp.org/news/a/striking-the-right-balance-government-contact-tracing-powers-and-the-right-to-privacy

its association to individualised, rather than communal, rights.[23] However, the African Commission on Human and Peoples' Rights (ACHPR) has published a revised Declaration on Principles of Freedom of Expression and Access to Information in Africa, 2019, which now expressly recognises the protection of personal information as an aspect of the right to privacy.

In addition, most African countries' individual constitutions directly protect privacy, though not always in relation to information. The right to privacy for information and data is often given expression through specific data protection laws.[24] Thirty-three African countries have data protection laws that could be directly applied to their country contexts.[25] Laws that limit data processing by the public and private sector help directly prevent privacy harms against citizens. The emerging international rights regimes on data protection are largely principles-based, and those principles typically include:

- Collection limitation
- Purpose specification
- Use limitation
- Data quality
- Security safeguards
- Openness
- Accountability
- Data subject rights.

Principles that consider data minimisation at collection are particularly noteworthy for contact tracing contexts, with the ACHPR Declaration specifically noting in Article 42 that data collection must be "in accordance with the purpose for which it was collected, and adequate, relevant and not excessive." Consider, too, limitations on use *and* retention: just because collecting data may be necessary for a purpose does not mean that the retention of that data can outlast its purpose. The scientific study that promoted digital contact tracing as a necessity for combatting COVID-19 itself acknowledged that such activities should only create a "temporary record".[26]

However, once data is collected, it is hard to "reverse" this process. Deletion of records needs to be strictly monitored, and anonymisation of data can be challenging – de-identification will ordinarily not be enough, with studies specific

23 Boshe, P. (2017). *Data Protection Legal Reform in Africa*. Passau University.

24 Case law related to data privacy, and associated legislation, has been demonstrated in such high-profile cases as *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties)* [2020] eKLR (Kenya) and *Madhewoo v The State of Mauritius & Another* 2015 SCJ 177 (Mauritius).

25 Greenleaf, G., & Cottier, B. (2020). 2020 ends a decade of 62 new data privacy laws. *Privacy Laws & Business International Report,* 24-26. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611

26 Ferretti, L., et al. (2020).Op. cit.

to mobile phone data showing only four data points from a call detail record could be used to re-identify a person.[27]

Left:"Privacy need not be unduly sacrificed in pandemic responses if rights-based solutions are properly explored".
Source: Etienne Girardet on Unsplash

THE RIGHT OF ACCESS TO INFORMATION

While the right to privacy provides obvious parameters for limiting contact tracing initiatives, so too the right to access information provides important accountability parameters. The right of access to information has been supported by strong campaigns across the African continent.[28] Article 9 (1) of the African Charter on Human and Peoples' Rights states expressly that "[e]very individual shall have the right to receive information."Public accountability for the state authorisation and implementation of contact tracing applications must correspond with the provision of sufficient information about both the system itself, and its implementation.[29] Even the algorithm that underscores the contact tracing process should be transparent, as should associated modelling.[30] Ideally, particularly given the risks associated with surveillance, oversight of the implementation of contact tracing should be judicial – and this judicial oversight needs to have sufficient access to information, too.[31]

27 de Montjoye, Y.-A., Kendall, J., & Kerry, C. (2014). *Enabling Humanitarian Use of Mobile Phone Data*. Brookings Institute. https://www.brookings.edu/research/enabling-humanitarian-use-of-mobile-phone-data

28 See, for example, the African Platform on Access to Information: http://www.africanplatform.org

29 Mansell, R. (2020, 23 April). Op. cit.; Razzano, G. (2020, 25 May). Covid-19 – why a mysterious disease shouldn't result in mysterious decisions. *Daily Maverick*. https://www.dailymaverick.co.za/opinionista/2020-05-25-covid-19-why-a-mysterious-disease-shouldnt-result-in-mysterious-decisions

30 Ferretti, L., et al. (2020).Op. cit.; Razzano, G. (2020, 25 May). Op. cit.

31 Kaye, D. (2020). Op. cit.

Information is needed not just for accountability purposes, but also to support a citizen's right to make an informed decision.[32] The rights to data privacy and access to information thus support each other in the contact tracing context: high levels of public trust are required to ensure an *effective* level of uptake by citizens, and access to information forms a vital precursor for ensuring real consent. In the fight against the Ebola virus, mistrust in government information directly impeded contact tracing efforts.[33]

Provision of suitable access to information has an essential role within the public health context of COVID-19: the "goal in a public health crisis must be for government to provide accurate information."[34] Contact tracing can certainly contribute to these ambitions by assisting in creating the data and evidence base for making public health decisions, but only if supported by a fully rights-respecting design and implementation.

APPLICATION TO SOUTH AFRICA

On 15 March 2020, South Africa declared a national state of disaster, which allowed for the passing of regulations to help manage the COVID-19 pandemic. Initial regulations, scant on details about a possible contact tracing solution, were quickly amended on 2 April 2020 (Disaster Management Act, 2002: Amendment of Regulations, 2020). These regulations outlined the South African government's main solution to contact tracing as being expanded powers for the health authorities to obtain geolocation data and personal identifiers of any person who is reasonably suspected to have contracted COVID-19, or who has come into contact with someone who has COVID-19, directly from telecommunication service providers (and without a court order).[35] This information is then fed into a contact tracing database held by the Department of Health (DOH), for which the Director-General is responsible. Though no order is required to collect the data, a respected former Constitutional Court judge, Justice Kate O'Regan, was appointed as the designated COVID-19 judge to monitor the collection and use of location data for the contact database.[36] Considered in terms of privacy and data protection, the dramatic delays in enacting South Africa's Protection of Personal Information Act, 2013 (POPIA) are highly problematic. POPIA created an Information Regulator, who has been in position since December 2016. Yet the main sections of the Act have only just recently been made operational from 1 July 2020. This operationalisation gives both public and private sector data processors a full year to become fully

32 Mansell, R. (2020, 23 April). Op. cit.

33 McDonald, S. (2016). Op. cit.

34 Kaye, D. (2020). Op. cit.

35 Gillwald, A., Rens, A., van der Spuy, A., & Razzano, G. (2020, 27 April). Mobile phone data is useful in coronavirus battle. But are people protected enough? *The Conversation*. https://theconversation.com/mobile-phone-data-is-useful-in-coronavirus-battle-but-are-people-protected-enough-136404

36 Ibid.

compliant from that date. The regulations make no reference to the Information Regulator or POPIA, probably as a result of the fact that when they were passed, POPIA was not yet fully enacted.[37] This means that, at one of the most pivotal moments in South Africa's data privacy history, the only office with the requisite insight and powers – and in the South African case, a dual mandate between access to information and privacy – is excluded from the implementation and accountability processes.

Nevertheless, data protection principles provide a useful frame for understanding the regulations. There is purpose limitation: data may only be collected, used and disclosed by authorised persons for the purposes of addressing, preventing or combatting the spread of COVID-19 through the contact tracing process for the tracing database.

There is also at least allusion to keeping the data secure: the regulations require the information to be kept "confidential". Unlike other countries which have centralised the data with security agencies, thus increasing concerns of abuse of data for surveillance purposes, the database vests with the DOH.[38] However, the agency itself does not have an impervious data protection record.[39] This highlights the need for effective accountability, and this is where key challenges emerge. While the Director-General provides weekly reports to the designated judge, this doesn't automatically provide her with direct access to the database – the key information necessary for properly informing oversight.[40]

The duration of the lawful data retention terminates with the end of the national state of disaster, though de-identified data will be retained. The ability of the state to effectively and authentically de-identify thus becomes of immense concern.[41] Sufficient access to information has to be provided not just to the overseeing judge, but in terms of records management to ensure purpose specification was complied with.[42] This is aided by the partial nod provided to direct data subject rights by the regulations, which require that every person whose information was obtained be notified of such within six weeks of the national state of disaster lapsing. It is not clear, however, why the regulations do not require alerting data subjects simultaneously as the data is collected, particularly as the purpose is for contact tracing rather than surveillance.

37 Ibid.

38 Wild, S. (2020, 12 May). Antipoaching Tech Tracks COVID-19 Flare-Ups in South Africa. *Scientific American*. https://www.scientificamerican.com/article/antipoaching-tech-tracks-covid-19-flare-ups-in-south-africa

39 Bateman, B. (2019, 11 March). Exclusive: National Health Lab Services is sharing patient records. *EWN*. https://ewn.co.za/2019/03/11/exclusive-national-health-lab-services-accused-of-unlawfully-sharing-patient-records

40 Gillwald, A., Rens, A., van der Spuy, A., & Razzano, G. (2020, 27 April). Op. cit.

41 de Montjoye, Y.-A., Kendall, J., & Kerry, C. (2014). Op. cit.

42 Kaye, D. (2020). Op. cit.

Data opportunism is always a concern in a large-scale data collection exercise. In terms of the abuse of this data for surveillance, real questions will concern that defined purpose: can we be assured the data will not be handed over to the security agencies for monitoring quarantine surveillance, for instance? Again, this is why accountability and access to information must be prioritised in both the drafting of the regulations, but also in the practice of their implementation.[43] Privacy implications are best understood in the context of both the technology concerned and the implementation reality.[44] The South African state is not seeking, currently, to institute a mobile application. Instead, the contact tracing database seeks to support manual tracing exercises, which currently rely on 60,000 health care workers who go door to door asking for symptoms.[45] In addition, primary health care workers and responders manually collate contact tracing details from patients that test positive, and businesses are beginning to collate contact tracing details as lockdown lifts. It is therefore important to remember that it is not the use of technology itself which threatens privacy – it is the nature of personal data, with the technology amplifying some of the risks. There has already been the report of a woman in the United States being stalked by an employee of a business to which she was required to hand over her personal data, without technology interceding.[46]

That broader data protection principles are not currently fully enforceable in a country where the mass collection of data is being actively driven by the state is a serious concern. While the regulations commit to limiting the retention of the data, it is worth noting that in the past, serious questions have been raised about the efficacy of the South African government's disease surveillance in practice – highlighting questions on the efficacy of the programme being instituted.[47] The proportionality and necessity of the government's response will become clearer with implementation, and with due consideration to both access to information and privacy.

CONCLUSION

Human rights provide an essential frame for considering contact tracing initiatives in the African context. Privacy, a right of increasing relevance in African human rights jurisprudence, need not be sacrificed for an effective fight against

43 Ibid.

44 Nissenbaum, H. (2009). *Privacy in Context*. Stanford University Press.

45 van Dyk, J. (2020, 26 March). Op. cit.

46 Vaas, L. (2020, 14 May). Woman stalked by sandwich server via her COVID-19 contact tracing info. *Naked Security*. https://nakedsecurity.sophos.com/2020/05/14/woman-stalked-by-sandwich-server-via-her-covid-19-contact-tracing-info

47 Benson, F. G., Musekiwa, A., Blumberg, L., & Rispel, L. C. (2016). Survey of the perceptions of key stakeholders on the attributes of the South African Notifiable Diseases Surveillance System. *BMC Public Health, 16*, 1120. https://doi.org/10.1186/s12889-016-3781-7

COVID-19. Instead, ensuring the interventions promote access to information, privacy and other rights should be a priority for contact tracing implementers to ensure public trust (and uptake). As one commentator noted: "You manage an epidemic by being more open, more democratic and allowing for critical review and comment."[48] When technology is considered outside of context, techno-centrism threatens to steamroll rights. This is especially because of the increasing reliance of such technologies on big (and personal) data. Yet considering proportionality and necessity, this techno-centrism itself – given digital inequalities – threatens the justifications for many contact tracing initiatives in our country contexts. Civil society actors seeking to assess contact tracing initiatives being proposed domestically should be guided first by defining technologies proposed in detail, as well as the intersections explored in this paper, to consider the real privacy risks in context.

Emerging African jurisprudence on privacy has focused strongly on legality and lawfulness. This lends support to activism to promote the adoption of principles-based data protection legal regimes. Importantly, too, as emerges from the examples considered, these data protection regimes must be complied with by both the state and private actors, as both have mass data collection incentives.

The South African case study in particular raises a very specific recommendation for the promotion of new contact tracing intervention: the role of data protection authorities should be prioritised. To not do so, is to fail to place these emergency responses within the strong controls that are beginning to emerge on personal privacy protection.

48 Wild, S. (2020, 12 May). Op. cit.

GENDER EQUALITY, MARGINALISED GROUPS AND DIGITAL RIGHTS

Tackling gender-based cyber violence against women and girls in Malawi amidst the COVID-19 pandemic

Author: Donald Flywell Malanga | Country: Malawi

INTRODUCTION

Gender-based violence against women and girls remains a global threat to the public health of women and girls during emergencies.[1] As the COVID-19 pandemic deepens the economic and social stress, coupled with restricted movement and social isolation measures, gender-based violence against women and girls is increasing exponentially. Prior studies suggest that one in three women worldwide have experienced some form of gender-based violence in their lifetime.[2]

Likewise, during COVID-19, as more women and girls turn to the use of the internet, mobile phones, social media and other digital platforms for sharing information, these technologies have also become a weapon against them. Emerging data shows that women and girls are subjected to various forms of gender-based cyber (online) violence. This refers to online behaviour targeting women and girls, intended to intimidate, to coerce, or to cause fear, anxiety, humiliation and extreme emotional distress.[3] A United Nations (UN) report indicates that cyber violence is just as damaging to women and girls as physical violence, and estimates that 73% of women have endured cyber violence and are 27 times more likely than men to be harassed online.[4]

---

1 WHO. (2020). *COVID-19 and violence against women: What the health sector/system can do*. https://apps.who.int/iris/bitstream/handle/10665/331699/WHO-SRH-20.04-eng.pdf

2 UN Broadband Commission for Digital Development. (2015). *Cyber Violence against Women and Girls: A world-wide wake-up call (Executive summary)*. https://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf

3 Inter-Parliamentary Union. (2015). *Countering cyber violence against women*. http://archive.ipu.org/splz-e/csw15/cyber.pdf

4 Maundu, C. (2020, 29 May). Online violence in times of COVID-19. *KICTANet*. https://www.kictanet.or.ke/online-violence-in-times-of-covid-19

While efforts to tackle gender-based cyber violence during COVID-19 are at a larger scale globally, it remains an extensive and widely under-reported online human rights violation in African countries, including Malawi. Besides, most available literature is limited to developed countries, while similar studies are lacking in Malawi. Therefore, drawing on the Technology-Facilitated Gender-Based Violence Framework,[5] the key objectives of this report are to document the form(s) of gender-based cyber violence behaviours that women and girls experience during COVID-19, and identify responses/strategies available to tackle this type of violence during the COVID-19 pandemic.

COUNTRY CONTEXT

Malawi gained its independence from Great Britain in 1964. The country has an estimated population of 17.7 million people, of which 85% live in rural areas.[6] The gross domestic product per capita is USD 411.[7] 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. The overall mobile penetration is estimated at 45.5% while internet penetration is 6.5%.[8] About 34.5% of women own a mobile phone, 0.6% own a desktop computer, 1.8% own a laptop, while just 4.7 % of them have access to the internet.[9] The low rate of information and communication technology (ICT) penetration in Malawi is attributed the country's weak economy, high value-added tax (VAT) imposed on importation of ICT gadgets, and other contextual factors.[10]

GENDER-BASED VIOLENCE SITUATION IN MALAWI

Section 24 of Malawi's constitution stipulates that "women and girls have the right to full and equal protection by the law, [and] have the right not to be discriminated against on the basis of their gender or marital status."[11] These rights are also operationalised in Malawi's Gender Policy (2015)[12] and National Action

5 Hinson, L., Mueller, J., O'Brien-Milne, L., & Wandera, N. (2018). *Technology-facilitated gender-based violence: What is it, and how do we measure it*? International Center for Research on Women. https://www.svri.org/sites/default/files/attachments/2018-07-24/ICRW_TFGBVMarketing_Brief_v8-Web.pdf

6 https://data.worldbank.org/indicator/SP.POP.TOTL

7 https://data.worldbank.org/indicator/NY.GDP.PCAP.CD

8 Malawi Communication and Regulatory Authority. (2015). Survey on access and usage of ICT services in Malawi: Report. http://www.macra.org.mw/wp-content/uploads/2014/09/Survey_on-_Access_and_Usage_of_ICT_Services_2014_Report.pdf

9 Ibid.

10 Malanga, D. F. (2019). Framing the impact of artificial intelligence on protection of women rights in Malawi. In A. Finlay (Ed.), *Global Information Society Watch 2019: Artificial intelligence: Human rights, social justice and development*. APC. https://giswatch.org/sites/default/files/gisw2019_web_malawi.pdf

11 http://www.malawi.gov.mw/images/Publications/act/Constitution%20of%20Malawi.pdf

12 https://cepa.rmportal.net/Library/government-publications/National%20Gender%20Policy%202015.pdf/at_download/file

Plan to Combat Gender-based Violence in Malawi (2014-2020).[13] Despite such policy intervention, gender-based violence remains high in Malawi. The root causes point to culture and unequal power relations between men and women, which ensure male dominance over women. The unequal status of women is further exacerbated by poverty and discriminatory treatment in the family and public life. Malawi is ranked 173 out of 188 countries on the UN's Gender Inequality Index.[14]

Like other countries in the world, Malawi has not been spared of the COVID-19 pandemic. As of 12 June 2020, Malawi had registered 481 cases: four deaths, 65 recoveries and 412 active cases in 24 districts.[15] In response to this pandemic, the Malawi government developed the National COVID-19 Preparedness and Response Plan.[16] As a result, restrictive measures were imposed, such as physical and social distancing, and closure of schools and universities.

METHODOLOGY

The researcher adopted a survey design employing a multi-method approach. A total of 67 women and girls aged between 15 and 45 years responded to a survey questionnaire, while 10 women and girls were personally interviewed as a follow-up. Women and girls who participated in this report owned and/or had access to various online/digital platforms such as social media, laptops, smartphones, basic phones, online personal accounts and the internet, among others. Additionally, a panel discussion of was conducted with eight experts, comprising representatives of a civil society organisation dealing with gender-based violence, law enforcement such as the police (Victim Support Unit), the ICT regulator, the parliament, and academia. This was crucial for the author to appreciate their understanding of gender-based cyber violence in Malawi before and during the COVID-19 pandemic, and suggest possible strategies to combat the problem. Consent to collect the data was obtained from the participants. Data collected was analysed descriptively and thematically.

FORMS OF GENDER-BASED CYBER VIOLENCE WOMEN AND GIRLS EXPERIENCE

AWARENESS OF CYBER VIOLENCE

The first question asked to respondents was to understand their awareness of gender-based cyber violence. It was found that 98.1% of

13 http://www.togetherforgirls.org/wp-content/uploads/2017/10/National-Plan-of-Action-to-Combat-Gender-Based-Violence-in-Malawi-2014-2020.pdf

14 https://www.usaid.gov/malawi/fact-sheets/malawi-gender-equality-fact-sheet

15 https://covid19.health.gov.mw

16 https://malawi.un.org/sites/default/files/2020-04/National%20COVID%2019%20Preparedness%20and%20Response%20Plan_08-04-2020_Final%20Version.pdf

participants agreed that they knew about the existence of the problem, even before COVID-19, while 2.4% of them did not know. This implied that the vast majority of sampled research participants knew about gender-based cyber violence.

FORM(S) OF CYBER VIOLENCE

Data showed that cyber stalking (92.5%), cyber bullying (83.6%), cyber harassment (76.1%), and online sexual exploitation (71.4%) are major forms of gender-based cyber violence behaviours that women and girls experience during COVID-19 pandemic. This was also confirmed by some of the participants interviewed*:*

> I am a nurse by profession, and since the coming of COVID-19, I have been receiving abuse and bullying messages on my mobile phone and social media relating to COVID-19. All this was online misinformation trending on social media stating that nurses are at high risks of contracting COVID-19. (Respondent 4)

> I am a young female lecturer but what we get from social media is terrible. Women are regarded as video shows. People just post all sorts abusive words, nude images, portraying women as useless. I think the authorities need to make perpetrators circulating such type of online abuses be punished. (Respondent 7)

A few respondents also experienced online hate speech, non-consensual pornographic materials, and online defamation as presented in Table 1. It was further corroborated by interviews that each act of cyber violence was repeated in varying frequency: "These attackers do these things sometimes during lunch time, during night, and at any time of the day and week. So, it is very disappointing" (Respondent 5). The majority of participants also conceded that even before the COVID-19 pandemic, they continued to suffer in silence from gender-based cyber violence.

Table 1: Forms of gender-based cyber violence women and girls experience

Women and girls' experience(s) of gender-based cyber violence	Frequency (multiple response)	Percentage
Cyber harassment	51	76.1
Cyber bullying	56	83.6
Cyber stalking (e.g. false accusations, threats, etc.)	62	92.5
Online hate speech	31	46.3
Online sexual exploitation	48	71.6
Non-consensual pornography	36	53.7
Online defamation	29	43.3
Others	13	19.4

FREQUENCY OF OCCURRENCE

Left: Smartphone camera
Source: Donald Malanga (Author)

Participants were asked to state the frequency with which they usually experienced cyber violence from the time COVID-19 restrictive measures were put in place

in Malawi on 23 March 2020. Respondents were given five options to choose from: daily, weekly, fortnightly, monthly, and do not know. The findings showed that 67.1% of respondents stated that they experienced one or more form of gender-based cyber violence daily, 26.4% indicated that gender-based cyber violence occurred weekly, while 4.5% of respondents indicated that they did not know. This was also corroborated by an interviewee who had this to say:

> We women are regarded as cartoons in our society. With the coming of COVID-19, when you try to open WhatsApp or emails you find messages about women being abused daily, at work, at home, during conferences and even when we have boarded minibuses or any other mode of transport. So, online violence against women has become a norm. It is very disappointing. Sometimes, the attackers take them as jokes, yet we get traumatised. (Key informant 2).

ICT MODE AND TACTICS USED

Research participants were also asked to state the ICT mode that attackers or perpetrators use to commit cyber violence behaviours. The majority of participants indicated that social media (62.5% or 42) such as Facebook and WhatsApp and personal online accounts (31.3% or 21) were the digital platforms most frequently used by perpetrators to commit these acts. On the other hand, entertainment and dating sites were the least frequently used. These findings were not surprising, considering the fact that in Malawi, the number of women and girls accessing social networking sites via smartphones is growing significantly. It was also revealed that perpetrators used hacking (19.7%), gender trolling (54.2%), fake accounts (33.1%), doxing (12.3%) and communication threats (4.2%) as main tactics to gain entry into women's and girls' online spaces.

The results were further corroborated by follow-up interviews and key informants. This is what some had to say: "I just came to know someone had posted a porno image to my email account. Yet, I did not know where he/she got may email account?" (Key informant 3); "They just invaded my WhatsApp and posted all sorts of images and abusive words relating to my political affiliation and my former husband. I was threatened that if I continued supporting this political party, I should check my movement" (Key informant 5).

RELATIONSHIP BETWEEN THE PERPETRATOR AND THE VICTIM/SURVIVOR

Prior studies indicate that gender-based cyber violence is informed by the connection or relationship that exists between the victim/survivor and the attacker/perpetrator.[17] In this study, participants stated that the relationships that existed between them and the perpetrators varied from personal (56.2%) such as relatives and ex-boyfriends, to organisational relationships (39.5%) such as co-workers. Only 7.8% of participants indicated that perpetrators were impersonating them.[18]

PERPETRATORS' MOTIVATION FOR COMMITTING GENDER-BASED CYBER VIOLENCE

Perpetrators' motivation refers to the emotional, psychological, functional or ideological drivers behind the perpetrators' behaviour. The motivation can be informed by political and ideological agendas, or driven by revenge, anger, jealousy, sexual desire or other similar factors.[19] As shown in Table 2, participants indicated that perpetrators' motives were inspired by revenge (83.1%), anger (76.4%), jealousy (69.3%), sexual desire (59.7%), and political agenda (32.8%). From the perpetrator's motivations, comes intent or intention. This is a determination of the perpetrator or attacker to harm someone. It was found that perpetrators' intentions were to psychologically (61.8%) and physically (38.5%) harm the victims or survivors.

Table 2: Motivations behind gender-based cyber violence

Motives	Frequency (multiple responses)	Percentage (100%)
Jealousy	46	69.3
Sexual desire	40	59.7

17 Hinson, L., Mueller, J., O'Brien-Milne, L., & Wandera, N. (2018). Op. cit.

18 Definition of some of the terminogies used in this report: Cyber bullying means intentional act of online or digital intimidation or embarrassment; cyber harassment means distributing unwanted sexually explicit emails, text (or online) messages; cyber stalking means repeatedly sending emails, text messages or online instant messaging platform messages that are offensive or threatening; non-consensual pornography involves the online distribution of sexually graphic photographs or videos without the consent the individual in the image; and doxing refers to the online researching and publishing of private information on digital platforms to publicly expose or shame the person targeted.

19 Hinson, L., Mueller, J., O'Brien-Milne, L., & Wandera, N. (2018). Op. cit.

Revenge	56	83.1
Political agenda	22	32.8
Anger	51	76.4
Monetary desire/agenda	14	21.5
Maintain social status	12	17.9
Ideological agenda	8	12.1

IMPACT OF GENDER-BASED CYBER VIOLENCE ON WOMEN AND GIRLS

Prior literature suggests that every victim or survivor is impacted in some way by their cyber violence experience. Those impacts may include harms to their physical and mental health, social status and economic opportunities, even death. As Table 3 indicates, findings revealed that sampled participants withdrew from online activity (68.7%), lost reputation (17.2%), and cut down on social activity (9%).

Table 3: Impacts of gender-based cyber violence on women and girls

Impact of gender-based cyber violence on women and girls	Frequency (N-67)	Percentage (100%)
Social		
Harm reputation	12	17.9
Withdrew from online activity	46	68.7
Isolated from family, friends or co-workers	2	3.0
Cut down on social activity	6	9.0
Moved out of the community	1	1.5
Psychological/emotional		
Anxiety	6	9.0
Living in a state of fear	33	49.3
Depression	2	3.0
Self-image damaged	21	31.3
Self-harming behaviours	1	1.5
Thoughts of suicide	1	1.5
Negative impact on job/school performance	3	4.5
Economic/financial		
Loss of income	51	76.1
Loss of educational opportunities	4	6.0
Loss of home	5	7.5
Inability to get a new job	6	12.0
Loss of property	1	1.5
Physical		
Self-harm	3	4.5
Physical abuse exacerbated by online violence	36	53.7
Physical harm and injury resulting from online violence	23	34.3
Physical illness	5	7.5

Participants were also abused online (53.7%) and harmed online (34.3%), which to some extent led to physical illness (7.5%). Furthermore, the findings showed that cyber violence has negatively impacted women and girls through consequences such as living in a state of fear (49.3%), self-image damaged (31.3%), and anxiety (9%). Other women stated that gender-based cyber violence has led them to loss of income (76.1%) and inability to get new employment opportunities (12%). Overall, this implies that gender-based cyber violence was socially, physically, psychologically and economically impacting women and girls during the COVID-19 pandemic.

RESPONSES/STRATEGIES TO TACKLE GENDER-BASED CYBER VIOLENCE

Prior studies indicate that victims/survivors of gender-based cyber violence can report their experiences to the police, seek health/psychological counselling or legal support services, and get help from their social networks.

SEEKING SOCIAL SUPPORT

As indicated in Table 4, the study found that women and girls blocked perpetrators on digital platforms (50.7%), left the digital platform (26.9%) or confronted the perpetrator physically or digitally (10.4%). The findings were further augmented by follow-up interviews. It was established that culturally, seeking social support because of gender-based cyber violence is not viewed as a serious matter. As a result, most victims never bother to seek counselling. As one respondent reported:

> I broke up recently with my ex-boyfriend. He threatened me and posted images and photos in a WhatsApp group. So what I did was just to leave the WhatsApp group and block the guy in all my online social networks. Reporting this issue to a counsellor? Our culture does not allow us to do that and it is not even taken seriously by the members of the community. (Key informant 8, respondent 5)

Table 4: Responses/strategies for tackling gender-based cyber violence against women and girls

Responses/strategies	Frequency (N=67)	Percentage (100%)
Seeking social support services		
Confronted attacker/perpetrator(s)	7	10.4
Blocked attacker/perpetrator(s) on digital platforms	34	50.7
Publicised personal information of attacker(s) online	1	1.5
Left the digital/online platform(s)	18	26.9
Exposed the attacker/perpetrator(s) to their family, friends and employers	2	3.0
Shared information through the media (newspapers, blogs, TV, radio, etc.)	-	-
Left to a transition place/house/refuge	1	1.5
Sought health/social counselling services	4	6.0
Seeking legal support services		
Reported to the police, attacker/perpetrator(s) arrested	2	3.0
Reported to the police, police took no action	21	31.3
Filed civil law suit against the perpetrator/attacker	1	1.5
Reported to the police, attacker/perpetrator convicted	1	1.5
Never reported to police/community leaders	42	62.7
Seeking Intervention from digital/online platform (Facebook, YouTube, pornography site, etc.)		
Digital/online platform blocked the attacker/perpetrator from using the platform	2	3.0
Digital/online platform removed the content	5	7.5
Appealed to digital/online platform but platform took no action	9	13.3
Never sought intervention from the digital/online platform owners	51	76.1

SEEKING LEGAL SUPPORT SERVICES

The findings showed that 62.7% of the respondents never reported the incidents to the police or community leaders, while 31.3% of respondents reported the incidents to police, but unfortunately the police took no action. Corroborating the findings with the key informants, it was revealed that in Malawi, gender-based cyber violence is an emerging concept. As a result, it has not received much attention compared to physical violence in most gender policy documents:

> In Malawi, cyber violence is a new form of gender-based violence. As a result, it is not recognised as important. In fact, you can see even in our National Gender Policy and National Action Plan to Combat Gender-Based Violence, there is nowhere in these documents where you find gender-based cyber violence is mentioned. (Key informant 3, respondent 5)

From this analysis, it was clear that Malawi does not have adequate laws that women and girls can appeal to for protection from gender-based cyber violence.

SEEKING INTERVENTION FROM ONLINE DIGITAL PLATFORM(S)

The results show that 76.1% of surveyed participants never sought any intervention from the online platform companies, while 13.3% appealed to online platforms, but the online/digital platform took no action. To further understand the situation, the participants interviewed conceded that they were not even aware of the procedures for victims of cyber violence to launch a complaint or seek intervention from the online companies such as Facebook. Consequently, they never took any action with the companies. This is what one participant had to say:

> At this time there is chaos on social media. Anyone can post whatever he/she wants. Although these postings tend to target us women and girls because of gender identity. So when it comes to reporting, I do not think we are aware of reporting such cyber violence to the social media companies or mobile operators. But, if we can be informed how this can be done, I think this can be a good idea. (Respondent 7, key informant 6)

LEVEL OF GENDER-BASED CYBER VIOLENCE DURING THE COVID-19 PANDEMIC

Emerging data shows that the prevalence of sexual and domestic gender-based violence against women and girls has increased significantly since the COVID-19 outbreak. In this case, gender-based cyber violence against women and girls is not exceptional in Malawi. In the current study, participants were asked to choose on a scale from 1 to 5 (lowest to highest), and determine the level of cyber violence. The majority of respondents (65.1%) indicated that it was low (26-49%), 27.4% of respondents stated it was the lowest (1-25%), 5.2% of respondents stated that the level of gender-based cyber violence is high (50-74%), and 2.5% of respondents stated that it was the highest (75-100%). Few of the respondents (1.5%) indicated that they were not sure (0%). This implied that in general, the study found that gender-based cyber violence is low but it is rising steadily.

CONCLUSION

Although not detailed, this report has demonstrated that women and girls experience various forms of gender-based cyber violence in Malawi, before and during the COVID-19 pandemic. These include bullying, defamation, stalking, sexual exploitation, hate speech, and non-consensual pornographic videos and images, among others. Perpetrators use digital platforms such as social media, online personal accounts, dating sites, and smartphones to carry out their acts of gender-based cyber violence against women and girls. The majority of sampled women and girls had both personal (ex-boyfriend) and institutional (co-workers) relationships with the perpetrators.

The report has also revealed that perpetrators' motives to commit such acts of cyber violence were involved revenge, anger, jealousy, sexual desire and political agendas, with the intentions to psychologically and physically harm the victims. To this effect, gender-based cyber violence has socially, physically, psychologically and economically impacted women and girls. Consequently, these acts of cyber violence infringe on principles of the African Declaration on Internet Rights and Freedoms such as gender equality; protection of marginalised groups and groups at risks; fostering security, stability and resilience of the internet; and privacy and personal data protection.[20]

When it comes to responses to tackle gender-based violence, the findings show that the sampled women and girls use individual coping measures, such as confronting and blocking the attacker or leaving the online platform. This is an indication that women and girls avoid online spaces for fear of experiencing gender-based cyber violence.[21] The sampled women and girls never bothered to seek for social/community and legal aid services due to lack of awareness of such supportive services. Furthermore, in Malawi, like other African countries, the majority of women and girls are often reluctant to report their online victimisations for fear of social repercussions. The principles of African Declaration also emphasise that women and girls should have the right to access to information online, the right to access to affordable internet, and the right to due process. Yet, from this report, it is clear that the majority of women's and girls' digital rights were violated.

Most importantly, it was also revealed that although Malawi has a National Gender Policy (2015), a National Action Plan to Combat Gender-based Violence (2014-2020), and the newly developed National COVID-19 Preparedness and Response Plan (March-June 2020) in place, these policy documents just mention gender-based violence in generic terms without due considerations to cyber violence against women and girls. Besides, a review of Malawi's National COVID-19 Preparedness and Response Plan shows that gender-based violence is mentioned twice in the 84-page document. However, there is no policy statement regarding the gender-based cyber violence against women and girls. This can be attributed to the fact that the cyber violence phenomenon is an emerging concept that has not gained much individual, social, community and legal support in the country. Therefore, the findings from this report have implications for the role of government, civil society, academia and technology companies in tackling gender-based cyber violence against women and girls in the country during and after the COVID-19 pandemic.

20 https://africaninternetrights.org/wp-content/uploads/2015/11/African-Declaration-English-FINAL.pdf

21 European Institute of Gender Equality (2017). Cyber violence against women and girls. https://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls.pdf

RECOMMENDATIONS

The actions steps to consider include, but are not limited to, the following:

- The government should formulate cyber violence policy in recognition of the fact that cyber violence against women and girls is a form of gender-based violence. Strategies for addressing cyber violence against women and girls must also include the voices of women who are victims of the phenomenon.

- There is a need to integrate gender-based cyber violence prevention measures into the National COVID-19 Preparedness and Response Plan. This will pave the way for the adoption of regulatory standards to tackle the harmful effects of acts of gender-based cyber violence against women and girls.

- Civil society organisations dealing with gender-based violence should lobby the government for awareness-raising campaigns and educating women and girls about gender-based cyber violence during this time of COVID-19. This awareness and training will increase women's and girls' safety and privacy online, and further empower them to make decisions to protect their online safety.[22]

- Online human rights advocates/defenders in the country can use the evidence generated from this report to inform supportive campaigns and call for legal protection of women and girls against gender-based cyber violence during and after COVID-19.

- The internet and online platforms such as Facebook should create clear options for getting images or abusive content removed. They should also respond immediately and effectively to complaints from victims of online abuse, and finally establish genuine consent for terms of use.

22 West, J. (2014). *Cyber-Violence Against Women*. Battered Women's Support Services. https://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf

Women face internet access challenge during the COVID-19 pandemic in Uganda

Authors: Peace Oliver Amuge And Sandra Aceng | Country: Uganda

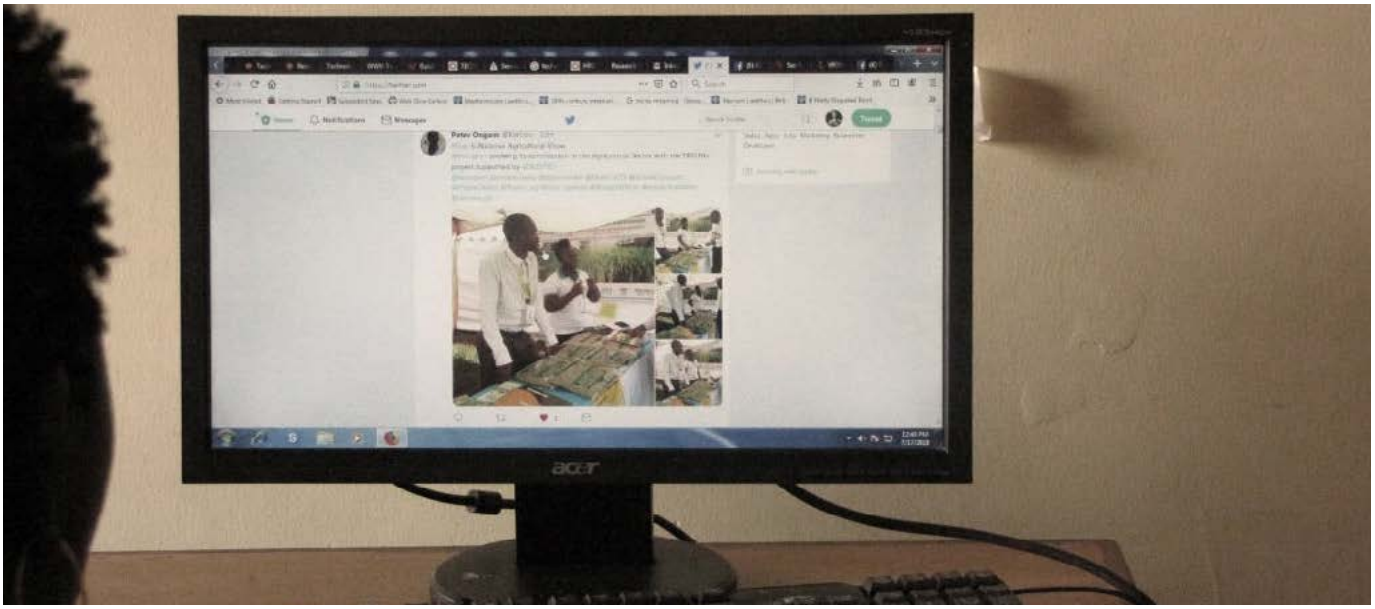
INTRODUCTION

This article analyses the challenge of internet access faced by women and other marginalised groups such as persons with disabilities in Uganda during the coronavirus (COVID-19) pandemic. It discusses how limited or no access to the internet affects women's digital human rights, as set out in the African Declaration on Internet Rights and Freedoms (African Declaration).[1] The article deals with existing information and communications technology (ICT) and internet policy gaps and COVID-19 national response strategies, and suggests possible recommendations to ensure a gender inclusive response with a special focus on women and other marginalised groups during and after the pandemic.

The COVID-19 pandemic has altered lifestyles and caused unprecedented governmental actions, including lockdowns and physical and social distancing measures. The pandemic rapidly increased internet usage for social interaction, advocacy work, business meetings, information sharing, online shopping, transactions, deliveries and online studies.

However, internet usage in Uganda is hindered by limited internet access, largely due to social media and mobile money taxation introduced in 2018. Additionally, costly internet data, poor connectivity, limited infrastructures especially in rural areas and slow internet speed have hit hardest on women's rights online.

1 https://africaninternetrights.org/articles/



Above: A woman reading information on Twitter
Photo Credit: WOUGNET

Uganda has one of the lowest internet penetration rates (14%) of the 10 African countries surveyed by Research ICT Africa (RIA) as part of the Global South After Access Survey conducted between 2017 and 2018. Besides the low internet penetration, less than half of the population own a mobile phone. Also, while data prices in Uganda appear competitive and relatively low compared to other African countries, data use remains constrained, even for those who have managed to overcome the price barrier of an internet-enabled device. [2]

The gender gap in Uganda's internet use is described as moderate, at 25% percent, but is larger than the gender gap in South Africa (12%), Lesotho (14%) and Senegal (21%).[3]

BACKGROUND

In Uganda, the government enforced a national lockdown in March 2020. As a result, many organisations have resorted to working remotely, using digital platforms like Zoom, Jitsi, Webex, Skype, BlueJeans and Google Hangouts to hold meetings with colleagues and partners and attend international conferences during the lockdown. For instance, worldwide, the user base of the Zoom video conferencing app "grew by another 50% to 300 million in the last three weeks at the beginning of April," according to Reuters.[4]

2 Gilwald, A., et al. (2019). *After Access: The State of ICT in Uganda*. Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf

3 Ibid.

4 Reuters. (2020, 22 April). Zoom participant numbers top 300 million despite growing ban list, shares hit record (April 23). *Reuters*. https://www.reuters.com/article/us-zoom-video-commn-encryption/zoom-users-top-300-million-as-ban-list-grows-idUSKCN22420R

With the lockdown, schools and institutions of higher learning closed, and this left students with only the option to study online or through TV. The closure of schools and day care centres has had a differential impact on women because they have to sacrifice their personal data for their children to be able to access classwork from the online platforms. On 1 June, during a presidential address on COVID-19, the government promised to provide at least two TV sets for each of the over 68,733 villages in the country to support long-distance learning, an initiative more expensive than the cost of internet access.

Above: ICT training at Refugee Settlement, Arua District in February 2020 Photo Credit: Platform Africa

The lack of internet access in Uganda is becoming even worse during the pandemic, especially for marginalised groups. Many people in these categories accessed and used the internet at workplaces and public access points such as restaurants and cafes that have been closed due to lockdown. Not all people have equal access in terms of bandwidth, suitable devices and necessary software. This caused many to go offline, further deepening the gender digital inequalities. The 2020 Mobile Gender Gap report shows that "the unconnected are disproportionately less educated, rural, and female."[5]

Digital inequalities can cause double inequalities, especially limiting opportunities for women and girls to acquire new skills and access accurate and relevant information online. Technology should be looked at and prioritised as an equaliser, not a divider.

One of the United Nations' Sustainable Development Goals (SDGs) is to achieve universal and affordable internet access for all by 2020, but in Uganda, many

5 Rowntree, O., & Shanahan, M. (2020). *Connected Women: The Mobile Gender Gap Report 2020.* GSMA https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/GSMA-The-Mobile-Gender-Gap-Report-2020.pdf

people, especially women, are still offline. With COVID-19 and the current rate of internet growth and adoption disrupted by expensive data, the country suffers a lack of competition in the telecoms sector. Currently, Uganda has only six companies providing internet-related services, with additional limitations such as imposed social media taxation, slow internet speed, lack of broadband affordability, poor infrastructure, etc. Therefore, affordable internet will not be achieved by 2020.

Uganda's Ministry of Health has established call centres for sharing updates related to COVID-19 and also extensively uses its various social media platforms. However, these require internet access and digital tools, which are still lacking among marginalised groups and communities.

Women are also constrained by inadequate digital skills, limited empowerment, expensive ICT tools, poor broadband connectivity, online safety concerns and relevant content online, according to the World Wide Web Foundation.[6]

Internet access is power, yet the online space is dominated by a patriarchal influence that often excludes women and women's issues online. Sometimes, even families disprove of women's activities online.

Principle 2 of the African Declaration provides for internet access and affordability, which is key during this pandemic. Principle 10 deals with rights for marginalised and at-risk groups and principle 13 focuses on gender equality.

However, women and other marginalised groups are least likely to have access to and use the internet due to factors such as high internet costs and unpaid care work, among others. The gender gap that existed before the COVID-19 outbreak has widened. With the lockdown, women and girls in abusive relationships are faced with increased control and internet access restrictions due to their confinement with abusers during lockdown periods.

Internet service providers have come up with supportive measures to promote access and use of the internet. MTN has introduced work-from-home bundles from 9:00 a.m. to 5:00 p.m. (Monday to Friday) at a fee of 2,000 Uganda shillings (USD 0.53). MTN has also provided free access to "some" education sites.

The Uganda Communications Commission (UCC) published a blog post providing ways to use internet data more efficiently without recognising that internet access is the first priority.[7] They articulated how internet users can

6 World Wide Web Foundation. (2015). *Women's Rights Online: Translating Access into Empowerment*. https://webfoundation.org/research/womens-rights-online-2015

7 Uganda Communications Commission. (2020, 29 April). How to Optimize Your Internet Data Bundle As You Continue to Stay and Work at Home following the COVID-19 Lockdown. https://uccinfo.blog/2020/04/29/how-to-optimise-your-internet-data-bundle-as-you-continue-to-stay-and-work-at-home-following-the-covid-19-lockdown

make the most use of their internet connection while at home, but this only applies to the few who already have access. These tips ignore the reality of a worsening gender digital divide.

Previous government initiatives such as free public Wi-Fi are only available in selected areas in Kampala city which excludes rural people and persons with disabilities who have mobility problems. Also, the time is not favourable for women as the service is available starting at 6:00 p.m. when women are usually occupied by domestic chores. During the lockdown period, free Wi-Fi remains limited and irrelevant. Internet access may be even worse with incoming 5G technology that requires more data for higher speeds.

To make matters worse, the 2018 social media tax – also called "over-the-top" or OTT tax – still requires every internet user to pay daily taxation of 200 Uganda shillings (USD 0.054) in order to access social media sites. The tax forced over five million internet users offline in three months. Other government taxes such as "pay-as-you-earn" (PAYE) personal income tax increased during the pandemic. According to Oxfam Uganda, the exchange rate has increased by 45% to an average of 3,800 Uganda shillings per USD. In 2012/2013, the PAYE threshold, which was equivalent to USD 94, is now equivalent to USD 64, implying a net reduction of USD 30 in earnings, which could explain the increasing poverty levels.[8]

PANDEMIC WIDENS THE GENDER DIGITAL DIVIDES

Like in most African countries, internet access is not free in Uganda. The internet is a social construct that impacts men and women differently. Previously, most women working in the formal sector accessed the internet at their workplaces, and now the majority are battling between the cost of internet and daily household needs. The Uganda Women's Network (UWONET) reported in March 2020 that 71% of women work in the informal sector, including retail business, markets, hospitality, vendors, and petty trade.[9] Retail and service industries have been among the hardest hit by the COVID-19 response. This means these women are not entitled to receive paid sick leave or family leave and hold no health insurance and social security, seriously threatening their livelihood.[10]

---

8 Tax Justice Alliance Uganda secretariat: SEATINI-Uganda. (2020, 1 April). Rethinking the Domestic Revenue Mobilisation Strategies Amidst the COVID-19 Pandemic in Uganda. *Oxfam Uganda*. https://uganda.oxfam.org/latest/press-release/rethinking-domestic-revenue-mobilisation-strategies-amidst-covid-19-pandemic

9 UWONET. (2020, 27 March). Press Release on Brutality and Use of Excessive Force by Security Forces in Enforcement of President's Directives on COVID-19. https://www.uwonet.or.ug/press-release-on-brutality-and-use-of-excessive-force-by-security-forces-in-enforcement-of-presidents-directives-on-covid-19

10 Wandera, D., & Muganga, E. (2020, 22 May). Children with hydrocephalus disease suffer during lockdown. *Daily Monitor*. https://www.monitor.co.ug/News/National/Children-hydrocephalus-suffer-lockdown-Museveni-Mbale/688334-5560358-3669gvz/index.html

In Uganda, women are also primary caregivers. On average, they spend about eight hours daily on unpaid care, leaving them with less time for paid work.[11] This means they are more likely to live in poverty, hence internet access becomes a luxury for women, rendering those without access more vulnerable to misinformation and disinformation.

Although women may have access to tech tools such as a mobile phone, married women – especially in rural areas – say their husbands restrict usage at home. According to 2019 research conducted by the Women of Uganda Network (WOUGNET) on the case of mobile broadband in Uganda:

> When each of the female respondents was asked where they obtain their money to buy data, 26% said they obtain the money mainly from their spouse and some quickly added that this comes with added costs with the spouse demanding to know who else she communicated to with the data they obtained.[12]

Above: Refugees using ICTs at Rhino Refugee Settlement in Arua District in February 2020 Photo Credit: Platform Africa

During this lockdown, the gender digital divide has further limited women's ability to work remotely. The Mobile Gender Gap Report 2020 findings show that there remains a "substantial mobile gender gap across low- and middle-income countries (LMICs) as over 300 million fewer women than men access the internet on mobile, and women are 8% less likely than men to own a mobile phone." The report further cites that "although the mobile internet gender gap is narrowing in LMICs, women still remain 20% less likely than men to use mobile internet."[13]

11 Oxfam Uganda. (2018, 28 August). Generations of Work Without Pay. https://uganda.oxfam.org/latest/press-release/generations-work-without-pay

12 Amuge, P. O., & Kakamagi, E. (2019). *Examining Women's Access to Digital Platforms: A Case of Mobile Broadband in Uganda.* WOUGNET. http://wougnet.org/files/mydocs/women-acess-to-digital-platform-download-version-1.pdf

13 Rowntree, O., & Shanahan, M. (2020). Op. cit.

The Ugandan Ministry of Education and Sports, UNICEF and the National Information Technology Authority have introduced "a free of charge and easy to use digital learning platform called Kolibri with education content approved by the National Curriculum Development Centre in Science and Mathematics for Secondary School learners and inclusive education for primary to keep children learning at home during the COVID-19 pandemic."[14]

However, to access Kolibri, the child needs "internet connectivity and gadgets such as a desk computer, laptop, or smartphone," according to UNICEF Uganda.[15] This is something Uganda is not ready for due to high internet and ICT costs, limited electricity, and poor infrastructure, especially in rural areas.

WOUGNET conducted a phone call interview with Iribagiza David, a fourth-year law student at Uganda Christine University, on 1 June. Iribagiza told WOUGNET that the university wanted to conduct online examinations, but that the government halted the plan due to internet access challenges for some students in rural areas who could not access internet facilities and ICT gadgets.[16]

"The students had mixed reactions, with a few embracing online studies and many against it, citing reasons like limited internet access, poor network and electricity problems due to constant load shedding in Uganda," he added. Iribagiza supposed female students would be more affected due to negative attitudes and cultural norms regarding gender and internet usage.

When previous health emergencies occurred in Uganda, such as Ebola, girls were often removed from or left schools first to attend to needs at home, even when schools remained open.[17] According to a 2018 UWONET report on unpaid care work, girls spend about 4.8 hours a day on unpaid care and domestic work while boys spend 3.8 hours. Although men's care workload decreases as they get older, girls' workload increases, leaving them with less time for leisure and school work.[18] With COVID-19, girls' home schooling has worsened due to limited internet and pressure to perform domestic chores.[19]

---

14 UNICEF. (2020, 26 March). UNICEF scales up support in 145 countries to keep children learning, as COVID-19 forces majority of schools worldwide to close. *UNICEF Uganda*. https://www.unicef.org/uganda/press-releases/unicef-scales-support-145-countries-keep-children-learning-covid-19-forces-majority

15 Ibid.

16 Interview with Iribagiza David, a fourth-year law student at Uganda Christine University on 1 June 2020.

17 OHCHR. (2020, 15 April). COVID-19 and women's human rights. https://www.ohchr.org/Documents/Issues/Women/COVID-19_and_Womens_Human_Rights.pdf

18 Uganda Women's Network. (2015). *On Rapid Care Analysis (RCA) & Household Care Survey (HCS) in Lamwo District, Acholi Sub-Region, Northern Uganda*. https://www.uwonet.or.ug/download/on-rapid-care-analysis-rca-household-care-survey-hcs-in-lamwo-district-acholi-sub-region-northern-uganda-2015/

19 World Bank Group. (2020, 16 April). Policy Note: Gender dimensions of the COVID-19 pandemic. http://documents1.worldbank.org/curated/en/618731587147227244/pdf/Gender-Dimensions-of-the-COVID-19-Pandemic.pdf

During the lockdown, most women in rural areas could not recharge their mobile phones due to inadequate access to electricity, as potential charging points were closed. Most women depend on families and their husbands for finances including charging and internet costs.

On 1 June, WOUGNET spoke to Grace Aceng, who lives in the rural area of Apac district, to understand what internet access has been like for her during this pandemic. Aceng told WOUGNET that the pandemic has brought additional challenges for women, such as financial disruptions, since most of the rural women depend on market vending but have not been able to run their businesses.[20]

Aceng added that the few women who accessed and used the internet before cannot afford it anymore due to the temporal closure of their businesses that previously supported them to buy airtime and data and pay OTT tax. "We face the challenge of slow internet speed, and most of the information sent on COVID-19 is in English. While I understand some words, I don't understand others," Aceng said.[21]

Women face limited access to sexual and reproductive health and rights (SRHR) information as well. For example, non-governmental organisations such as Uganda Youth Alliance for Family Planning and Adolescent Health (UYAFPAH) are now employing social media to bridge the gap on access to SRHR services and information by peers during the lockdown and for those unable to access social media, they are using peer educators in different communities.[22] However, social distancing has impacted the ability to do physical outreach.

Evelyn Lirri, a female freelance journalist, shared her experience on internet access during the pandemic via WhatsApp with WOUGNET on 18 May. Lirri said that internet access remains challenging in terms of cost:

> I buy monthly data for 50,000 Uganda shillings (USD 13), which is 20 gigabytes, but the speed is so slow, sometimes it doesn't work, yet I rely heavily on the internet to do my work, research, conduct interviews, etc. I have failed to attend some Zoom meetings where experts are speaking about COVID-19 because the internet is slow and unreliable.[23]

People with disabilities also have low incomes and cannot afford expensive internet rates in Uganda, including expensive assistive technologies. According to a 2018 UCC study on access and usage of ICTs by people with disabilities (PWDs) in Uganda, it found that "there is still a huge gap in access and use of

20 Interview with Grace Aceng, a farmer in Apac District, 1 June 2020.

21 Ibid.

22 https://www.facebook.com/846550665392209/posts/2930157317031523/

23 Interview with Evelyn Lirri, a female freelance journalist in Kampala District, 18 May 2020.

ICTs by PWDs majorly caused by high prices of ICT assistive technologies in relation to their incomes, ignorance and limited educational opportunities, lack of affirmative action and waiver of policies on PWDs, awareness of location to access the devices, no suitable technologies for PWDs, lack of awareness and information on ICT for PWDs."[24]

The study further showed that "only 15% mentioned they were able to access the internet and 25% didn't know about the internet whilst more male PWDs (6.2%) accessed it than their female counterparts (4%)."[25]

On 19 May, WOUGNET spoke to Shamim Nampijja from the National Union of Women with Disabilities (NUWODU) about the experience of PWDs during the pandemic. Nampijja mentioned that the government had excluded PWDs from the COVID-19 National Task Force. She revealed that OTT tax is one of the limiting factors to internet access for PWDs. "Women and girls with disabilities in the rural areas have been disproportionately affected by lack of internet access hence a lack of access to information," she said. "Most of the COVID-19 related discussions on national television, radio have been carried forward without including PWDs," she added.[26]

Photo Credit: Platform Africa

The second principle of the African Declaration states that internet access should be available and affordable to all people in Africa without discrimination on any ground such as race, colour, sex, language, religion, political or other opinions, national or social origin, property, birth or another status.

24 Uganda Communications Commission. (2018). *Access and Usage of Information and Communications Technologies (ICTS) by People with Disabilities (PWDS) in Uganda*. https://www.ucc.co.ug/wp-content/uploads/2017/09/Final-Report-on-Access-and-Usage-of-ICTs-by-PWDs_Public-Dissemination.pdf

25 Ibid.

26 Interview with Shamim Nampijja from the National Union of Women with Disabilities (NUWODU), 19 May 2020.

However, women and marginalised groups in Uganda continue to struggle to access the internet and these divides have only widened during the pandemic. This is a threat to the achievement of Uganda's Digital Vision 2040, which intends to empower its citizens with the aim to achieve the goals of universal inclusion, sustainable development, economic progress and poverty eradication through digital innovation.[27]

The gender divide may also affect the achievement of the UN's SDG 1.4, which is to ensure that all men and women, especially the poor and vulnerable groups, have equal rights to economic resources and appropriate new technology by 2030;[28] as well as SDG 5(b), which focuses on the use of enabling technologies, in particular ICTs, to promote women's empowerment.[29]

High internet costs with OTT taxes have forced many internet users to use virtual private networks (VPNs) to access the internet for education, information, communication and commerce. However, VPN usage consumes more data because the encryption process may add about 10-15% more data usage based on the strength of the encryption process. Besides data consumption, privacy issues remain questionable.[30] Many women use VPNs despite putting their privacy at risk.

The Ugandan government put several COVID-19 legal measures and policies in place that greatly helped to flatten the curve of COVID-19 spread. For example, the Public Health (Control of COVID-19) Rules, 2020 under Sections 11 and 27 of the Public Health Act banned or closed many public gatherings and meetings.[31] However, the government did not provide alternative ways to access information about these laws and policies offline.

Uganda was recently recognised as the country in Africa with the most favourable laws on ICT, but not much has been done yet to connect unconnected communities.[32] Uganda has only one community network, Battery-Operated System for Community Outreach (BOSCO) Uganda.[33] However, with the new normal of social distancing, the number of women accessing the centres for internet access and use has decreased, as confirmed by a BOSCO Uganda staff member.

---

27 https://ict.go.ug/initiatives/digital-uganda-vision

28 https://indicators.report/targets/1-4/

29 https://indicators.report/goals/goal-5/

30 Uganda Communications Commission. (2020, 29 April). Op. cit.

31 Uganda Legal Information Institute. (2020, 25 March). COVID-19 Legal and Policy Response Resource Guide for Uganda. https://ulii.org/blogs/admin/25-march-2020/covid-19-legal-and-policy-response-resource-guide-uganda; Ministry of Public Service. (2020, 25 March). Circular Letter No. 3. of 2020: Guidelines on Preventive Measures Against Corona Virus (COVID-19). https://ulii.org/system/files/CIRCULAR%20LETTER%20NO.%203%20OF%202020%20COVID-19_recognized.pdf

32 https://twitter.com/UCC_Official/status/1186551803967619072

33 http://boscouganda.com

CONCLUSION

COVID-19 has not affected everyone equally. Governments and stakeholders need to fight existing inequalities like the gender digital divide, which further widened due to the pandemic. The internet is a key public good. At a time when most activities take place online, internet access must be a top priority. The Ugandan government should consider endorsing the African Declaration on Internet Rights and Freedoms to ensure digital human rights.

Gender-inclusive public access policies must be developed to actively support women and other specific marginalised groups to get online. Women who face barriers to access devices and data at home must be able to connect online in safe, established locations such as marketplaces or near schools.

Both the public and private sectors in Uganda should work to build an inclusive broadband pro-competition regulatory framework with incentives that encourage investment and innovation for the country to reach universal access. This will help the government reduce internet-related costs and give more people – especially women and marginalised groups – the opportunity to get online.

The government should also scrap the social media tax and reduce taxes on ICT tools, data and internet services. Telecom companies should zero-rate public service sites so that people do not have to use their data to access useful information during a pandemic.[34]

To achieve internet access and affordability, there is a need for the Ugandan government to adhere to the principles of the 2019 African Commission on Human and Peoples' Rights (ACHPR) Declaration of Principles on Freedom of Expression and Access to Information, specifically the right to internet access as set out in Part IV, Principle 37, which includes these obligations:

> 3. States shall, in cooperation with all relevant stakeholders, adopt laws, policies and other measures to provide universal, equitable, affordable and meaningful access to the internet without discrimination, including by:
>
> a. developing independent and transparent regulatory mechanisms for effective oversight;
> b. improving information and communication technology and internet infrastructure for universal coverage;
> c. establishing mechanisms for regulating market competition to support lower pricing and encourage diversity;

34 Sarpong, E. (2020, 15 April). Covid-19 shows why internet access is a basic right. We must get everyone connected. *World Wide Web Foundation*. https://webfoundation.org/2020/04/covid-19-shows-why-internet-access-is-a-basic-right-we-must-get-everyone-connected

d. promoting local access initiatives such as community networks for enabling the increased connection of marginalised, unserved or underserved communities; and
e. facilitating digital literacy skills for inclusive and autonomous use.

4. In providing access to the internet, States shall take specific measures to ensure that marginalised groups have effective exercise of their rights online.[35]

This will ensure sustainability for women's rights online and narrow the gender digital divide as set out in Principle 13 of the African Declaration.[36]

35 https://www.achpr.org/presspublic/publication?id=80

36 https://africaninternetrights.org/articles

Reflections on COVID-19 policy responses in Uganda and the relevance of the African Declaration on Internet Rights and Freedoms for promoting women's rights online

Author: Amuku Isaac | Country: Uganda

INTRODUCTION

The COVID-19 pandemic has shown why the protection of human rights online is more important now than ever before. The internet has been a gateway for access to critical information, services and opportunities available to many people for the first time, as noted by the GSMA mobile gender gap report.[1] With more than half of the world's population under lockdown conditions, more women and girls are using the internet with greater frequency, and actions must be taken to ensure that there are no limitations on women's access and use of the internet. The Africa Declaration on Internet Rights and Freedoms, a pan-African initiative, provides standard measures and guidelines which African governments must follow to avoid formulating and implementing policies that curtail internet rights and infringe freedoms.[2] This article provides a reflection on COVID-19 policy responses in Uganda and the relevance of the African Declaration in promoting women's rights online, with reference to 10 of the 13 principles contained in the Declaration.

CONTEXT

This year marks seven years since the African Declaration was agreed and drafted to promote human rights standards and principles of openness in internet policy formulation and implementation on the continent. However, with the outbreak

1 GSMA. (2020). *Connected Women: The Mobile Gender Gap Report 2020.* https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/GSMA-The-Mobile-Gender-Gap-Report-2020.pdf

2 https://africaninternetrights.org

of COVID-19 in December 2019, the achievements made over the years are predicted to be rolled back due to a myriad of policy responses aimed at containing the spread of the virus. By 1 July 2020, all 57 African countries and small states were affected by the pandemic, with Uganda's first confirmed case of COVID-19 reported on 21 March 2020.[3]

Left: Kampala International University students searching for COVID-19 information at the WOUGNET secretariat. Source: WOUGNET

THE SOCIAL, POLITICAL AND ECONOMIC POLICY RESPONSES TO CONTAIN THE SPREAD OF THE VIRUS IN UGANDA

The government of Uganda's first set of policy measures to contain the spread of the virus took effect on 18 March 2020. The measures instituted included closing all educational institutions, suspending all religious gatherings, banning all political and cultural gatherings, suspending all inbound and outbound movement of passengers by air, water and land except for cargo airplanes and trucks, restricting weddings to only 10 people, and allowing only close relatives to attend burials. Furthermore, discos, dances, bars, sports, music shows, cinemas and concerts were suspended. A temporary lockdown and a night curfew from 7:00 p.m. until 6:00 a.m. was also instituted. All citizens were advised to adhere to the guidelines issued by World Health Organization (WHO) and Ugandan Ministry of Health (MOH) to stay safe. Various traditional and modern information and communication technologies (ICTs) were used to sensitise the masses about COVID-19. These platforms include television, radio and social media platforms like Twitter and Facebook. The latest COVID-19 updates in English and more than 61 local languages in Uganda were also shared on the MOH website.

THE GENDER DIGITAL DIVIDE

The gender digital divide has been recognised as one of the major challenges in achieving gender equality in the Sustainable Development Goals (SDGs), particularly Target 5.b for enhancing the use of enabling technologies to promote women's empowerment.[4] The International Telecommunication Union (ITU) indicates that women are still lagging behind men in their ability to take advantage of the

3 Biryabarema, E., & Obulutsa, G. (2020, 21 March). Uganda says has confirmed first coronavirus case. *Reuters*. https://www.reuters.com/article/health-coronavirus-uganda/uganda-says-has-confirmed-first-coronavirus-case-idUSL8N2BE0XB

4 https://sdgs.un.org/goals/goal5

power of digital technologies, with only 48% of women being online as compared to 58% of men globally, and in Africa with only 22.6% of women being online as compared to 33.8% of men.[5] The Uganda Communication Commission (UCC) indicates that only 44% of women are online in Uganda, as compared to 62% of their male counterparts, further reflecting the gender digital gap.[6]

This gender digital gap, according to the Alliance for Affordable Internet and Web Foundation, has been exposed by COVID-19 across the globe, where billions of people are cut off from accessing vital information on health and safety, online learning, and the opportunity to voice their views and engage in commerce.[7] Moreover, women's rights online, including freedom of expression, have been undermined by high levels of online violence, resulting in many of them resorting to self-censorship.[8]

As the virus continues to rapidly spread in Africa, where Uganda is no exception, misinformation and disinformation continue to spread faster than the virus, causing negative impacts on public health and safety. Women are the most affected by this as they lack access to credible information.[9]

In Uganda, access to the internet continues to grow rapidly, with 18.8 million people using digital platforms and social media to engage in politics, governance and socioeconomic development.[10] However, the existing policies do not take into consideration the needs and challenges faced by women while accessing and using the web. The Women of Uganda Network (WOUGNET)[11] therefore conducted an assessment in Uganda during the period of the COVID-19 pandemic to explore and document government policy responses and how the African Declaration can be used to promote women's rights online. The findings of this assessment indicate that many women could not afford to access and use the internet on a regular basis due to high costs and, in some places, poor internet connectivity. Furthermore, many women reported having experienced more online threats and attacks from men for expressing their views online during the pandemic, which undermines their opportunities to enjoy their full rights online.

---

5 ITU. (2019). *Measuring digital development: Facts and figures 2019.* https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

6 UCC. (2015). *Access and use of communication services*. https://www.ucc.co.ug

7 Jorge, S., Sarpong, E., & Nakagaki, M. (2020). *Covid-19 Policy Brief: Internet Access & Affordability.* Alliance for Affordable Internet and Web Foundation. https://docs.google.com/document/d/1b4G6kBtK3saFNTSqkYnhhxWyeh17WN3b8jNlcBoIrt4/edit

8 UN Women. (2020). *Online and ICT-facilitated violence against women and girls during COVID-19*. https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19-en.pdf?la=en&vs=2519

9 Sharpe, E. (2020). *Covid-19 Policy Brief: Misinformation & Freedom of Expression.* World Wide Web Foundation. https://docs.google.com/document/d/1XwcQDtr_aSYbL7mU2biLt9cqwTzZdoDElia5knO2on0/edit

10 See the "ICTs at a Glance" section on the home page of the Ministry of ICT & National Guidance website: https://ict.go.ug

11 https://www.wougnet.org

WOMEN'S RIGHTS ONLINE IN UGANDA

The African Declaration is more relevant today than ever to uphold and promote fundamental human rights, particularly women's rights online,[12] because it advocates for the creation of a favourable internet policy environment for more women to enjoy their full rights and freedoms online. The relevant principles are discussed below.

OPENNESS

Principle 1 requires that the internet should enable a common exchange of information and knowledge for everyone. A female representative from the National Organization of Peer Educators (NOPE) Uganda[13] noted that she has been spending more time on the internet during the pandemic than ever before to access information about the virus, complete her office work remotely, learn new ideas and keep in touch with her family and friends. However, the nationwide lockdown led to the closure of many businesses in the informal sector that are primarily run by women, which affected their sources of income to enable them to access and use the internet.

Another daunting challenge during this pandemic is a lack of electricity needed for connecting devices in the rural areas of Uganda, where the majority of women and young girls live, as noted by students from Kampala International University to whom WOUGNET spoke. Research ICT Africa noted that the urban-rural electrification divide in Uganda is high, with only 7% of households in rural areas connected to the main electricity grid, as compared to 48% in urban areas. This partly explains why only 9% of Ugandans living in rural areas have access to the internet and about a third (30%) of urban dwellers are using the internet.[14]

ACCESS AND AFFORDABILITY

Principle 2 requires the internet to be available and affordable to all persons in Africa without discrimination. In this pandemic, a female programme officer from Kubere Information Centre (KIC)[15] reported having spent a lot of money to purchase the data bundles that she could not afford on a regular basis because her business was closed. Further, a sales representative from MTN Uganda reported that she was able to use the internet regularly because the company

12 African Declaration on Internet Rights and Freedoms Coalition. (2020). *Position paper in response to the COVID-19 pandemic*. https://africaninternetrights.org/sites/default/files/AfDec_COVID-19_Position-paper_Eng.pdf

13 https://www.betterplace.org/en/organisations/24252-nope-uganda

14 Gillwald, A., Mothobi, O., Tusubira, F., & Ndiwalana, A. (2019). *After Access: The State of ICT in Uganda.* Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf

15 https://www.wougnet.org/project/kubere-information-center

provided free data bundles to enable her to keep in touch with customers while at home. While internet access has become more affordable, particularly on mobile phones, costs are still expensive for many Ugandans.[16] Moreover, structural inequalities, such as women's low levels of income, education and employment opportunities, limit their internet access and use.

FREEDOM OF EXPRESSION

Principle 3 provides for the right to freedom of opinion and expression for all citizens. Indeed, citizens' right to freedom of speech and expression, both online and offline, is protected in Uganda through the country's constitution,[17] but online threats and restrictions from governments and individuals based on suspicions continue to be the major limiting factor to the full enjoyment of these rights among women, as noted by a female city lawyer during a phone interview. Furthermore, WOUGNET spoke to the research and communication officer at the Centre for Multilateral Affairs,[18] who mentioned that many women have been threatened and attacked online during this pandemic by male individuals and government officials. However, few people realise that this undermines the rights of women.

RIGHT TO INFORMATION

Principle 4 requires everyone to have access to information on the internet. In Uganda, every citizen has the right to access information and records in the possession of the state or any other public body, except where the release of the information is likely to prejudice the security of the state or interfere with the right to the privacy of any other person.[19] While speaking to the research and communication officer at the Centre for Multilateral Affairs, it was noted that the MOH has provided adequate information about COVID-19, regularly engaged with citizens, and run the state virtually. This was done in response to the WHO's call for governments to establish transparent and understandable communication lines of dialogue with citizens and stakeholders to build trust and deliver advice on protective behaviours that individuals can adopt to bring the spread of the virus under control. The majority of women and persons with disabilities have been excluded from accessing this information, since it has not been conveyed in the local languages and sign language to ensure that all members of the population are appropriately informed and empowered by the information being communicated by the government. Moreover, the latest updates and statistics on COVID-19 were being conveyed largely through social

16 WOUGNET. (2020). *Bridging the Digital Gender Gap in Uganda: An assessment of women's rights online based on the principles of the African Declaration on Internet Rights and Freedoms.* https://africaninternetrights.org/en/resource/bridging-digital-gender-gap-uganda-assessment-women%E2%80%99s-rights-online-based-principles

17 Constitution of the Republic of Uganda. https://www.statehouse.go.ug/government/constitution

18 https://thecfma.org

19 Access to Information Act of 2005, Article 5. http://judiciary.go.ug

media, which the majority of women and persons with disabilities have no access to because of barriers such as lack of affordability, digital illiteracy, concerns around online safety and security, and lack of relevant content. This situation obviously poses obstacles to their enjoyment of human rights online.

CULTURE AND LINGUISTIC DIVERSITY

Principle 6 states that individuals and communities must have the right to use their own language or any language of their choice to create, share and disseminate information and knowledge through the internet. A monitoring and evaluation associate at NOPE Uganda noted that local radio and television stations have played a key role in sharing COVID-19 information in local languages. However, most of these stations are profit-oriented, and only share updates at specific times of the day, unlike the internet. The majority of women and young girls were not able to access credible and updated information because the government has been using television and social media technologies, which do not reach all 45 million Ugandans due to limited access and coverage in the rural areas where the majority of women and young girls live.

RIGHT TO DEVELOPMENT AND ACCESS TO KNOWLEDGE

Principle 7 states that every individual and community has the right to development, and the internet has a vital role to play in helping to achieve the full realisation of nationally and internationally agreed sustainable development goals. The internet has provided new opportunities during this period of the pandemic for more women to attend webinars and learn new skills at no cost in their areas of specialisation. However, schoolchildren and other learners have lost this opportunity during the pandemic due to limited access to internet and ICTs as schools started to use online platforms to carry out lessons. Online studying has also been affected by the high cost of internet bundles coupled with over the top (OTT) tax, which has put women and young girls at a disadvantage. This high cost of the internet has impacted negatively on social networking use for women because the majority could not afford to buy the data packages of their choice.[20]

PRIVACY AND DATA PROTECTION

Principle 8 requires everyone to have the right to privacy online and protection of personal data concerning him or her. Appropriate technology should be used to communicate on the internet, and the collection or processing of personal data should be transparent and in compliance with well-established laws. The Data Protection and Privacy Act, 2019 protects the privacy of the individual and of personal data by regulating the collection and processing of personal

20 Gillwald, A., Mothobi, O., Tusubira, F., & Ndiwalana, A. (2019). Op. cit.

information in Uganda. However, during this pandemic, there has been significant collection and processing of personal information. Article 13 of the Public Health (Control of COVID-19) Order, 2020 contravenes the right to privacy and personal data protection by granting the MOH powers to collect personal data and monitor all persons residing in a declared infected area under medical inspection or examination. The Ministry has been using mobile phones to track and monitor people who have been under mandatory institutional quarantine, which has affected their online freedom of expression and privacy, as noted by a representative of Barefoot Law Uganda.[21]

SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

In terms of principle 9, all citizens have the right to benefit from security, stability and resilience of the internet. The Declaration calls on governments to formulate and implement standardised policies that promote a secure, stable, resilient, reliable and trustworthy network for their citizens. However, this right has been curtailed by Public Health (Control of COVID-19) Order, which allows observation or surveillance of citizens by the medical officer both offline and online. Furthermore, there has been a surge in misinformation and disinformation, which has caused panic and fear among the population. Women are the most affected group, because many have been forced by COVID-19 policy responses to stay at home where they do not have access to timely and credible information about the virus, while those who are able to be online lack skills on how to browse the internet, making them vulnerable to misinformation and its associated effects.

MARGINALISED GROUPS AND GROUPS AT RISK

In terms of principle 10, everyone is entitled to use the internet to exercise and enjoy their human rights, and for participation in social and cultural life, without discrimination of any kind. During the pandemic, women and persons with disabilities remain forgotten when it comes to online rights and freedoms. They have been particularly affected because most of them earn daily incomes, and live in rural areas with limited access to mobile phones and internet connectivity. Furthermore, COVID-19 policy measures have not been inclusive for persons with disabilities, since most of them need assistive technologies to have access to information, which the majority in Uganda cannot afford.

GENDER EQUALITY

in order to address gender digital divide, principle 13 of the Declaration calls for the formulation of gender-sensitive internet policies to eliminate all forms of discrimination on the basis of gender. A fact that threatens to deepen the existing inequalities and undermine global development is the persistent gender

21 https://barefootlaw.org

digital divide.[22] WOUGNET's assessment of women's rights online in Uganda, based on the Declaration, indicates that the gender digital divide has increased over the years due to the high cost of data, lack of digital skills, and online gender-based violence, which all undermine women's access to and use of the internet.[23] The pandemic has shown that the existing discrimination in policy making has restricted and limited women's internet rights and freedoms over the years, which has been exacerbated by the current context. The majority of women still largely depend on their husbands to buy their mobile phones and data, and their husbands consequently dictate what women should do with them. Women's digital rights and safety are also being compromised by increased threats of violence and attacks from men, which often prevents women from freely expressing themselves online.

CONCLUSION

The African Declaration on Internet Rights and Freedoms is a prime document for African states to adopt in order to promote digital human rights, specifically women's rights online, during the COVID-19 pandemic. It is evident that the women and girls who have access to the internet are using the internet more than ever before to access information about the pandemic, do school assignments, conduct research, carry out digital transactions, attend meetings, work remotely and participate in developmental conversations in online spaces. However, this does not translate to gender digital equality in Uganda and some parts of Sub-Saharan Africa, because the majority of women and girls do not have access to fast and unlimited broadband connections at their home, work place or place of study on a regular basis using the appropriate devices. The factors that contribute to the ongoing gender digital divide in general are lack of access and affordability, restrictions on freedom of expression from government and individuals, the linguistic monopoly of English on the internet as the major medium of communication, and indiscriminate surveillance of individuals or the monitoring of their communications. We call upon the government, private sector and all citizens to collaborate and embrace the Declaration in order to bridge the gender digital divide and enhance women's rights online.

22 Sambuli, N., Brandusescu, A., & Brudvig, I. (2018). *Advancing Women's Rights Online: Gaps and Opportunities in Research and Advocacy*. World Wide Web Foundation. http://webfoundation.org/docs/2018/08/Advancing-Womens-Rights-Online_Gaps-and-Opportunities-in-Policy-and-Research.pdf

23 WOUGNET. (2020). Op. cit.

The gender digital divide and COVID-19: Towards feminist internet regulations in Southern Africa

Author: Tina Power | Region: Southern Africa

INTRODUCTION

The full impact of COVID-19 is yet to be fully understood, and, while there are many unknowns, the rapid and continued reliance on the internet cannot be denied. The internet has been lauded as a lifeline and critical force during this global health crisis,[1] but without equal and meaningful access to the internet, its ability to solve problems is limited. The gender digital divide in the Southern African region ordinarily discourages gender equality and entrenches the discrimination of marginalised and at-risk groups. Within the context of a global pandemic, the pervasiveness of existing inequalities and structures of discrimination are magnified.[2] The time has come – a feminist internet is imperative.[3]

The African Declaration on Internet Rights and Freedoms (African Declaration)[4] and the Feminist Principles of the Internet (FPIs)[5] advocate for an internet that is accessible, available, useable and affordable to all persons, without discrimination. Realising these principles has become increasingly urgent in the context of the

1 Jorge, S., Sarpong, E., & Nakagaki, M. (2020). *COVID-19 Policy Brief: Internet Access & Affordability.* Alliance for Affordable Internet and Web Foundation. https://a4ai.org/research/covid-19-policy-brief-internet-access-and-affordability

2 United Nations. (2020). *Policy Brief: The Impact of COVID-19 on Women.* UN Women and United Nations Secretariat. https://www.unwomen.org/en/digital-library/publications/2020/04/policy-brief-the-impact-of-covid-19-on-women

3 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

4 https://africaninternetrights.org/articles

5 https://feministinternet.org/en/principles

COVID-19 pandemic. Against the backdrop of structural inequality and contemporary challenges, this article reviews the COVID-19 regulations in select countries[6] in the Southern African region to determine the extent to which the regulations and responses meet the standards envisaged in the African Declaration and the FPIs, in particular, whether present responses recognise the principles of internet access, gender equality, and non-discrimination of marginalised groups and groups at risk.[7] As becomes apparent, the responses by states in the region are largely underwhelming. While most states reviewed included some reference to information and communications technologies (ICTs), recognition of digital gender inequality is lacking, as are meaningful responses to it.

This article highlights that certain conditions have aligned to present a unique opportunity to recalibrate existing efforts, shift narratives and develop new standards that can enable and reflect genuine equality and inclusion on the internet. These conditions include (i) pre-existing inequalities and vulnerabilities; (ii) the magnification of these issues in the present context; (iii) inadequate regulatory responses; and (iv) the online nature of the COVID-19 pandemic. Combined, these conditions present an opportune moment for the FPIs to be re-galvanised and infused, alongside the African Declaration, into the ICT regulatory response to COVID-19 in the region. While the COVID-19 context presents innumerable challenges, it has sparked important conversations around online spaces and digital rights, and within this crisis, there are opportunities for the FPIs and the African Declaration to be realised. This article suggests that now, more than ever, is the time to ensure that we have a feminist internet. The article concludes with recommendations on suggested requirements for feminist ICT regulations.

COVID-19 AND THE MAGNIFICATION OF THE GENDER DIGITAL DIVIDE

It is common cause that digital transformation continues to expand, offering significant opportunities and empowering those who have access to online spaces. However, it is also common cause that the benefits of digital transformation are not equally shared, and access, use and ownership of digital tools is neither equitable nor inclusive.[8] Digital divides highlight the varying disparities in meaningful access, use and ownership of ICTs, and capture the online manifestations of structural and systemic inequalities that persist offline.[9] One

6 Botswana, Malawi, Namibia, Zimbabwe and South Africa have been selected to provide a spectrum of responses and realities within the region.

7 Principles 2, 13 and 10 of the African Declaration.

8 Organisation for Economic Co-operation and Development (OECD). (2018). *Bridging the Digital Gender Divide: Include, Upskill, Innovate.* https://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf

9 See Association for Progressive Communications (APC). (2017). Bridging the gender digital divide from a human rights perspective: APC submission to the Office of the High Commissioner for Human Rights. https://www.ohchr.org/Documents/Issues/Women/WRGS/GenderDigital/APC.pdf; see also Mutsvario, B., & Ragnedda, M. (2019). Comprehending the Digital Disparities in Africa. In B. Mutsvario & M. Ragnedda (Eds), *Mapping the Digital Divide in Africa: A Mediated Analysis.* Amsterdam University Press. https://assets.ctfassets.net/4wrp2um278k7/6eNjNfkQbsLHEEUZMkegdx/66ba7342323fff1250a9552e-72fe33fe/9789048538225_ToC_Intro.pdf

of the more pervasive digital divides relates to gender disparities. The gender digital divide, the "measurable gap between women and men in their access to, use of and ability to influence, contribute to and benefit from ICTs,"[10] creates significant barriers in the realisation of human rights and impedes social and economic development.[11]

It is difficult to ascertain the full extent of the gender digital divide in Africa, particularly given the fact that Africa is one of the regions that has ranked lowest with regard to the availability of sexdisaggregated ICT data.[12] Nevertheless, there are indications that the prevalence of the gender digital divide in Africa is a cause for concern. For example, reports indicate that Africa is the only region with a marked increase in the internet user gender gap.[13] Sub-Saharan Africa appears to be in line with the continental trend, with over 300 million unconnected women living in the region.[14] More recent data suggest that women in Sub-Saharan Africa are 14% less likely to own a basic mobile phone and 34% less likely to own a smartphone that can connect to the internet.[15]

While the gender digital divide ordinarily has a disproportionate impact on gender equality and marginalised and at-risk groups,[16] in the context of a global pandemic the pervasiveness of these issues is magnified, and an already dire situation is amplified as many aspects of daily life move online.[17]

In the COVID-19 climate, unequal access to reliable information means limited access to health care and educational materials.[18] The disparity in the use

---

10 United Nations. (2020). Op. cit.

11 For purposes of this article, the understanding of the gender digital divide takes into account considerations that "[g]ender is a broad and fluid social construct that is not limited to the conventional male/female dichotomy that commonly informs gender analysis in ICT." See Sey, A., & Hafkin, N. (Eds.) (2019). *Taking Stock: Data and Evidence on Gender Equality in Digital Access, Skills and Leadership*. United Nations University and EQUALS. https://www.itu.int/en/action/gender-equality/Documents/EQUALS%20Research%20Report%202019.pdf; see also APC. (2017). *Bridging the gender digital divide from a human rights perspective: APC submission to the Office of the High Commissioner for Human Rights*. https://www.ohchr.org/Documents/Issues/Women/WRGS/GenderDigital/APC.pdf

12 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."

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

14 GSMA Connected Women. (2015). *Bridging the gender gap: Mobile access and usage in low- and middle-income countries*. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/02/Connected-Women-Gender-Gap.pdf

15 OECD. (2018). Op. cit.

16 APC. (2017). Op. cit.

17 Mlambo-Ngcuka, P. & Albrectsen, 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

18 Statement of Feminists and Women's Rights Organizations from the Global South and from marginalized communities in the Global North. (2020). *Call for a Feminist COVID-19 Policy*. https://feministallianceforrights.org/blog/2020/03/20/action-call-for-a-feminist-covid-19-policy

and ownership of ICTs becomes stark when women, children and vulnerable groups cannot access services for fear of being monitored by perpetrators or family members.[19] Economically vulnerable members of society, who are now expected to work from home with inefficient ICT infrastructure, are placed in an even more precarious situation.[20] In a time where access to the internet is becoming indispensable to everyday life, those who are unable to connect are isolated socially, economically and politically.[21] The Association for Progressive Communications (APC) has explained:

> Communities without access to the internet or with limited connectivity are more isolated and vulnerable, and are unable to readily access the public health information and services they need. This will result in deepened social and economic inequalities in the future. A lack of internet access can also exacerbate an already repressive, harmful and unequal context for women and people of diverse genders and sexualities.[22]

Women, girls and marginalised communities are at even more risk of falling behind and having to fight to access, enjoy and realise their human rights, both online and offline. The pre-existing access barriers, amplified by COVID-19, illustrate the dire need for adequate and appropriate responses. A feminist internet is imperative.

REGULATORY GAPS AND OPPORTUNITIES FOR FEMINIST RESPONSES

This section is dealt with in two parts. First, a cursory review of the COVID-19 regulations and responses of selected countries in the region reveals that there is insufficient recognition of the principles of internet access, gender equality, and non-discrimination of marginalised groups and groups at risk. Second, the responses, in many ways, fall short of the principles of the African Declaration and the FPIs. These inadequacies, existing issues and now the online nature of the COVID-19 pandemic present a unique opportunity to re-imagine how best to bring the FPIs and the African Declaration to the fore.

FINDING THE GAPS

Most COVID-19 responses included some reference to communication or technology as an essential service, whereas others were more proactive in enabling

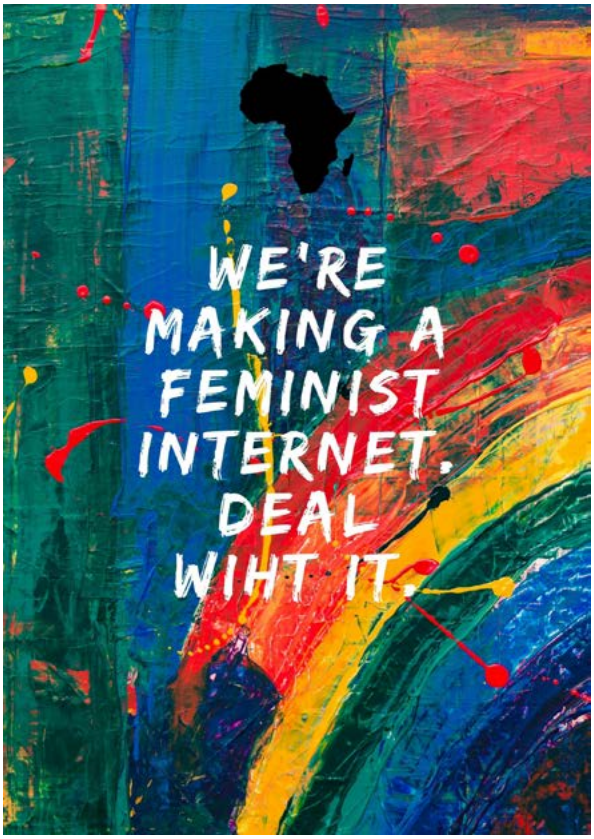
19 UN Women. (2020). *COVID-19 and Ending Violence Against Women and Girls*. https://reliefweb.int/sites/reliefweb.int/files/resources/issue-brief-covid-19-and-ending-violence-against-women-and-girls-en.pdf

20 Magenya, S. (2020, 17 March). Making a feminist Internet in Africa: Why the internet needs African feminists and feminisms. *GenderIT.org*. https://www.genderit.org/editorial/making-feminist-internet-africa-why-internet-needs-african-feminists-and-feminisms

21 Turianksyi, Y. (2020, 14 May). COVID-19: Implications for the 'digital divide' in Africa. *Africa Portal*. https://www.africaportal.org/features/covid-19-implications-of-the-pandemic-for-the-digital-divide-in-africa

22 APC. (2020). Op. cit.

access to ICTs during periods of lockdown.[23] Despite Botswana's high rankings in the region for affordable smartphones and mobile data, and strong "policy and regulatory frameworks in place to encourage growth and ensure provision of affordable and equitable access,"[24] its ICT COVID19 response is found wanting. Apart from listing "communication services" and "communication supplies" as essential in the COVID-19 Regulations, Botswana appears to have done very little in terms of ensuring or facilitating better access and connectivity, particularly during the lockdown period.[25] The Botswana Communications Regulatory Authority (BOCRA) issued several notices, largely relating to the publication of false news,[26] and the use of online platforms to remotely access BOCRA services.[27] There appear to be no recorded measures or responses concerning the gender digital divide and the disproportionate gendered impact of COVID-19 on digital rights.



Left: Protest poster
Source: Tina Power

The Malawi Public Health Rules listed "information and communication" as an essential service.[28] The reference to communication and media services online as an essential service is an indication of the government's recognition of the need for access to information online during this critical time. Further to this, in April 2020, the Malawian government appeared to take more proactive measures, engaging with mobile network operators to facilitate the provision of

23 African Declaration on Internet Rights and Freedoms Coalition (AfDec Coalition). (2020). *Position paper in response to the COVID-19 pandemic*. https://africaninternetrights.org/updates/2020/06/article-902

24 Alliance for Affordable Internet (A4A1). (2019). *The 2019 Affordability Report.* https://a4ai.org/affordability-report; see also The Economist. (2020). *The Inclusive Internet Index*. https://theinclusiveinternet.eiu.com/explore/countries/BW

25 Republic of Botswana. (2020). *Emergency Powers (Covid-19) Regulations, 2020 – S.I. No. 61 of 2020.* https://www.tralac.org/documents/resources/covid-19/countries/3352-botswana-extraordinary-government-gazette-emergency-powers-covid-19-regulations-2-april-2020/file.html

26 BOCRA. (2020, 27 March). Public Notice: Publishing, Forwarding or Creating False Information Using Online Platforms is an Offence. https://www.bocra.org.bw/public-notice-3

27 BOCRA. (2020, 24 March). Public Notice: Use of Online Platforms to Remotely Access BOCRA services. https://www.bocra.org.bw/public-notice-2

28 Malawi Ministry of Health. (2020). *Public Health (Corona Virus Prevention, Containment and Management) Rules, 2020*. https://africanlii.org/akn/mw/act/gn/2020/5

free internet to learners.[29] While these are steps in the right direction, the efforts of the Malawian government need to be significantly increased if there is any chance of elevating Malawi out of its low global ranking for internet access.[30] Similarly to Botswana, there are no recorded COVID-19 responses that target equal and inclusive access, despite Malawi having a "huge gender digital divide".[31]

The Namibian COVID-19 Regulations list ICTs as a critical service stating that "data centers, fibre optic infrastructure, towers and antennae will need to operate at high efficiency to ensure connectivity remains stable."[32] This expanded recognition of connectivity is notable. The Namibian government has made concerted efforts to facilitate access to the internet for educational purposes, setting aside funds to ensure internet connectivity for universities.[33] However, there is limited evidence to suggest that there have been measures responding to gender equality and non-discrimination, which is a poor reflection of Namibia's past efforts of addressing the digital gender divide.[34]

Zimbabwe's initial Public Health Order was silent on ICTs; however, this was amended and it now includes a reference to "communications and telecommunication services", including the internet and any public or licensed broadcasting service, as an essential service.[35] Despite this acknowledgement, Zimbabwe's ICT response has been of concern.[36] Amidst already high data prices and announcements by mobile operators of further price increases, there were increasing concerns regarding access in a COVID-19 context, prompting a request for the decrease in the cost of mobile data and internet fees.[37] Fortunately, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) heeded the call and announced the allocation of free temporary spectrum for

29 Gondwe, G. (2020, 24 April). Free Internet for Malawi's learners. *ITWeb*. https://itweb.africa/content/rW1xL759R3O7Rk6m

30 Freedom House. (2019). *Malawi: Freedom on the Net 2019*. https://freedomhouse.org/country/malawi/freedom-net/2019; see also https://theinclusiveinternet.eiu.com/explore/countries/MW/

31 Mthawanji, D. (2019, 9 May). Malawi: Putting MGDS III under gender microscope. *Gender Links*. https://genderlinks.org.za/news/putting-mgds-iii-under-gender-microscope

32 Republic of Namibia. (2020). *COVID-19 Regulations Proclamation 9 of 2020*. https://africanlii.org/akn/na/act/p/2020/9

33 Ngatjiheue, C. (2020, 9 June). Namibia: Govt Pumps N$9m into University internet. *All Africa*. https://allafrica.com/stories/202006100153.html

34 Bidwell, N. (2018, 4 July). Measuring the digital divide: Why we should be using a women-centred analysis. *GenderIT.org*. https://www.genderit.org/feminist-talk/review-measuring-digital-divide-why-we-should-be-using-women-centered-analysis; The Economist. (2020). *The Inclusive Internet Index*. https://theinclusiveinternet.eiu.com/explore/countries/NA/performance/indicators/readiness/policy/national-female-e-inclusion-policies

35 Government of Zimbabwe. (2020). *Public Health (COVID-19 Prevention, Containment and Treatment) (National Lockdown) (Amendment) Order, 2020 (No. 3)*. https://www.veritaszim.net/node/4083

36 AfDec Coalition. (2020). Op cit.

37 MISA Zimbabwe. (2020, 8 April). Internet access a fundamental human right – data must fall! https://zimbabwe.misa.org/2020/04/08/internet-access-a-fundamental-human-right-data-must-fall; Thompson, J. (2020, 1 May). Another data price hike shock for Zimbabweans. *Times Live*. https://www.timeslive.co.za/news/africa/2019-05-01-data-price-hikes-shock-zimbabweans

the main mobile network operators.[38] The freeing up of temporary spectrum is a welcomed development. While POTRAZ has indicated that it continues to regulate tariffs and find a balance between affordability for consumers and ensuring the survival of operators, it is likely that data prices will remain high and connectivity will remain a challenge for many ICT users in Zimbabwe. Further to this, and despite also being known for its gender digital divide, there appear to be no recorded responses that specifically address it in a COVID-19 context.[39]

South Africa has been more responsive, publishing directions early on in the pandemic that emphasised the importance of continued access to the internet.[40] These directions resulted in the Independent Communications Authority of South Africa (ICASA) allocating temporary spectrum to major mobile networks.[41] The directions further prohibited all licensed entities from effecting price increases.[42] Mobile network operators in South Africa have contributed toward facilitating access during the pandemic, decreasing data prices and providing access to a zero-rated USSD line for reporting infections and accessing critical information.[43] More recently, the Acting Minister of Communications and Digital Technologies published directions that provide a framework for the zero-rating of websites for education and health.[44] However, similarly to the above states, South Africa has not explicitly addressed the gender digital divide, although its overall promotion of access is a step in the right direction.

This brief mapping exercise illustrates the gaps in the regulatory response to COVID-19, gaps which can adversely affect women, girls, and members of marginalised communities. While states have noted the import of access, few states have adopted measures that meaningfully try to ensure it. The gender

38 Mudzingwa, F. (2020, 10 May). POTRAZ Gives Mobile Operators Additional Spectrum for the Rest Of 2020: Internet Use Has Ballooned. *TechZim*. https://www.techzim.co.zw/2020/05/potraz-gives-mobile-operators-additional-spectrum-for-the-rest-of-2020-internet-use-has-ballooned

39 Nyamutswa, C. (2018, 3 January). Bridging the Gender Divide. *ITU*. https://www.itu.int/en/council/cwg-internet/Pages/display-oct2017.aspx?ListItemID=34

40 Department of Telecommunications and Postal Service. (2020). *Electronic Communications, Postal and Broadcasting Directions issued under Regulation 10(8) of the Disaster Management Act, 2002 (Act 57 of 2002)*. https://www.gov.za/sites/default/files/gcis_document/202003/43164gon-417.pdf

41 ICASA. (2020, 17 April). Temporary radio frequency spectrum issued to qualifying applicants in an effort to deal with COVID-19 communication challenges. https://www.icasa.org.za/news/2020/temporary-radio-frequency-spectrum-issued-to-qualifying-applicants-in-an-effort-to-deal-with-covid-19-communication-challenges

42 The prohibition on price increases has since been removed. Department of Telecommunications and Postal Service. (2020). *Amendment of Electronic Communications, Postal and Broadcasting Directions issued under Regulation 10(8) of the Disaster Management Act, 2002 (Act 57 of 2002)*. https://www.gov.za/sites/default/files/gcis_document/202005/43351gon590.pdf

43 Khumalo, S., & van der Merwe, M. (2020, 20 March). MTN Slashes Data Prices. *News24*. https://www.news24.com/fin24/Companies/ICT/mtn-slashes-data-prices-20200320; Buthelezi, L. (2020, 10 March). Vodacom to slash data prices by at least 30%, clients to get free access to some websites. *News24*. https://www.news24.com/fin24/Companies/ICT/vodacom-to-slash-data-prices-by-at-least-30-20200310

44 Department of Telecommunications and Postal Service. (2020). *Directions on Zero-Rating of Websites for Education and health issues under regulation 4(10) of the Regulations made under the Disaster Management Act, 2002 (Act 57 of 2002)*. https://www.gov.za/sites/default/files/gcis_document/202006/43411gon651.pdf

digital gap has largely been ignored, leaving space for continued discrimination and harm.

The FPIs envisages a feminist internet that starts with "enabling more women and queer persons to enjoy universal, acceptable, affordable, unconditional, open, meaningful and equal access to the internet."[45] This type of access is needed, particularly during this time, and in a region where the current gender digital gap continues to leave millions offline. The African Declaration captures the central role that access to the internet plays in the realisation, exercise and enjoyment of human rights. It promotes the values of equal access, to learn about, define, use and shape the internet. The pre-existing inequalities now compounded by a global pandemic require heightened responses from states. While the inclusion of ICTs as essential and critical services is important, it is arguably the bare minimum in the current COVID-19 context. The regulatory frameworks and responses within the region fall short of the standards of access and equality envisaged by the FPIs and the African Declaration.

Furthermore, the lack of measures enabling meaningful and equal access during the pandemic proves a lack of inclusive discussions regarding crucial internet-related decisions. Both the FPIs and the African Declaration encourage a multistakeholder approach to internet governance.[46] This requires that the voices of those who face multiple forms of discrimination and who have been historically underrepresented in decision-making processes are invited to the table and are given an opportunity to contribute towards the policies and regulations that shape how people access the internet. The current regulations are clearly missing a feminist voice.

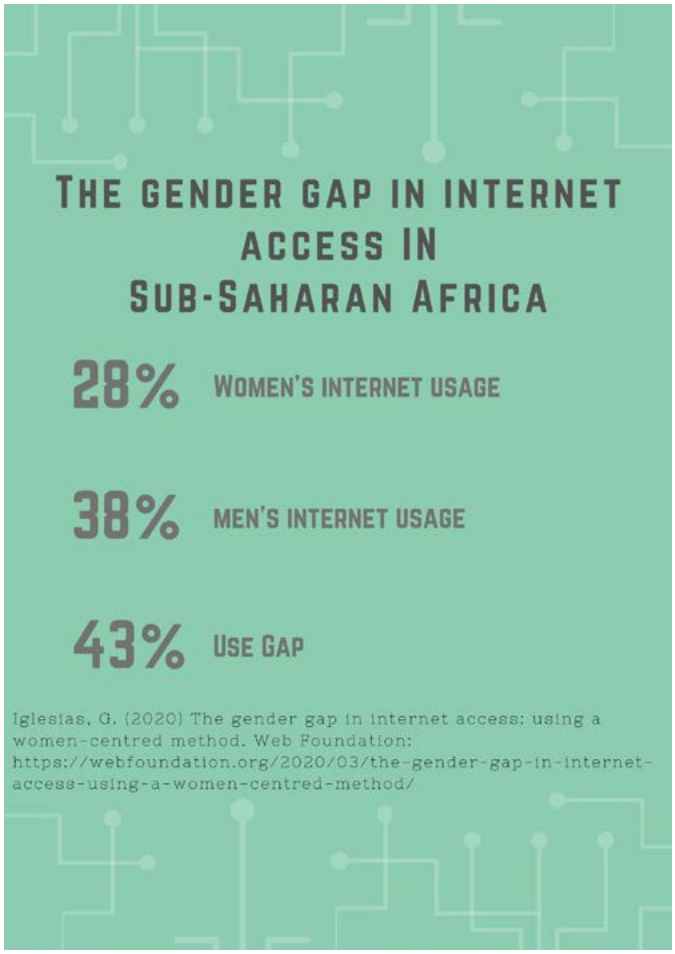
FILLING THE GAPS

The pre-existing access barriers, which have been amplified by COVID-19, warrant better responses, and now is the time to push states to do better. This next part will highlight that the gaps identified above, coupled with the immediate issues presented by COVID-19 and the realisation of the long-term reliance on the internet, are essential components of a formula that makes this moment an opportune one for the FPIs to be re-galvanised to ensure that feminist regulations take us through this crisis and become part of our post-COVID-19 existence.

45 https://feministinternet.org/en/principles

46 The FPIs state: "Our principle on governance highlights the need to democratise the multi-stakeholder process, as well as get more feminists and queer activists onto the discussion tables in order to advocate for a gender perspective in crucial internet-related debates;" Principle 12 of the African Declaration states: "Everyone has the right to participate in the governance of the Internet. The Internet should be governed in such a way as to uphold and expand human rights to the fullest extent possible. The Internet governance framework must be open, inclusive, accountable, transparent and collaborative."

There is increasing acceptance that "internet rights and freedoms are more important now than ever before," particularly considering lockdown, social distancing, and reconfigurations to education systems and economic activity.[47] For individuals, governments, educational institutions, businesses and health care institutes, access to the internet has become crucial, and it is apparent that "internet access is a lifeline – not a luxury."[48] Access to the internet enables the dissemination of information and is integral to any disaster management response.[49] Beyond the clear need for immediate access to the internet, the COVID-19 pandemic has cemented the notion that the world can exist online and will largely remain online going forward. Analysts predict that "[i]n the post-pandemic world, technology will be as ubiquitous as it is now, if not more."[50] Prolonged and increased tech dependence will become an integral part of society and how we learn, communicate and trade.



Left: The gender gap in internet access: using a women -centred method. Web Foundation. https://webfoundation.org/2020/03/the-gendergap-in-internet-access-usinga-women-centred-method/ Source: Iglesias, G. (2020)

Our current and future realities dictate that internet access is crucial. While this may be so, the above discussion on gender digital inequality and the underwhelming responses from states in the region indicate that the internet as a solution is meaningless without equal access. In other words, "If digital technology and the internet are the lifeline of our days, then a feminist

47 AfDec Coalition. (2020). Op. cit.

48 Sarpong, E. (2020, 15 April). Covid-19 shows why internet access is a basic right. We must get everyone connected. *Alliance for Affordable Internet*. https://a4ai.org/covid-19-shows-why-internet-access-is-a-basic-right-we-must-get-everyone-connected; see also United Nations Economic Commission for Africa. (2020, 10 June). COVID-19: Africa in urgent need of affordable broadband internet. https://www.uneca.org/stories/covid-19-africa-urgent-need-affordable-broadband-internet

49 APC. (2020). Op. cit.

50 Rasheed, Z. (2020, 26 March). Our lives after the coronavirus pandemic. *Al Jazeera*. https://www.aljazeera.com/news/2020/03/world-coronavirus-pandemic-200326055223989.html

internet becomes an imperative."[51] That is why, given the urgent need for access, listing ICTs as an essential service is simply not enough. Magenya explains that presenting the internet as a solution to a social problem in the absence of equality of access, use and representation is a falsehood.[52] She explains further that "this is why we need even more African feminists and feminisms on, in, around the internet, to counter the idea that technology somehow levels the playing field for all, and is an infallible solution to all our problems."[53]

Taking the pre-existing status quo and adding a new reality that is internet reliant creates a key moment for change. The time is now for activists to critically re-imagine how best to prioritise the FPIs and the African Declaration. This moment provides an opportunity for targeted advocacy around COVID-19 responses, as well as an opportunity to ensure the principles of the FPIs and the African Declaration are present post-COVID-19. Feminist regulations and responses can have the potential to address past and present inequalities, recognise and prioritise the needs of the most vulnerable members of our societies, and pave the way forward for an inclusive, accessible and meaningful response. It is necessary to echo existing calls for feminist COVID-19 policies:

> It is critical that governments utilise a human rights and intersectional based approach to ensure that everyone has access to necessary information, support systems and resources during the current crisis.[54]

When calling for feminist regulatory and policy responses, it is important to ensure that among other things, such responses are of a high quality, and include objectives and frameworks for implementation and impact assessments and ensure meaningful opportunities for participation.[55] Further to this, there are three stepping stones toward the inclusion of feminist regulations in Southern Africa. The first is an acknowledgment by states that there are pre-existing structures of inequality and discrimination and that the harms of such inequalities are amplified in a COVID-19 context. Second, there needs to be regulatory reform of the current COVID-19 responses. The principles of the FPIs and the African Declaration need to be infused into the regulations and responses. A significant part of this step requires feminist voices to be part of the decision-making processes. States must ensure that there is "meaningful inclusion and participation of all stakeholders in internet policy decision-making processes and forums" during the pandemic.[56] Third, the measures and responses need to manifest

51 APC. (2020). Op. cit.

52 Magenya, S. (2020, 17 March). Op. cit.

53 Ibid.

54 Statement of Feminists. (2020). Op. cit.

55 For further recommendations on regulatory and policy governance see OECD Regulatory Policy Committee. (2012). *Recommendations of the Council on Regulatory Policy and Governance*. https://www.oecd.org/gov/regulatory-policy/49990817.pdf

56 APC. (2020). Op. cit.

in reality. States need to engage with creative solutions in the short, medium and long term. These measures must be both local and regional and must be supported by the African Union and the African Commission on Human Rights.

CONCLUSION

The impact of COVID-19 on existing digital gender inequalities has gone almost unnoticed by states in Southern Africa. Urgent acknowledgement by states is necessary, but this recognition must also be coupled with appropriate, inclusive and meaningful measures that ensure access to the internet amidst the current crisis. Equally, the role of the private sector cannot be ignored, and during regulatory reform processes, states must undertake to engage with the private sector mobile network operators and telecommunications service providers to facilitate free ICT services and/or reduce the prices of services.

Drawing on and reinforcing existing recommendations,[57] this article presents specific recommendations for regulatory reforms. ICT-specific regulations, from the relevant ministries, need to be published in order to address access to ICTs during the global pandemic. All and any decisions made must be open, inclusive, accountable, transparent and collaborative and include feminist voices. Below are the suggested inclusions for feminist ICT regulations:

- Recognition of the impact of COVID-19 on existing digital gender equalities is imperative, including express recognition that women, girls and marginalised communities in the region risk falling further behind as a result of the pandemic.

- The regulations must include an explicit acknowledgement that access to ICTs means affordable, meaningful and equal access.

- There must be an affirmation that existing access to ICTs cannot be restricted during this time of crisis.[58]

- States must take urgent steps to enable the establishment and use of Universal Service and Access Funds and Digital Inclusion Initiatives and Funds.[59]

---

57 AfDec. (2020). Op. cit.; Jorge, S., Sarpong, E., & Nakagaki, M. (2020). Op. cit.

58 International experts on freedom of expression and freedom of the media have stated that "internet access is critical at a time of crisis. It is essential that governments refrain from blocking internet access; in those situations where internet has been blocked, governments should, as a matter of priority, ensure immediate access to the fastest and broadest possible internet service. Especially at a time of emergency, when access to information is of critical importance, broad restrictions on access to the internet cannot be justified on public order or national security grounds." OHCHR. (2020, 19 March). COVID-19: Governments must promote and protect access to and free flow of information during pandemic – International experts. https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729&LangID=E

59 Jorge, S., Sarpong, E., & Nakagaki, M. (2020). Op. cit.

- Digital literacy materials must be developed and made accessible. These materials must be understandable and appropriate for meaningful digital literacy training. The training and tools must address safety, online harm and privacy.

- States, along with the relevant regulatory bodies, must provide temporary spectrum relief.

- Zero-rated information portals must be established. Zero-rated content must include portals that provide: vital information about the COVID-19 pandemic; health-related and educational information; platforms for reporting gender-based violence; spaces that provide psycho-social support; and sites that provide digital literacy training.

- Access to education must not be hampered. The provision of online teaching and learning materials must be coupled with digital tools to facilitate access. Online resources must be zero-rated and digital tools to facilitate access must be made available to those who need them. While digital tools are being distributed, collaboration with schools and post offices is necessary to deliver teaching and learning materials to ensure that no learner falls behind.

- Policies must be developed, and measures must be put in place, to address and curb technology-related and ICT-facilitated violence.

- Oversight and review mechanisms must be included in the regulations to ensure that they develop at a speed commensurate with technological developments.

Regulations along these lines, coupled with proper implementation, can lessen the gender digital divide and can set the correct tone for internet access beyond the pandemic. "In this global health crisis, the web is both a lifeline and a critical force in helping to curb the spread of COVID-19,"[60] but its value is limited if there is non-existent or inequitable access. For the internet's potential to be meaningful, the FPIs and the African Declaration must be infused into COVID19 responses. The time is now for concerted efforts to ensure this. "In this global moment of crisis and isolation, the need for a feminist internet, one that includes and centres the voices of African feminists, is no longer necessary, it is crucial."[61]

60 Jorge, S., Sarpong, E., & Nakagaki, M. (2020). Op. cit.

61 Magenya, S. (2020, 17 March). Op. cit.

FREEDOM OF EXPRESSION AND OTHER DIGITAL RIGHTS

Combate à COVID-19 em Moçambique: Experiências e práticas virtuais

Autor: Dércio Tsandzana | País: Moçambique

INTRODUÇÃO

Moçambique é um país com cerca de 30 milhões de habitantes[1], dos quais apenas 18% têm acesso à internet[2], sobretudo nas grandes cidades – centros urbanos. Porém, nos últimos anos aumentou o surgimento de iniciativas que usam as novas tecnologias como forma de mobilização social e política, sobretudo por jovens. Para além dos cidadãos, os políticos no geral e os governantes em particular aderem com maior regularidade ao uso de diversas plataformas digitais para se comunicar com os cidadãos, mas não só.

O presente texto vai procurar discutir o surgimento e aplicação de algumas iniciativas locais que usam a tecnologia, sobretudo a internet, como forma de mobilização para acesso à informação contra a pandemia da COVID-19 em Moçambique. Essencialmente, vamos partilhar experiências de actores do sector da saúde e da sociedade civil que se empenham no combate ao novo coronavírus. Para a sua concretização, o texto terá em conta uma pesquisa documental e entrevistas[3]. Como resultado final, espera-se a apresentação do escopo geral sobre o uso das tecnologias digitais no combate à COVID-19 em Moçambique, razão pela qual pretendemos apresentar algumas iniciativas que foram desenvolvidas por entidades públicas e privadas, desafios e visão dos mentores sobre o impacto de tais iniciativas.

Um dos primeiros exemplos que procuraremos explorar é sobre os contornos do surgimento e da implementação de uma plataforma denominada "Fica

1 Dados do recenseamento geral da população e habitação – relatório final, INE, 2019.

2 https://datareportal.com/reports/digital-2020-mozambique

3 As entrevistas foram feitas durante o mês de Maio, a partir da plataforma Skype. Os entrevistados acordaram que as citações pudessem ser feitas com os seus nomes próprios.

Atento" – criada pelo Instituto Nacional de Saúde de Moçambique (INS) –, cuja missão é difundir informação oficial sobre os contornos da evolução da pandemia em Moçambique. O interesse será perceber por parte dos seus criadores que avaliação pode ser feita em termos de funcionamento e apropriação para os objectivos pelos quais foi criada. O outro exemplo a ser explorado é o surgimento de uma plataforma designada "CovidMoz", cuja missão tem sido a partilha em tempo real de dados sobre a evolução da pandemia em Moçambique. O nosso interesse ao destacar a plataforma será no sentido de perceber de que forma a mesma não pode significar uma sobreposição de acções, no sentido em que existe praticamente um exemplo similar que é feito pelo INS. Interessa-nos ainda perceber qual tem sido o público-alvo desta última plataforma e que tipo de *feedback* por parte dos usuários existe sobre a mesma.

CONTEXTO E SURGIMENTO DE INICIATIVAS DIGITAIS EM TORNO DA COVID-19 EM MOÇAMBIQUE

Moçambique, tal como outros países da África, adoptou medidas de restrição para a circulação de pessoas, sobretudo com a decretação de Estado de Emergência. Após a decretação do primeiro Estado de Emergência no mês de Março, o país prolongou por duas vezes a vigência desse mesmo Estado em consequência do aumento e propagação do vírus, sendo que até 29 de Julho o país estará sob medidas de limitação que se caracterizam essencialmente por limitação da circulação de pessoas e bens, bem como a restrição de alguns serviços. Em decorrência do contexto, surgiram questionamentos sobre como é que as autoridades iriam implementar tais medidas do ponto de vista de aplicação da lei, sem com isso significar a violação de direitos fundamentais e de liberdade dos cidadãos, sobretudo de informação e de imprensa. Por exemplo, numa das passagens, o Decreto que estabeleceu o Estado de Emergência refere que, durante a vigência do mesmo, os órgãos de comunicação social que veicularem informação sobre a COVID-19 contrárias às oficiais são sancionados, o que pode sugerir que todos os órgãos que não veiculem informações fornecidas por entidades governamentais estarão a emitir inverdades.

Sabe-se ainda que o Governo introduziu, desde o fim do mês de Março, uma monitoria e rastreio por meio de GPS de todas as pessoas que entrassem em Moçambique por via dos aeroportos e fronteiras, mas desconhece-se ao certo de que forma esses dados são usados em termos de privacidade e segurança de dados. No mesmo, dizia-se que as autoridades policiais e de saúde "devem criar as condições necessárias para, em tempo real, localizar por localização geográfica" todos que chegaram a Moçambique e qualquer pessoa que tenha entrado em contacto directo com a COVID-19. Ou seja, apesar da existência de um quadro legal por meio de Decreto presidencial, desconhecem-se os contornos em que questões sobre segurança e privacidade dos cidadãos na internet são garantidos ao longo da vigência do Estado de Emergência ou da pandemia em si – um acto que pode ir ao contrário do que é estipulado na Declaração

Africana sobre Direitos e Liberdades na internet[4], em quatro princípios: (1) acesso à informação; (2) privacidade e proteção de dados pessoais; (3) liberdade de expressão e (4) direito à informação.

DUAS FERRAMENTAS NUMA SOCIEDADE DESPROVIDA DE ACESSO À INTERNET

No role de disseminação, sabe-se que o Instituto Nacional de Saúde (INS) de Moçambique[5] dispõe de uma conta oficial na plataforma WhatsApp que permite interacção instantânea com usuários que queiram saber da evolução da doença em Moçambique, um exemplo inspirado em outros países do mundo. Ao longo da nossa entrevista[6], Mussa Chaleque começou por dizer que havia uma preocupação por parte do INS no quesito da comunicação institucional, pois havia muitas "fake news" e várias pessoas não sabiam o que se passava sobre a COVID-19 em Moçambique[7]:

> Aliás, muita gente perguntava se a informação que circulava em vários meios digitais, com maior difusão no WhatsApp, era do Ministério da Saúde ou não, sobretudo em comparação com os outros países, razão pela qual surgiu a ideia de se criar uma plataforma digital que começou pelo INS, antes mesmo de o Ministério da Saúde (MISAU) reagir enquanto entidade competente. Assim, a criação da plataforma foi a primeira iniciativa, e o espelho inicial foi a África do Sul.

A plataforma foi criada em uma semana como espaço de comunicação e interacção. Porém, verificou-se que após a sua criação havia de ter outras plataformas complementares, e uma delas foi do diagnóstico e avaliação de risco da COVID-19, que foi feita em parceira com uma entidade de saúde local de Moçambique. Adicionalmente, o Facebook forneceu um mecanismo de comunicação gratuito ao Ministério da Saúde – uma conta WhatsApp que ajuda na divulgação rápida e fiável da informação, sendo que no primeiro dia foram perto de 6000 pessoas aderentes em menos de 24 horas – e, até o momento em que fizemos a entrevista, havia um registo de perto de 62000 usuários. Contudo, Chaleque afirmou que há problemas com as operadoras móveis para melhor difusão das plataformas ora criadas. Houve, igualmente, a tentativa de criação de um mecanismo de comunicação em SSD, mas o que se fez foi apenas juntá-lo ao Ministério da Saúde, porque já existia uma plataforma antes denominada "Pensa".

---

4 A declaração pode ser descarregada em língua portuguesa em: https://africaninternetrights.org/pt

5 O acesso pode ser feito em: https://covid19.ins.gov.mz

6 Entrevista realizada no dia 28 de Maio de 2020 (plataforma Skype).

7 Sobre isto, importa referir que no dia 24 de Junho foi organizado um diálogo virtual, sobre "Fake news e media digitais em tempos de COVID-19", que contou com Mussa Chaleque, do INS.

Por outro lado, encontramos a "CovidMoz", uma plataforma interactiva virtual que foi lançada no dia 26 de Abril. Essa plataforma surgiu porque os seus mentores[8] sentiram que não havia nada igual em Moçambique, daí terem tido a vontade de avançar com a iniciativa. Embora os seus criadores tenham criado tal aplicação de forma espontânea e como hobby, eles afirmaram que "sentiam alguma inveja por ver que lá fora existia algo do género, sobretudo para não depender de informação do Governo, para que as pessoas estejam cientes e tomarem alguma decisão".

COMO GARANTIR PRIVACIDADE E SEGURANÇA?

Para Luís Pereira e Clayton Matule – criadores da "Covidmoz" – as questões sobre segurança devem merecer destaque em qualquer tipo de aplicação na internet. Para eles, existe a noção segundo a qual qualquer usuário deixa sempre traços no website que é acessado, mas sabem que cada aplicação pode ter escolhas como pedir *feedback*, mas para o caso deles não precisam de dados desses mesmos utilizadores, embora não tenham certeza se o servidor que usam trata desse tipo de dados, mas não garantiram que precisam guardar essa informação. Referiram ainda que as notificações que podem fazer são do tipo *push-notification*, desde que a pessoa use um dispositivo que aceite receber esses dados de alerta, mas sem ficar com os dados do usuário, sem gravar dados de localização. Assumem que esse é um assunto sensível, sobretudo depois de ver que o Google e a Apple lançaram um trabalho conjunto para fazer rastreio sobre casos da COVID-19. Clayton Matule contou:

> Não quero dar razão, mas nós estamos aqui para encontrar soluções e ajudar, porque todos queremos apoiar, e não faz sentido violar a privacidade das pessoas para ganhar dinheiro. Há que ter um bocado de ética e empatia para respeitar quem acede o nosso espaço, mas vamos ser honestos, ninguém lê os termos e condições, por isso mesmo vimos muitos casos de pessoas enganadas por aplicações.

Chaleque revelou-nos que não teria muito para dizer sobre questões de segurança e privacidade, porque o INS não faz muita colecta de dados. A única coisa que é feita pela instituição é disponibilizar um campo para que as pessoas coloquem perguntas e depois encontrem respostas na base dos e-mails que depois não são usados para nenhum efeito, nem mesmo para o envio do boletim informativo sobre a pandemia. Sobre rastreio e seguimento GPS, foi-nos explicado que existem três equipas (laboratório, vigilância e comunicação), mas essa plataforma é usada pela equipa da vigilância e não por parte do sector de comunicação do INS.

8 Entrevista realizada no dia 21 de Maio de 2020 (plataforma Skype).

UMA INOVAÇÃO QUE É MAIS DO MESMO?

Chaleque revelou-nos:

> Nós tentamos imitar a base de criação do nosso website, sobretudo com a África do Sul. Alguns trazem mais informação, sobretudo práticas de como as pessoas devem se comportar em casa (na família ou na escola), enquanto a nossa plataforma é mais directa e apenas informativa. Vemos que outros websites são mais avançados, mas temos dificuldades porque há realidades que não combinam com Moçambique, sobretudo quando queremos tratar de rastreio geográfico das pessoas.

A realidade descrita acima deve-se pelo facto de, em Moçambique, muita gente não estar a usar celular com grande capacidade (*smartphone*), embora esteja em criação uma nova plataforma para melhor dinamizar a comunicação e trazer aspectos de interacção, um trabalho que decorre em parceria com o Banco Mundial, uma vez que as outras plataformas parecem mais caprichadas, explicou o entrevistado. Essa realidade faz-nos constatar que a inovação digital em tempos de pandemia é limitada[9]. Aliás, os mentores da aplicação "CovidMoz" foram unânimes em afirmar que, para iniciar a sua iniciativa, tiveram que visitar algumas vezes a plataforma do INS, embora tenham sentido que, sendo uma página com caráter institucional, a mesma possuía mais informação do que devia:

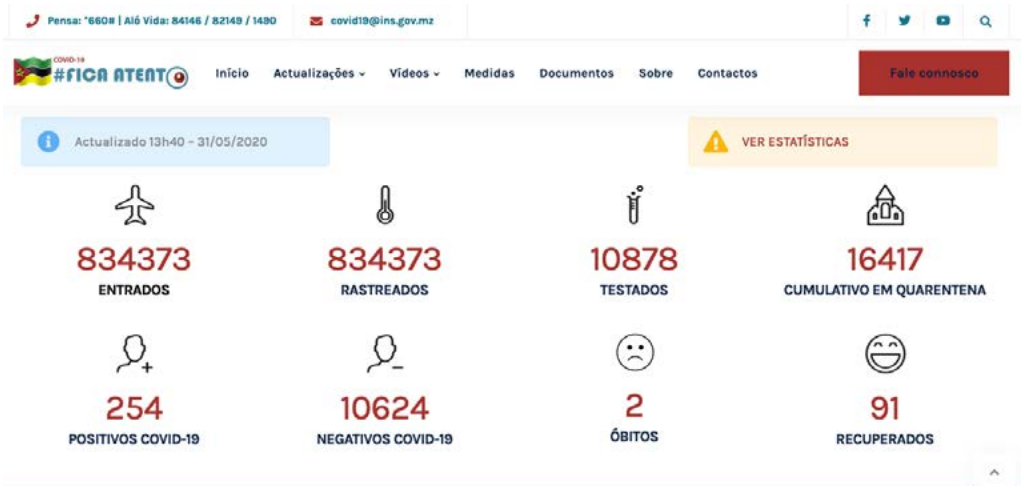
> Há muitos vídeos e tanta informação, sendo que muitas pessoas não têm nada a ver com tal informação, daí criamos algo mais simples e directo ao ponto. No nosso website as pessoas podem ter mais informação e directa. Muita gente já não busca muita informação, só entram para buscar os casos da COVID-19, mas o INS demorava colocar informação e sempre trazia documentos com demora de actualização, enquanto as páginas do Facebook e WhatsApp já tinham essa informação.

Os entrevistados contaram que viram a necessidade de tornar o processo fácil, daí que decidiram começar sozinhos o trabalho, mesmo sem o INS, sendo que naquele mesmo instante em que os dados são publicados, eles fazem a actualização virtual dos dados, sem poder esperar até ao momento da difusão da informação em espaços como a televisão ou rádio, mesmo que sempre tenham tido o Ministério de Saúde como fonte de privilégio. Para eles, a maior diferença que podem estabelecer com o INS é pelo facto de se poder encontrar informação no mapa de forma detalhada, não só pelo país de forma global, mas igualmente por províncias, o que fez com que a forma como o INS apresentava

9 O Ministério da Ciência e Tecnologia, Ensino Superior e Técnico-Profissional (MCTESTP), procedeu no dia 6 de Junho, em Maputo, a entrega de diplomas de honra aos autores de inovação em resposta à COVID-19. Um dos trabalhos reconhecidos é a plataforma "REPORTA" – um aplicativo móvel desenvolvido pelo Instituto para Democracia Multipartidária (IMD) e MídiaLab, com o apoio do MCTESP, e que serve para autoavalição, monitoria de nível de infecção pelo novo coronavírus em Moçambique.

os dados mudasse depois de terem lançado a aplicação "CovidMoz", contaram os entrevistados. Em termos de inovação, nota-se claramente que, apesar de a aplicação "CovidMoz" basear-se na informação obtida por parte do INS, ela apresenta melhor leitura de detalhes, ao trazer uma simplificação alargada (ver imagens abaixo – captura de ecrã feitas no dia 31 de Maio de 2020).

Left: Foto captura de ecrã CovidMoz 31 de Maio de 2020



Left: Foto captura de ecrã INS Moçambique 31 de Maio de 2020

SEGURANÇA, PRIVACIDADE E FEEDBACK DOS USUÁRIOS

Os mentores da aplicação "CovidMoz" referiram que muitas pessoas têm enviado e-mails para parabenizar pelo trabalho, e sobretudo sugestões. Assumem que existe quem os critica, e um dos exemplos foi o facto de terem colocado o total de visitantes e sem detalhar a localização dos mesmos, o que criou alguma confusão nas pessoas que aderiam ao website. Aliás, revelaram que, em termos de acesso na página, já contam com perto de 22.000 utilizadores (dados até 21 de Maio), mas sentiram alguma redução nos últimos dias, embora ficasse na média de 500 pessoas ao dia. Usando esses dados, referiram que começaram a validar o *input* das pessoas para poder melhorar ou mudar a plataforma em

si, uma vez que o *feedback* era enviado por WhatsApp ou então por e-mail. Sublinharam ainda que um dos pedidos levantados pelos usuários foi sobre as notificações em caso de nova actualização. Porém, um dado nos chamou atenção quando referiram que se formos analisar os números em termos geográficos, os moçambicanos são praticamente a minoria na estatística. Para eles, quem acessa a internet não usa de forma devida, porque usa-se mais para redes sociais e não acesso à informação:

> Acaba sendo difícil responder se os nossos acessos são mesmo de Moçambique, porque até já pensamos em divulgar mais a aplicação, mas nós não somos uma instituição formal do Estado e não podíamos fazer aplicações directas ou simples como SSD, embora se aceite que é sempre bom ter informação para muitas mais pessoas ao nível do país, sendo que nós só fazemos o mínimo e quiçá um dia alguém que tiver recursos possa ajudar-nos nesse trabalho.

Para o caso de INS, o nosso interlocutor revelou-nos que já foi feito um rastreio do relatório para aferir o número de acessos, sendo que constatou-se existirem milhares de visitas por dia – desde o lançamento no dia 22 de Março – um dia antes de casos por coronavírus –, embora o número depois tenha reduzido –, mesmo que tais números mostrem o website já tenha recebido uma média 650.000 visitantes, desde o dia da sua criação até o dia da realização da entrevista, 21 de Maio. Nesse grau, encontra-se a cidade de Maputo como a primeira com cerca de 140.000 visitantes, um volume de acessos que fez com que a equipa de *FAQ* (questões frequentes) acabasse estando sem possibilidade de dar resposta, por conta da elevada demanda dos usuários. Para o caso da ferramenta do diagnóstico de risco, foi o acesso a partir da plataforma WhatsApp com 83%.

Em termos futuros, os criadores da plataforma "CovidMoz" referiram que pensam em continuar com a iniciativa, porque essa é sua missão, até o dia em que acabarem os casos de infecção em Moçambique. Eles acreditaram na longevidade do trabalho, sobretudo porque são serviços gratuitos não onerosos: "(...) para nós, enquanto existirem meios que nos informam, iremos sempre actualizar a nossa aplicação, porque perguntamo-nos o que podia ser de nós se um dia a informação não fosse mais dada na televisão. Um dia, esperamos poder fazer resumos longos e de evolução temporal para a criação de gráficos e tabelas durante o tempo que durar a pandemia", disseram eles.

CONCLUSÕES

O presente texto mostra-nos que a eclosão da pandemia trouxe uma avalanche de informação, sobretudo nos primeiros dias do mês de Março. Com isso surgiram igualmente várias correntes que promoveram a disseminação de conteúdo falso (fake news), o que fez com que entidades como Instituto Nacional de Saúde (INS) tivessem que criar um espaço para difundir "informação oficial".

Ao mesmo tempo que avançaram iniciativas digitais, vimos a decretação de Estado de Emergência para conter a propagação do vírus no país. Nesse contexto, entendemos que o surgimento de plataformas digitais mostra-se como oportuna, mas não pode ser considerada como abrangente numa sociedade em que o acesso à internet permanece um desafio[10]. Pudemos perceber que algumas das iniciativas aqui apresentadas possuem capacidade de evolução, mas os seus mentores receiam que o uso não seja eficaz.

Diante dessa realidade, precisamos recordar que à luz da Declaração sobre Princípios de Liberdade de Expressão e Acesso à Informação em África, no seu capítulo IV – sobre a liberdade de expressão e o acesso à informação na internet – refere-se que: (1) os Estados deverão facilitar os direitos à liberdade de expressão e de acesso à informação on-line e aos meios necessários para o exercício desses direitos; (2) os Estados deverão reconhecer que o acesso universal, equitativo, acessível e significativo à internet é necessário à realização da liberdade de expressão, ao acesso à informação e ao exercício de outros direitos humanos e (3) os Estados deverão, em cooperação com todas as partes interessadas, adoptar leis, políticas e outras medidas com vista a proporcionar acesso universal, equitativo, económico e significativo à internet, sem discriminação, inclusive por parte dos Estados.

Podemos ainda sublinhar que permanecem zonas cinzentas sobre como as entidades governamentais usam a informação digital decorrente das plataformas, o que nos faz questionar como os usuários podem sentir-se seguros ao usar tais espaços, sobretudo aqueles que são da pertença de entidades como Ministério da Saúde, caso concreto e particular da aplicação "Pensa"?

10 Em Abril, Ericino de Salema, do EISA Moçambique, escreveu um texto para reflectir sobre as oportunidade do uso do Governo Electrónico em momentos de COVID-19.

Les politiques sénégalaises de lutte contre la pandémie COVID-19 et leur impact sur les droits humains en ligne

Auteur : Astou Diouf | Pays : Sénegal

INTRODUCTION

Notre monde est en train de vivre une pandémie jamais vécue dont la transmission virale a surpris tout le monde. Le COVID-19, n'a épargné quasiment aucun pays, même si c'est à des degrés divers. Dans cette situation, plusieurs gouvernants à travers le monde adoptent des mesures, des stratégies et des politiques de lutte contre la pandémie du coronavirus.

Certaines de ces stratégies et politiques s'appuient sur les outils et les services innovants qu'offrent les Technologies de l'Information et de la Communication (TIC).

En réalité, le numérique constitue pour l'État du Sénégal[1] un secteur économique à part entière. Dans sa dimension transversale, il ouvre de nouvelles perspectives, d'où l'introduction du concept moderne de « *société de l'information* ».

Toutefois, nous constatons en Afrique de plus en plus d'abus à travers les politiques de lutte contre le COVID-19, portant souvent gravement atteinte aux droits numériques tel que la liberté d'expression[2], la vie privée, les données à caractère personnel[3] et l'accès à l'information vraie.

---

1 Le Sénégal a décliné une stratégie numérique (SN2025) arrimée au Plan Sénégal Emergent en 2016 : « *le numérique pour tous et pour tous les usages en 2025 au Sénégal avec un secteur privé dynamique et innovant dans un écosystème performant* ».

2 https://www.achpr.org/public/Document/file/French/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_FRE_2019.pdf ; Déclaration de Principe sur la Liberté d'expression en Afrique, 2002.

3 Article 4 de la loi n° 2008-12 du 25 janvier 2008 sur la protection les données à caractère personnel.

Notre pays le Sénégal ne fait pas exception. C'est pourquoi, face aux enjeux stratégiques de lutte contre la pandémie du COVID-19, de la complexité de la maladie, et de l'importance de la garantie des droits et libertés fondamentaux, notre étude entend explorer le sujet suivant : **les politiques sénégalaises de lutte contre la pandémie COVID-19 et leurs impacts sur les droits humains en ligne.**

CONTEXTE

La pandémie COVID-19 est la crise sanitaire mondiale de notre époque et le plus grand défi auquel nous ayons été confrontés depuis la Seconde Guerre mondiale[4]. Depuis son apparition l'année dernière en Asie, le virus s'est propagé partout dans le monde.

« L'Afrique est atteinte par le COVID-19 au moment où plusieurs de ses pays, malgré les défis du sous-développement, sont sur une trajectoire d'émergence alors que d'autres continuent de faire face à la lutte contre le terrorisme. Le COVID-19 freine ainsi l'élan des uns, aggrave la situation des autres et remet en cause les efforts de tous. De plus, il soumettra à rude épreuve des systèmes nationaux de santé publique déjà vulnérables »[5], pour reprendre les propos de Macky Sall, Président de la République du Sénégal.

Au Sénégal, le gouvernement a adopté des plans de contingentement pour endiguer la propagation du virus qui s'y développe officiellement depuis le 2 mars 2020.

La lutte contre la pandémie du Covid-19 n'est pas que sanitaire, l'utilisation des TIC en respectant les droits humains, pourrait grandement contribuer aux actions menées par le brave personnel de santé.

En effet, les technologies numériques démontrent aujourd'hui, qu'elles peuvent être avantageuses aussi bien en temps normal qu'en temps de crise.

À cet effet, le gouvernement du Sénégal par le biais des TIC a mis en place des stratégies sanitaires, sociales, économiques et juridiques pour éradiquer cette pandémie.

Toutefois, certaines stratégies ou politiques relatives à l'usage des outils numériques peuvent avoir des conséquences néfastes sur les droits humains en ligne, notamment la liberté d'expression sur internet, liberté d'information, les données personnelles et la vie privée.

4 https://www.undp.org/content/undp/fr/home/coronavirus.html

5 https://www.adie.sn/actualites/l%E2%80%99afrique-et-le-monde-face-au-covid-19-point-de-vue-d%E2%80%99un-africain-%E2%80%93-par-macky-sall

Plus le numérique gagnera du terrain dans nos vies et plus la protection des droits humains en ligne deviendra l'affaire de tous et une préoccupation majeure pour les organismes de défense des droits et libertés fondamentaux.

Conscient que la protection des droits humains en ligne joue un rôle essentiel dans le développement des TIC, il importe de les respecter. Pour ce faire, tous les pays africains doivent absolument renforcer et protéger leurs infrastructures essentielles de l'information, mais aussi l'élaboration de politiques gouvernementales respectueuses des droits humains. Pour dire, qu'il est primordial pour lutter contre les violations des droits humains dans la gestion du COVID-19, les États africains doivent se conformer à la Déclaration Africaine des Droits et Libertés de l'Internet[6].

Ainsi, les politiques sénégalaises de prévention, de confinement et de traitement du COVID-19 qui impliquent l'usage des technologies numériques doivent tenir en compte du traitement de données à caractère personnel de santé ayant pour finalité : le suivi des cas possibles et confirmés d'infection par le virus SARS-COV-2, le suivi des personnes dites contact d'un cas confirmé et la vie privée des patients.

C'est dans ce contexte que le projet de la Coalition de la Déclaration Africaine des Droits et Libertés sur Internet (AfDec) relatif à « Sécuriser les droits de l'homme en ligne en Afrique grâce à un réseau fort et actif de la «Déclaration Africaine des Droits et Libertés sur Internet»»a été mis en œuvre. Ce projet vise à promouvoir les droits de l'homme en ligne.

PANDÉMIE COVID-19 AU SÉNÉGAL ET DROITS HUMAINS EN LIGNE

L'analyse des politiques sénégalaises de lutte contre la pandémie COVID-19 pose une préoccupation essentielle qui est celle de la protection des droits humains en ligne.

Étant donné que la pandémie se déplace comme une vague, le gouvernement, les autorités sanitaires, les établissements de santé et leur personnel ont déployé des efforts pour endiguer la propagation du virus. C'est pourquoi des éléments de réponse mériteraient d'être apportés sur la question suivante : **Quelles sont les mesures prise par l'État du Sénégal qui impliquent les technologies numériques dans la gestion de la pandémie à l'aune des droits humains en ligne ?**

Le Sénégal, qui a traversé l'épidémie d'Ebola en 2013 et 2014, n'a pas attendu la multiplication des cas pour prendre des mesures rigoureuses[7]. Afin d'enrayer les risques de contagion au coronavirus, le Président de la République Macky

6 https://www.2idhp.eu/images/declaration-africaine-des-droits-et-libertes-de-l-internet_170314.pdf

7 https://fr.unesco.org/news/covid-19-au-senegal-mesures-fortes-endiguer-contagion

Sall a proclamé le mardi 24 mars 2020 l'état d'urgence[8] et le couvre-feu sur l'ensemble du territoire en vertu de l'article 69 de la Constitution[9] et de la loi 69-29 du 29 avril 1969.

Aussi, l'informatique, « science de traitement automatique et rationnel de l'information en tant que support des connaissances et des communications »[10] est l'un des moyens qui ont permis à l'État du Sénégal de lutter contre la propagation du coronavirus. Ainsi pour éradiquer la pandémie, le gouvernement par le biais des technologies numériques a mis en place des stratégies sanitaires, économiques, sociales et juridiques.

Sur le plan sanitaire, le numérique est d'une grande nécessité aussi bien au niveau de la sensibilisation, de l'information, de la prévention, du confinement et du traitement du COVID-19 que du mode organisationnel des différents acteurs[11]. C'est dans ce cadre que l'Agence De l'Informatique de l'État (ADIE)[12], actrice majeure dans le secteur du numérique au Sénégal a tenu à jouer sa partition dans la guerre contre le coronavirus.

À cet effet, elle a mis à la disposition du Ministère de la Santé et de l'Action Sociale (MSAS) une plateforme, un *chatbot* et des outils pour une communication à distance efficace pour la cellule de crise.

De plus, l'ADIE a doté les forces de défense et de sécurité, le SAMU, de téléphones intelligents offrant des options de communication par voix ou vidéo, avec partage de documents et intégration de la géolocalisation[13].

Ces outils de communication et de coordination permettront au ministre et aux autorités impliquées dans cette lutte, de voir à distance, ce qui se passe sur le théâtre des opérations selon le Directeur Général de l'ADIE.

L'ADIE a aussi appuyé le MSAS dans la lutte contre le COVID-19, à travers la mise à disposition de téléphones intelligents eLTE, pour la coordination des opérations sur le terrain, la mise en place de la plateforme de sensibilisation et

8 Décret n° 2020-830 du 23 mars 2020 proclamant l'état d'urgence sur le territoire national **:** https://www.sec.gouv.sn/actualit%C3%A9/d%C3%A9cret-n%C2%B0-2020-830-du-23-mars-2020-proclamant-l%E2%80%99%C3%A9tat-d%E2%80%99urgence-sur-le-territoire-national

9 Constitution du 7 janvier 2001 (JORS, n° 5963 du 22 janvier 2001).

10 Le petit Larousse illustré, Larousse HER 2000, p. 546.

11 *Cheikh Bakhoum, Directeur de l'ADIE:* https://cio-mag.com/covid-19-ladministration-en-mode-teletravail-grace-a-des-outils-mis-en-place-par-ladie-au-senegal/

12 DECRET n° 2011-1158 en date du 17 août 2011 modifiant le décret n° 2004-1038 du 23 juillet 2004 portant création et fixant les règles d'organisation et de fonctionnement de l'ADIE.

13 https://cio-mag.com/covid-19-ladministration-en-mode-teletravail-grace-a-des-outils-mis-en-place-par-ladie-au-senegal/

d'information covid19.gouv.sn[14] et d'un agent conversationnel, à travers le numéro de téléphone 76 600 05 26[15] pour répondre aux questions des populations en lien avec le coronavirus.

Les autorités sanitaires envisagent même le recours au digital pour le dépistage et le suivi des personnes contacts nécessitant la collecte de données personnelles[16]. C'est dans ce cadre, que le ministère a demandé l'avis de la Commission de Protection des Données à caractère Personnel (CDP) pour la mise en œuvre de solutions digitales e-santé et potentiellement de localisation.

Aussi le MSAS a mis en place un système de traçage téléphonique pour le suivi des cas potentiels de contamination, c'est ce qui avait permis d'établir que le cas communautaire[17] de Louga avait été infecté à Pikine[18]. Ce système de traçage pourrait être potentiellement attentatoire aux données personnelles et la vie privée.

C'est dans ce sens que la CDP a précisé dans un communiqué, que le traçage des données personnelles, relatives à la santé des personnes suivies, doit être mis en œuvre exclusivement par des professionnels de santé[19].

Malgré tout cela, on a noté une atteinte flagrante des données personnelles de santé dans la gestion de la crise. Il en est ainsi, du cas d'un célèbre artiste-comédien sénégalais testé positif au coronavirus et faisant partie de la liste de patients en réanimation[20] selon les informations du site surleterrain.sn. Cela pose donc le problème non seulement de la confidentialité, mais également celui de l'accès aux données personnelles des patients.

Toutefois, il importe de rappeler que la diffusion des cas de coronavirus ne doit pas en aucun cas porter atteintes aux droits humains en ligne.

Par conséquent, la protection des données à caractère personnel doit demeurer applicable quel que soit l'urgence aussi bien pour l'identification et le suivi des personnes infectées.

---

14 Cette plateforme donne aux citoyens toutes les informations relatives au coronavirus, l'évolution, les statistiques, les conseils dans le cadre de la prévention.

15 Le MSAS, en collaboration avec l'ADIE lance la plateforme covid19.gouv.sn et le chatbot Docteur Covid via WhatsApp

16 https://www.socialnetlink.org/2020/04/covid-19-et-donnees-personnelles-au-senegal-la-cdp-se-prononce/

17 Selon le MSAS, l'utilisation de la technologie pour retracer le parcours de chaque cas communautaire est prévue, même si cela nécessitera une législation spéciale par rapport aux données personnelles : http://emedia.sn/VIDEO-LES-PARCOURS-DES-CAS-COMMUNAUTAIRES-SERONT-TRACE

18 https://senego.com/cas-communautaires-le-tracage-telephonique-autorise-par-la-cdp_1081172.html.

19 https://www.senegalinfos.com/covid-19-tracage-des-cas-communautaires-la-commission-de-protection-des-donnees-personnelles-pose-des-conditions

20 https://laviesenegalaise.com/le-comedien-samba-sine-alias-kouthia-teste-positif-au-coronavirus/

Du point de vue social, il est important de retenir que la distanciation sociale fait partie des mesures efficaces dans le cadre de la lutte contre le coronavirus. Ce n'est pas pour autant que les activités professionnelles et étatiques doivent cesser. Dès lors, la technologie devient ce connecteur logique entre les personnes physiques et morales, les institutions[21]. Le Sénégal, pays de plus en plus tourné vers la technologie numérique et digitale, ne déroge pas à cette règle.

C'est dans ce cadre que le Chef de l'État a décidé, à partir du 1er avril 2020, et jusqu'à la fin de la pandémie du COVID-19, de la tenue de la réunion hebdomadaire du Conseil des Ministres en visioconférence. Pour la mise en œuvre du Smart Conseil des Ministres, l'ADIE a déployé dans plusieurs sites, un dispositif de visioconférence qui permet aux différents participants de communiquer tout en partageant des documents.

Au surplus, l'ADIE propose à toute l'Administration des outils de télétravail tels que la messagerie administrative, la plateforme OPTICA, l'outil de conférence sur internet web-conférence ou encore le Système électronique de Gestion du Courrier (SyGEC).

En réalité, le coronavirus ne doit pas pour autant être à l'origine de la cessation des activités professionnelles.

Cependant, étant donné que cette technique de captation d'images et de sons, collecte un certain nombre de données personnelles, celle-ci doit se faire dans le strict respect de la vie privée et surtout de la loi sur la protection des données à caractère personnel.

C'est pourquoi, des garanties particulièrement solides de politiques de confidentialité sont nécessaires pour s'assurer de la sécurité des droits humains en ligne.

Sur le plan économique, le Sénégal a mis en place un Programme de Résilience Économique et Sociale (PRES), d'un coût global de 1000 milliards de FCFA, soit environ 2 milliards de dollars US, en vue de lutter contre la pandémie et soutenir les ménages, les entreprises. L'État du Sénégal a créé également un Fonds de Riposte contre les effets du COVID-19, FORCE-COVID-19, financé par l'État et des donations volontaires, pour couvrir les dépenses liées à la mise en œuvre du PRES.

Aussi, pour permettre aux Sénégalais de la diaspora de bénéficier des fonds qui leur sont dédiés dans le cadre de l'initiative Force COVID-19 lancée par le Président de la République, le Ministère des Affaires Étrangères et des Sénégalais de l'Extérieur (MAESE), avec l'appui de l'ADIE, a mis en place la plateforme d'aide à l'inscription de la diaspora[22].

21 https://www.adie.sn/actualites/lutte-contre-le-covid-19-apr%C3%A8s-le-e-conseil-le-gouvernement-du-s%C3%A9n%C3%A9gal-d%C3%A9roule-le-smart

22 https://forcecovid19diaspora.sec.gouv.sn/formulaire,

Ce dispositif de formalisation numérique vient en complément du dispositif papier toujours valide dans les pays de résidence des Sénégalais de l'extérieur. Le service est accessible sur tout type de terminal au travers d'un navigateur. Il a été conçu pour être facilement utilisable par les personnes en situation de handicap[23].

Selon le MAESE, des dispositions sécuritaires ont bien été prises en compte pour protéger les données personnelles. En effet, les données personnelles collectées sont stockées sur les serveurs de l'État et protégées par la loi n°2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel.

Même si la sécurité numérique est portée au rang des priorités de l'action gouvernementale, la maîtrise effective des textes législatifs et réglementaires doit être précédée d'une réforme significative et digne de ce nom pour garantir les droits fondamentaux. Pour rappel, l'avant-projet de loi 2020 relative à la protection des données à caractère personnel en remplacement de la loi de 2008 est en cours. Cet avant-projet a pour objectif d'apporter une innovation majeure dans le système de protection des données personnelles.

Au plan juridique, face au constat d'une importante progression de la pandémie préjudiciable aux citoyens, l'ADIE en partenariat avec Facebook a mis au point un *chatbot* permettant de lutter contre les fausses nouvelles concernant la pandémie COVID-19. Ce point est d'autant plus crucial pour le gouvernement que les fake news se multiplient depuis l'avènement de la pandémie. Aujourd'hui, le Sénégal compte plus que jamais à mener la lutte sur le terrain physique comme sur la Toile.

Quoi qu'il en soit, la lutte contre les fausses nouvelles doit tenir compte des exigences de la Déclaration de principes sur la liberté d'expression et l'accès à l'information en Afrique[24].

Dans le but de lutter contre les fausses nouvelles en ligne, la plateforme COVID19.gouv.sn mise en place par l'ADIE, fournit des informations fiables sur COVID-19, des conseils pratiques et des vidéos de sensibilisation, ainsi que des statistiques sur la propagation du virus via un tableau de bord interactif montrant les données pour chaque localité. Les Sénégalais peuvent également signaler un cas d'infection via la plateforme covid19.gouv.sn.

Convaincu que les fausses infos sont dangereuses, le législateur sénégalais, à travers l'article 255 du Code pénal sanctionne la publication, la diffusion, la divulgation ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses.

---

23 https://www.adie.sn/actualites/force-covid19-diaspora-la-plateforme-dinscription-lanc%C3%A9e%C2%A0

24 https://www.achpr.org/public/Document/file/French/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_FRE_2019.pdf

Toutefois, nous estimons nécessaire que la répression des fake news soit bien encadrée et qu'une définition claire et acceptée soit donnée aux fausses nouvelles, pour ne pas restreindre la liberté d'expression sur internet et l'accès à l'information ou envoyer en prison ceux qui ne font qu'exprimer leur opinion non admise[25].

En effet, des Sénégalais ont fait l'objet d'enquête à la gendarmerie simplement pour avoir exprimé leur opinion sur la pandémie COVID-19 pour nier son existence[26].

Ainsi, pour se conformer à la Déclaration Africaine des Droits et Libertés de Internet, il importe de tenir en compte ce principe fondamental: « Toute personne a le droit d'avoir des opinions sans ingérence aucune. Toute personne a droit à la liberté d'expression sur l'Internet, ce qui implique le droit de rechercher, de recevoir et de répandre des informations et des idées, sans considération de frontières. Le droit à la liberté d'expression sur Internet ne peut être soumis à aucune restriction, sauf celles prévues par la loi, pour un objectif légitime, nécessaires et proportionnées dans une société démocratique, conformément aux normes internationales en matière de droits de l'homme »[27].

CONCLUSION

Telles qu'elles fonctionnent depuis des mois, les politiques sénégalaises de lutte contre la pandémie COVID-19 et leur impact sur les droits humains en ligne ont réussi à assurer une stabilité certes précaire mais contrôlable dans une large mesure.

L'analyse des politiques nationales de prévention, de confinement et de traitement du COVID-19, nous a permis de constater que les mesures sanitaires, sociales, économiques et juridiques mises en synergie par le gouvernement apportent leur pierre à l'édifice, et aident les populations à supporter les conditions difficiles de la pandémie.
Il ne faut cependant pas perdre de vue que les technologies numériques utilisées pour la gestion de la crise peuvent parfois se révéler dangereuses sur la vie privée des citoyens en général et des personnes atteinte du virus SARS-COV-2 en particulier. La gestion de la pandémie par l'usage des technologies numériques peut également porter atteinte à la liberté d'expression sur internet et du droit à l'information.

25 https://www.igfm.sn/plainte-du-ministere-de-la-sante-mbaye-pekh-convoque-par-la-section-de-recherches

26 https://www.dakaractu.com/SECTION-DE-RECHERCHES-Fallou-Galass-Sylla-s-explique%C2%A0Moustapha-Messere-promet-une-video-Selbe-Ndom-s-excuse-Gana_a185498.html

27 https://africaninternetrights.org/wp-content/uploads/2014/09/Declaration-French_28-Aug-2014.pdf

Quoi qu'il en soit, le traitement de données à caractère personnel doit être proportionnel aux objectifs poursuivis par la Déclaration Africaine des droits et libertés de l'Internet et de l'article 35 alinéa 2 de la loi de 2008 sur les données à caractère personnel : les données personnelles « doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement ».

Ainsi donc, pour les politiques sénégalaises de lutte contre la pandémie COVID-19, qui impliquent l'usage des technologies numériques en rapport avec les droits de l'homme en ligne, nous recommandons aux parties prenantes (État, secteur privé et société civile) que :

- L'usage des technologies numériques tienne compte du respect fondamental des droits et libertés des personnes humaines notamment la liberté d'expression et d'opinion en ligne ;

- Toute restriction au droit à la vie privée soit prévue par la loi et soit proportionnelle, légitime, et nécessaire. L'État doit s'engager à ne pas porter atteinte à la vie privée des personnes infectées dans le cas de la gestion de la pandémie du COVID-19 ;

- Les politiques nationales de lutte contre le coronavirus respectent le droit à la protection des données à caractère personnel ; les impératifs d'éradication de la pandémie soient conciliés avec le respect des droits numérique ;

- Les organisations de la société civile, devraient continuer à jouer un rôle clé en matière de défense et de protection des droits humains en ligne comme le prévoit la Déclaration Africaine des droits et liberté de l'Internet ;

- Le renforcement des capacités à l'intention des parties prenantes (État, secteur privé et société civile) sur le respect de la liberté d'expression et de la confidentialité des correspondances et de l'accès à l'information vraie en période de crise sanitaire afin de construire une société de l'information respectueuse des droits humains en ligne.

Mask or muzzle: The impact of COVID-19 measures on digital rights in Kenya

Author: Francis Monyango | Country: Kenya

INTRODUCTION

When we first heard of COVID-19 and how it was ravaging Europe, we did not think that it would have a great impact on our laws, especially digital rights. The expectation was more on the government imposing limitations on freedom of assembly, to enforce social distancing, and on the right to privacy, since contact tracing involves sharing people's personal information with third parties. Upon the confirmation of the first COVID-19 case in Kenya, the government swung into action by enacting various pieces of legislation and measures. While the measures were well intended, the manner in which existing laws have been interpreted during this COVID-19 period has proved the adage that the road to hell is paved with good intentions.

THE SYSTEMATIC SHRINKING OF THE DIGITAL RIGHTS SPACE

In this article, I will discuss the COVID-19 measures that touch on digital technologies and their impact on digital rights as stated in the African Declaration on Internet Rights and Freedoms.[1] I will then show how existing laws have been implemented during this COVID-19 period in ways that undermine digital rights also contained in the African Declaration. The last part of the article will discuss what Kenya needs to do when implementing COVID-19 measures without unnecessary infringements to people's digital rights.

THE ADVENT

In late February, a Kenya Airways staff member was suspended for filming a China Southern Airlines plane landing with 239 passengers at the Jomo Kenyatta

1 https://africaninternetrights.org

International Airport. The video, which was shared online, led to an uproar by Kenyans. This prompted three court petitions by the Law Society of Kenya, two doctors and a lawyer who quickly secured court orders suspending flights from China for 10 days because of the coronavirus concerns.[2]

Weeks later, the Ministry of Health confirmed Kenya's first COVID-19 case in Nairobi on 12 March 2020. The case was of a Kenyan citizen who had travelled back to Nairobi from the United States via London, United Kingdom on 5 March 2020.[3]

THE POLICY MEASURES

As soon as this was announced, the government swung into action by invoking public health measures such as asking companies to allow their staff to work from home, travel restrictions, closing schools, suspending of public gatherings, and a nightly curfew to delay the spread of the disease, while the country ramped up investment in its health care systems.[4] The law used was the archaic Public Health Act of 1921.[5]

These measures were introduced through subsidiary legislation and presidential orders and they limited the exercise of people's rights and liberties such as the right to privacy and freedom of assembly and movement, among many others. Other measures included encouraging the use of cashless payment systems such as mobile money in transactions.

Cashless payments

In a bid to encourage social distancing, President Uhuru Kenyatta encouraged players in the financial sector to explore ways of deepening mobile money usage to reduce the risk of spreading the virus through physical handling of cash. This directive plus a meeting between Safaricom and the Central Bank of Kenya led to the company announcing that all person-to-person transactions under KES 1,000 (USD 10) would be free for 90 days. The company also allowed small and medium-sized enterprises (SMEs) to increase their daily M-Pesa mobile money transaction limits from KES 70,000 to KES 150,000 (USD 700 to USD 1,500).

These measures had an impact, and the Central Bank of Kenya governor, Patrick Njoroge, stated in a presentation in May that there was a significant increase in

2 Wangui, J. (2020, 18 March). Coronavirus: Suspended KQ employee eyes court. *Daily Nation*. https://www.nation.co.ke/kenya/news/coronavirus-suspended-kq-employee-eyes-court-255684

3 Ombuor, R. (2020, 13 March). Kenya Confirms First COVID-19 Infection. *VOA*. https://www.voanews.com/science-health/coronavirus-outbreak/kenya-confirms-first-covid-19-infection

4 World Bank (2020, 29 April). COVID-19 Dampens Kenya's Economic Outlook as Government Scales up Safety Net Measures. https://www.worldbank.org/en/news/press-release/2020/04/29/covid-19-dampens-kenyas-economic-outlook-as-government-scales-up-safety-net-measures

5 http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%20242

transaction volumes and values. The KES 101-500 and KES 501-1000 bands had recorded an increase of 857,341 and 692,385 more transactions, respectively. These statistics confirmed that the waiver of fees for up to KES 1,000 encouraged more mobile money transactions. The new band of KES 70,001 to KES 150,000 also recorded an increased average of 19,949 transactions per week. The increase in values of bank to e-wallet transfers shows that there is some success in the measure of reducing use of physical cash by Kenyans.[6]

Access to the internet and Google Loon

President Uhuru Kenyatta approved Google Loon services in Kenya to enable universal 4G data coverage in the country. The president said that the approval was in line with the government's measures to respond to the disruptions caused by the COVIC-19 pandemic that has seen many people work from home to avoid contracting the respiratory illness.[7] In this project, Google Loon is partnering with government-owned mobile network operator Telkom to provide internet connectivity to areas that are typically underserved, using high-altitude balloons with solar-powered cellular network gear on board, replacing the need for permanent tower infrastructure in environments where that option is either not practical or unaffordable.[8]

This measure is in line with Principle 2 of the African Declaration on Internet Rights and Freedoms, Internet Access and Affordability, which states that access to the internet plays a vital role in the full realisation of human development. The principle calls on states to facilitate high-speed internet access, such as by establishing necessary infrastructure, while making it as affordable as possible. The Google Loon project gives life to this principle during this time where internet access is needed for people to work from home as they practice social distancing.

The measure also aligns with Principle 7, which provides for the right to development and access to knowledge. Internet access at this time is crucial to enable school-going children to learn from home, as we figure out how life will go on with the COVID-19 pandemic.

IMPACTS ON THE RIGHT TO PRIVACY

Self-quarantine enforcement through mobile surveillance

As soon as it locked its borders, the Kenyan government started using electronic surveillance to monitor individuals who had sworn to self-quarantine after

6 Central Bank of Kenya. (2020). Presentation on the Status and Outlook of Kenya's Banking Sector. www.centralbank.go.ke/uploads/presentations/1483113962_PRESENTATION%20ON%20KENYA'S%20BANKING%20SECTOR%20SITUATION%20AND%20OUTLOOK.pdf

7 Presidency of Kenya. (2020, 23 March). Kenya Approves Roll Out Of Google Loon 4G To Mitigate Coronavirus Work Disruptions. https://www.president.go.ke/2020/03/23/kenya-approves-roll-out-of-google-loon-4g-to-mitigate-coronavirus-work-disruptions

8 Jackson, E. (2020, 23 March). Kenya Approves Google's Loon Internet Project. *The Kenyan Wall Street*. www.kenyanwallstreet.com/kenya-approves-googles-loon-internet-project/

returning from countries ravaged by the novel coronavirus. The surveillance was to ensure that the individuals did not step out of their quarantine locations. Those who swore to self-quarantine were supposed to state where they would do so and were not supposed to switch off their gadgets. Those who breached the movement restrictions were picked up by medical personnel and police and taken to government-run quarantine centres.

The Standard newspaper reported about a woman who had come from the UK and promised to self-quarantine for 14 days but went to her workplace. Security agencies tracked her to her office and took her to a government medical facility.[9] The real-time monitoring of people's movements in Kenya through their mobile phones is only permissible through an investigation warrant.[10] With the COVID-19 pandemic, this targeted surveillance became normal.

The National Transport and Safety Authority (NTSA) contact tracing (passenger manifest) with payment gateway services tender

Despite hailing itself as the Silicon Savannah due to the wide use of mobile devices, Kenya, like many other countries, did not bother with a contact tracing application. This is due to peculiar factors in the mobile economy such as the widespread use of feature phones, which cannot work with such a measure. Many Kenyans, however, use public transport, where they are exposed to other people, some of whom may be infected with COVID-19. In May, the National Transport and Safety Authority (NTSA) published terms of reference for prequalification of service providers who would provide it with contact tracing (passenger manifest) with payment gateway services. This was aimed at achieving compliance with the presidential directive on cashless payments and at the same time providing for deployment of an effective contact tracing application.[11]

The Authority intends on introducing mandatory use of cashless payment for all public service vehicles as permitted by the law, which authorises them to impose any such conditions on the licence to secure the safety and convenience of the public.[12]

Principle 8 of the African Declaration states that everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. The principle requires targeted surveillance of online communications to be governed by clear and transparent laws.

---

9 Ombati, C. (2020, 24 March). State taps phones of isolated cases. *The Standard*. https://www.standardmedia.co.ke/nairobi/article/2001365401/state-taps-phones-of-isolated-cases

10 Section 52, Computer Misuse and Cybercrimes Act. http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018

11 www.ntsa.go.ke/2020/notices/TOR%20Contact%20Tracing.pdf

12 Section 30 (2) of the National Transport and Safety Authority Act. http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2033%20of%202012

While the Declaration requires that communications surveillance must be both targeted and based on reasonable suspicion of commission or involvement in the commission of serious crime and judicially authorised, it does not anticipate situations where surveillance may be needed for public health purposes, like now. And it is at this point that the principles of privacy by design, informed consent and the purpose limitation in data protection law are supposed to be alive.

Contact tracing technologies, when deployed, should only collect the most necessary and least intrusive data from the people under surveillance. This intentional purpose limitation will ensure that a public health activity does not turn into a mass surveillance activity. People need to be adequately informed of the limitations to their right to privacy during this COVID-19 period due to contact tracing and there must be full enactment of the data protection law. A similar approach was recommended by the United States Supreme Court, which held that public health surveillance and reporting are only permissible when they are directly linked to the preservation of health. Access to health information and records systems should still respect a patient's confidentiality and privacy.[13]

IMPACTS ON FREEDOM OF EXPRESSION

"Fake" and or "misleading" COVID-19-related information

Blogger Cyprian Nyakundi was arrested for allegedly posting on Twitter that a top tax authority official travelled abroad and failed to self-quarantine on his return. He is not the only blogger who has been arrested for COVID-19-related posts. Blogger Robert Alai was also arraigned before a court of law for allegedly publishing false information about the novel coronavirus on his social media platform. A civilian who goes by the name Elijah Muthui Kitonyo was arrested in Mwingi town for allegedly publishing false information that could result in panic on social media.[14]

In what can be said to be favouritism, a member of parliament (MP), John Kiarie of Dagoretti South, wrote a Twitter thread claiming that 7,000 people were quarantined by the government in various facilities. Health Cabinet Secretary Mutahi Kagwe refuted his claims, saying the figure was grossly exaggerated. The MP was summoned by the police and he presented himself to Kabete Police Station. After being questioned, he agreed to clarify and apologise for his post. The MP was not charged like other persons arrested for posting similar things online.[15]

The Computer Misuse and Cybercrimes Act contains a provision that makes it an offence to publish information that is false over a computer system, so as

13 *Planned Parenthood of Central Missouri v Danforth.* https://www.law.cornell.edu/supremecourt/text/428/52

14 Ongeri, L. (2020, 30 May). COVID-19: Freedom of expression, power and rule of law. *iFreedoms Kenya*. https://www.ifree.co.ke/2020/05/covid-19-freedom-of-expression-power-and-rule-of-law

15 Ibid.

to cause panic, chaos or violence among citizens of the republic. The provision also makes it illegal to discredit the reputation of a person. Those found guilty of committing this offence shall on conviction be liable to a fine not exceeding KES 5,000,000 (USD 50,000) or to imprisonment for a term not exceeding 10 years, or to both.[16]

The Bloggers Association of Kenya had gone to court to challenge 26 sections of the Computer Misuse and Cybercrimes Act which contravened rights enshrined in the constitution, such as freedom of expression, opinion and the media. They managed to get these 26 sections suspended.[17] However, in February 2020, Justice Makau dismissed the whole case as he found the law valid and constitutional.[18] The Bloggers Association of Kenya has since then appealed the judgement at the Court of Appeal.

False advertising

Dr. Pranav Pancholi and Sylvia Ndinda, both of Avane Dermatology Cosmetic Clinic and Medical Spa, were arraigned at the Milimani Law Courts following their arrest by Directorate of Criminal Investigations officers and the Kenya Medical Practitioners and Dentists Board for publishing a false advertisement on social media regarding COVID-19 rapid self-test kits. The two had published an advert selling self-test kits for early diagnosis that offered results in 15 minutes. The advert also alleged that the test required no special facility or equipment, required no special training to use, and combined an antibody test for COVID-19.

False advertising is a crime and is prohibited in the Consumer Protection Act, 2012, which shields consumers from unprofessional practices by businesses. The two suspects pleaded not guilty and were released on bail.[19]

Cyberbullying

Kenya's first COVID-19 recovery patient, Brenda Ivy Cherotich, who was also patient zero, was heavily bullied by Kenyans online after she came forward to speak to Kenyans on her recovery journey. A section of Kenyans online took to social media to discredit and question the truth in her story. Some went to the extent of sharing her personal conversations and nude images, which led to her being heavily trolled and bullied online.[20]

---

16 Section 23, Computer Misuse and Cybercrimes Act. http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018

17 Wangui, V. (2018, 30 May). BAKE is successful after court suspends 26 sections of the Computer Misuse and Cybercrimes Act. *iFreedoms Kenya*. https://www.ifree.co.ke/2018/05/bake-is-successful-after-court-suspends-26-sections-of-the-computer-misuse-and-cybercrimes-act

18 Bloggers Association of Kenya (BAKE) v Attorney General & 5 others [2018] eKLR.

19 Ongeri, L. (2020, 18 March). Two accused of allegedly advertising fake Covid-19 test kits on social media. *iFreedoms Kenya*. https://www.ifree.co.ke/2020/03/two-accused-of-allegedly-advertising-fake-covid-19-test-kits-on-social-media

20 Ongeri, L. (2020, 3 April). Brenda Ivy Cherotich and Yvonne Okwara victims of cyberbullying in recent times. *iFreedoms Kenya*. https://www.ifree.co.ke/2020/04/brenda-ivy-cherotich-and-yvonne-okwara-victims-of-cyberbullying-in-recent-times

This angered Health Cabinet Secretary Mutahi Kagwe, who expressed his disappointment that the efforts of the health authorities and the two recoveries were viewed as public relations gimmicks. He even called on the police to arrest social media abusers. TV personality Yvonne Okwara called the actions on social media shameful and this also put a target on her back, with Kenyans on Twitter harassing her as well. The Computer Misuse and Cybercrimes Act contains a provision on cyber harassment but no one is on record for being arrested and charged for cyber harassment during this COVID-19 pandemic period.[21]

Principle 3 of the African Declaration is on freedom of expression. This right includes freedom to seek, receive and impart information and ideas of all kinds through the internet and digital technologies and regardless of frontiers. The exercise of this right should only be limited by law, such as in the Kenyan situation, where the Constitution of Kenya is clear on limitations to the right to freedom of expression. The principle mentions the limitations listed under international human rights law (namely the rights or reputations of others, the protection of national security, or of public order, public health or morals), and adds that limitations must be necessary and proportionate in pursuance of a legitimate aim. The Kenyan Computer Misuse and Cybercrimes Act has a provision that reintroduces criminal defamation, and that is the provision that has been used to charge bloggers in Kenya.

RECOMMENDATIONS

Due to the emerging violations of online rights, privacy and freedom of expression, national policy-making bodies that are making law in response to COVID-19 should consider the following recommendations.

LEAD THE NARRATIVE

Threats to online rights in Kenya are from the application of existing laws. Section 23 of the Computer Misuse and Cybercrimes Act has had many social media users arrested and charged. The provision was one of the 26 provisions in the Act that had been suspended by the high court when the Bloggers Association of Kenya filed a case in court challenging their constitutionality. In the final judgement that was issued in early 2020, the case was dismissed, thus bringing the provision back to life. While it is in the state's best interest that there is accurate information out there, due to the prevalence of disinformation in this age, a proactive approach wins over policing speech.

The state should be the first to share all necessary information with its people and encourage healthy debate on issues. Being ahead of the narrative wins public trust and removes the vacuum in which misinformation thrives.

21 Section 27, Computer Misuse and Cybercrimes Act. http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018

FOLLOW THE LAW

The Constitution of Kenya has a very balanced approach to human rights. It is a social contract between the Kenyan people and the Kenyan government, thus any measure that limits people's rights due to the COVID-19 pandemic should be constitutional. The measures that work force the government to take seriously its socioeconomic obligations of access to health care and water. Curbing COVID-19 also entails limiting various rights such as the right to privacy and freedom of movement, expression and assembly. These limitations should be provided for by law and should pursue a legitimate aim as expressly listed under international human rights law, as stated in Principle 3 of the African Declaration.

PUBLIC PARTICIPATION

The 2010 constitution requires public participation in key decision-making processes. However, progress towards this goal has been slow. Participation is costly and difficult to manage, especially in a country that is large and ethnically diverse. In the wake of COVID-19, people can no longer convene. However, legislative government bodies are innovating ways of collecting public views. Many counties in Kenya are forming ward-level WhatsApp groups to enable the collection of public views from people for the public participation process.

Such brilliant ideas on how technology can be used for the public participation process should be included in the Public Participation Bill, which is still in parliament. Technology should be used to ensure that policy making is an inclusive process by giving people access to channels where they can voice their opinions on the various draft laws that will affect them upon enactment.

CONCLUSION

In this article, I have highlighted several measures that have impacted the exercise of civil rights and liberties in the digital sphere. Some of the measures have been positive, such as the promotion of cashless payments and mobile money in order to reduce contact with paper cash while encouraging social distancing. The other positive development has been the boost to internet access through the Google Loon project. Some measures have shown the government's surveillance capabilities and intentions, such as self-quarantine enforcement through mobile surveillance and the NTSA contact tracing and payment gateway services tender.

Incidents that affected digital rights are arrests due to the spread of "fake" and/or "misleading" COVID-19-related information. This came in the wake of a clampdown on disinformation by state agencies. Other unfortunate incidents were cases of cyber bullying against recovered COVID-19 patients.

All these affected the following principles in the African Declaration on Internet Rights and Freedoms:

- Principle 2. Internet Access and Affordability
- Principle 3. Freedom of Expression
- Principle 4. Right to Information
- Principle 7. Right to Development and Access to Knowledge
- Principle 8. Privacy and Personal Data Protection.

To ensure a proper balance is maintained while legislating on COVID-19, national policy-making bodies should proactively lead the narrative on all communications, follow the law, and engage members of the public when legislating. This will ensure that the government gets full support from the citizens in its fight against COVID-19.

INTERNET ACCESS AND AFFORDABILITY

COVID-19 exposes the damage of the ex-regime's empowerment policy on ICTs and the impact of US sanctions against Sudan

Author: Wala Mohammed | Country: Sudan

For decades, the internet has not reached all areas in Sudan; this year, out of a total population of 43 million, only 13.38 million are internet users. This is evidence that neither the previous nor current rulers made real efforts to implement the principles of the African Declaration on Internet Rights and Freedoms,[1] such as citizens' rights to access information on the internet, and that internet access should be available and affordable to all.

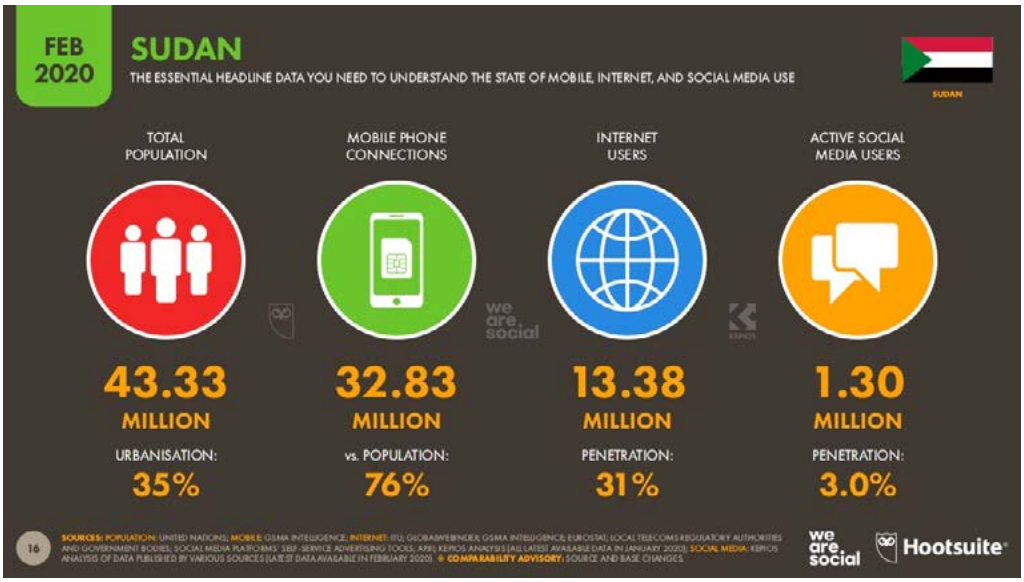
The transitional government has yet to fully utilise information and communications technologies (ICTs) in developing the country's economy, health systems and education. This is due to several reasons, including the most significant reason which is the US sanctions against Sudan.

Sudan is now in the first year of the three transitional periods that started in August 2019, following eight months of peaceful demonstrations to remove the dictatorial regime of Omer Al-Bashir. Although the number of internet users has increased in Sudan, online public services and information are not yet available to serve citizens' rights to information. The inherited ICT infrastructure, systems and policies from the ex-regime restrained the transitional government's response to the COVID-19 pandemic. However, ministers are currently struggling to find systems that could support their decision making.

The Federal Ministry of Health (FMoH) has announced a national COVID-19 response plan at a cost of USD 76 million, while only 200 million Sudanese pounds (USD 3.6 million) have been pledged by the businessmen's union, telecommunication companies and the banking union. Also, the FMoH in

1 https://africaninternetrights.org/articles

coordination with telecommunications companies sent text messages to users on preventing the spread of COVID-19 and raising awareness.



Left: Sudan
Source: United Nations

According to a UN Office for the Coordination of Humanitarian Affairs report,[2] the first COVID-19 case in Sudan was confirmed on 13 March. Thereafter, Sudan's Transitional Government closed all ports, airports and land crossings and declared a public health emergency. The government ordered an inter-state public transportation halt, and a countrywide-imposed curfew, on 30 March. Following this, on 18 April, authorities established a total lockdown, with people allowed to purchase essential goods between the hours of 6:00 a.m. and 1:00 p.m.[3]

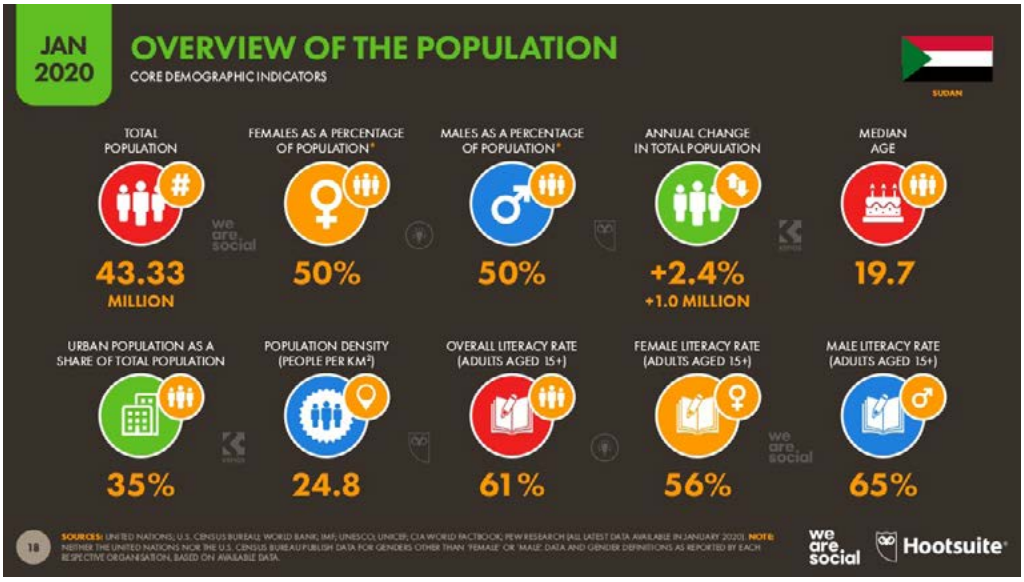
WOMEN ARE THE MOST AFFECTED BY THE LOCKDOWN

Before the spread of COVID-19, on 8 March 2020, feminists groups were protesting to change the Personal Status Law instituted by the previous regime.[4] The law contains oppressive articles on marriage, divorce and spousal obedience, which means a husband's permission is needed for work and travel. This law has affected women's access to education and their ability to be financially self-sufficient. Sudan's laws facilitate and encourage child marriage, giving it an Islamic legitimacy, but there are no open data policies which will allow citizens to access information that reveals the number of young girls who were forced to get married, before and during the lockdown.

2 https://reports.unocha.org/en/country/sudan

3 HCT/UNCT. (2020). *Sudan COVID-19 Country Preparedness and Response Plan.*https://www.reliefweb.int/sites/reliefweb.int/files/resources/200504_Sudan%20HCT-UNCT%20Covid-19%20Plan.pdf

4 Saleh, S. (2020, 10 March). Sudanese Women Call For Amending the Country's Personal Status Law. *Asharg Al-Awsat.* https://english.aawsat.com/home/article/2172347/sudanese-women-call-amending-countrys-personal-status-law



Left: Overview of the Population
Source: United Nations

Supporting women online is close to impossible, particularly those who are vulnerable to violence, and those working in the informal sector.[5] Unfortunately, the majority of women cannot afford digital devices and are not digitally literate. Many women also lack the confidence to use digital technologies, due to educational, cultural and financial factors which contribute to the gender digital divide.

Before the lockdown, one used to see women with tea and food stands scattered all over the city earning pension money. These ladies are among the most marginalised groups in terms of the absence of laws that protect them in their workplace from gender-based violence and the security forces. Still, they face violence from the security forces during the lockdown, after the majority of them slowly got back to the streets when they were confronted with financial hardships due to the lockdown extension.

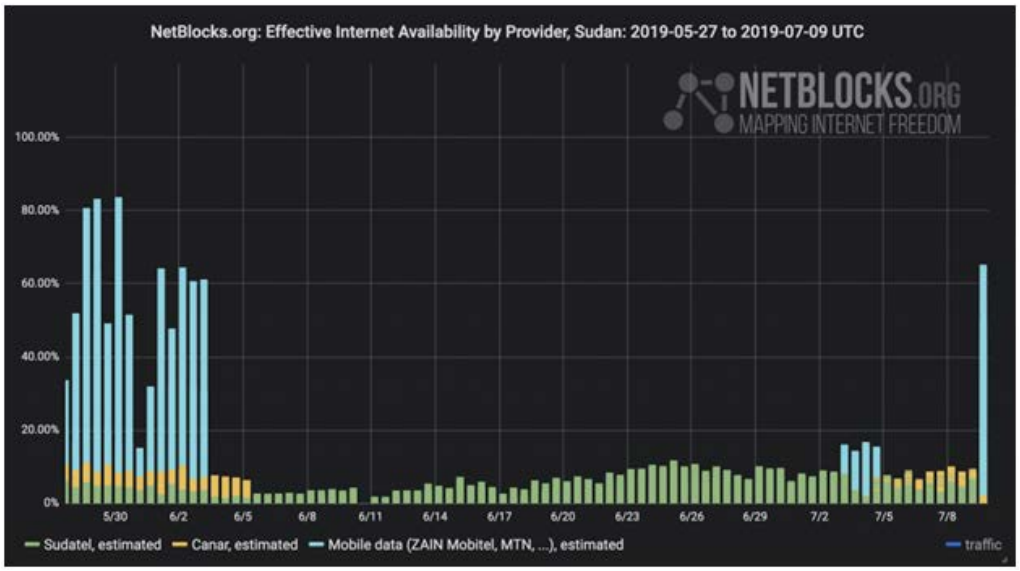
After more than 60 days of complete lockdown, the Ministry of Labour and Social Development, together with the Supreme Committee for Health Emergencies, faced challenges to reach out and support about 15,000 women with their families. About 12,000 of them have submitted their data and contact details. However, the ministry does not have the technical solutions that support the distribution of resources, and most of those women still do not have bank accounts or digital devices.

Lately, this situation sparked several questions and complaints by members of the women's union, with a representative of the "tea ladies" saying in an interview (translated):

5 UNFPA. (2020, 22 March). Sudan GBV Sub Sector Guidance on Covid-19, 1st Bulletin. https://www.humanitarianresponse.info/fr/operations/sudan/document/sudan-gbv-sub-sector-guidance-covid-19-1st-bulletin-22-mar-2020

> We demand that the transitional government and the Supreme Committee for Health Emergencies acknowledge our rights to dignity and safety and fulfil their obligations towards women working in the informal sector and on the outskirts of Khartoum, even women outside the union, to provide them with assistance in light of the continued implementation of the curfew and to cooperate with the union in providing aid and consumer goods.[6]

Although about 60% to 70% of the people on the frontlines of the revolution that took Bashir down were women, the transitional government continues to ignore their representation in the transitional government. Politics are still dominated by men from political parties, civil society and the military, negotiating the country's political future, and women once again have been pushed aside.



Left: Effective Internet Availability by Provider, Sudan
Source: Netblocks.org

THE IMPACT OF THE EX-REGIME'S EMPOWERMENT POLICY ON INTERNET RIGHTS AND DEVELOPMENT

In 1989, the Sudanese government was overthrown in a military coup led by an army brigadier, Omer Al-Bashir. His regime was inviting new members to pledge loyalty to his political party, targeting civil society and union leaders, as well as members of the military itself. There were "ghost houses" in residential areas across the country that were dedicated to torturing those who disobeyed the regime's orders. Slowly, the government's network extended and became a source of strength. The regime's allies were given rewards with positions at universities, in government, the national intelligence service, media, private sector, telecom sector, the civil service and the diplomatic corps. The army became politicised and subordinated to the regime. There were no more military leaders, only the regime's loyalists.

6 https://www.youtube.com/watch?v=ni99NSydVB4

In 1993, the government privatised the telecommunication sector and formed the National Telecommunication Corporation (NTC) under the Telecommunication Act in 2001.[7] The NTC is the federal regulatory authority of the information and telecommunication sector throughout the territories of the Republic of Sudan. The corporation has designated its functions and power to plans, policies and regulations for telecommunication services and to ensure their national availability, balanced development and the realisation of social and national objectives. The ruling regime appointed their associates at the NTC to pass the regime's orders; this is when the political activists, journalists and human rights defenders faced arbitrary detention by the National Security and Intelligence Service (NISS), who obtained their personal data and other information without complying with the basic principles of privacy and communication surveillance.[8] As reported in 2014 by The Citizen Lab:

> Sudan is one of 21 governments that are currently using or have used Hacking Team's RCS [remote control system] spyware. [...] Hacking Team distinguishes RCS from traditional surveillance solutions (e.g., wiretapping) by emphasizing that RCS can capture data that is stored on a target's computer, even if the target never sends the information over the Internet. RCS's capabilities include the ability to copy files from a computer's hard disk, record Skype calls, e-mails, instant messages, and passwords typed into a web browser. Furthermore, RCS can turn on a device's webcam and microphone to spy on the target.[9]

In August 2019, as part of the institutional reform, the Ministry of Information and Communications Technology was dissolved, exposing the regulatory body (NTC) to political interference by the Sovereign Council. Some institutions that were working under the ministry were moved: the National Telecommunication Corporation to work under the Sovereign Council, the National Information Centre under the Council of Ministers, and the Nile Center for Technology Research under the National Intelligence Service.

The various ICT bodies under different authorities are now working without proper policies, strategies and technical leadership aimed at serving the national security and development goals. Currently, the Ministry of Labour and Social Development is challenged to collect basic information about families that need financial support during the lockdown. Evidence of emergency response efforts have shown that the government is distributing food packages by depending on

---

7 NTC Sudan. (2006). *Sudan key indicators of the telecommunication/ICT sector.* ITU. https://www.itu.int/md/dologin_md.asp?id=D02-ISAP2B.1.1.1-INF-0007!!PDF-E

8 Abubkr, L. (2014, 10 April). Online surveillance and censorship in Sudan. *APC*. https://www.apc.org/en/blog/online-surveillance-and-censorship-sudan

9 Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J. (2014, 17 February). Mapping Hacking Team's "Untraceable" Spyware. *The Citizen Lab*. https://www.citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware

Left: Sudan Central Bureau of Statistics: Inflation rate
Source: tradingeconomics.com

resistance committees formed during the revolution in different neighbourhoods. However, the existing mechanism cannot effectively track the food packages distributed, or validate the actual numbers of all families supported.

On 10 May this year, intercommunal clashes broke out in Kassala state between the Nuba and the Beni Amer tribes.[10] Internet services were cut off for about three days on the three mobile phone network operators (Zain, MTN and Sudani) in the cities of Kassala,[11] while internet services were still available on the fixed Sudatel network. As is the case with other countries, the Telecommunication Regulatory Act 2018 is not precise about the justifiable limitations of freedom of expression that allow the government to cut off the internet.

The recent affiliation of the NTC to the Sovereign Council is a parlous indicator, especially since some members of the Sovereign Council were occupying positions within the Transitional Military Council, and were involved in shutting down the internet at the time of the Khartoum Massacre[12] for over a month. On 9 July 2019, Netblocks reported on the shutdown that "internet measurements confirmed that the new restrictions understood to have been ordered by Sudan's Transitional Military Council were more severe than those implemented during the rule of ousted president Omar al-Bashir."[13]

On the first anniversary of the Khartoum Massacre in June 2020, while the resistance committees and the family of martyrs committees across the capital city of Khartoum were preparing for the memorial, the ministries' websites were

10 Sudan Tribune. (2020, 10 May). 10 killed in fresh tribal violence in eastern Sudan. *Sudan Tribune*. https://www.sudantribune.com\spip.php?article69318

11 Mohammed Salih, Z. (2020, 25 May). Coronavirus in Sudan exposes new leaders. *BBC*. https://www.bbc.com/news/world-africa-52735520

12 Human Rights Watch. (2019, 17 November). "They Were Shouting 'Kill Them'": Sudan's Violent Crackdown on Protesters in Khartoum. https://www.hrw.org/report/2019/11/18/they-were-shouting-kill-them/sudans-violent-crackdown-protesters-khartoum#3086

13 NetBlocks. (2019, 9 July). Sudan internet shows signs of recovery after month-long shutdown. https://netblocks.org/reports/sudan-internet-recovery-after-month-long-shutdown-98aZpOAo

hacked for over eight hours by hackers named JanJaweb. They were posting updates on Twitter that they hacked the ministries' and academic institutions' websites. This incident carried a powerful message that the government's websites are not protected and that the transitional government must focus on establishing a technical and executive body/ministry that leads to securing

Left: Sudanese activists protest in Khartoum demanding amendments of the Personal Status Law
Source: Aawsat

national information.

US SANCTIONS AFFECTING THE RESPONSE TO THE COVID-19 PANDEMIC

In 1993, the United States designated Sudan as a state sponsor of terrorism,[14] a distinction currently shared by just two other countries, Iran and Syria. As a result, the US imposed economic and technological sanctions on Sudan, including certain restrictions on financial transactions and banking systems. Then, in 1997, the US issued an executive order that imposed a comprehensive trade embargo on Sudan and froze its government's assets in the US, claiming that the policies and actions of the government of Sudan included continued support for international terrorism and continuing efforts to destabilise neighbouring governments. In 2006, the US Department of the Treasury blocked the assets of Sudanese individuals involved in the violence and imposed sanctions on 30 companies owned or controlled by the government of Sudan.

In 2015, the US government issued a general licence to provide internet users with easy access to the internet, alongside a wide range of software, hardware and online services.[15] In January 2017, they temporarily lifted economic and trade sanctions against Sudan,[16] due to cooperation from the Sudanese government in

14 Prendergast, J., & Brooks-Rubin, B. (2016). *Modernized Sanctions for Sudan: Unfinished Business for the Obama Administration*. The Enough Project. https://enoughproject.org/files/Modernized_Sanctions_for_Sudan_042016.pdf

15 Kenyanito, E. P. (2015, 19 February). U.S. eases sanctions on tech exports to Sudan. *Access Now*. https://www.accessnow.org/us-eases-sanctions-tech-exports-sudan

16 Rosenberg, M. (2017, 17 October). U.S. Lifts Sudan Sanctions. *International Trade*. https://internationaltrade.foxrothschild.com/2017/10/articles/export-compliance/u-s-lifts-sudan-sanctions

fighting terrorism, reducing conflict, and denying safe haven to South Sudanese rebels, as well as improving humanitarian access to people in need. This was followed by the permanent lifting of all 1997 sanctions after Sudan cut all ties with the North Korean regime of Kim Jong Un. Finally, as of October 2017, the sanctions imposed by the United Nations Security Council in relation to the Darfur conflict remain in place.

Due to the comprehensive sanctions imposed on Sudan, the country has relatively small and fragile academic communities and low rates of investment in science, technology, engineering and mathematics (STEM). Most of the government institutions, civil society organisations, universities and the commerce sector are struggling to access ICTs and the internet to manage their business continuity during the lockdown. Even though the sanctions around communication technologies were lifted since 2015,[17] the trade embargo still impeded access to a long list of technologies and devices under the US Export Administration Regulations,[18] including electronics, computers, technology for civil end-use or civil infrastructure, telecommunications and information security technologies and free-of-charge systems for government use. All these items remain on the commerce control list and require legal authorisation to be exported or re-exported to Sudan.

On the other hand, the lifting of 20-year-old US sanctions has so far failed to produce a hoped-for boost in foreign investment. Sudan has a black market that has effectively replaced the formal banking system and is making the economic crisis more pressing, with a 114% inflation rate.[19] The US sanctions paralysed the country in coping with the technology revolution and hindered citizens' access to knowledge and enjoyment of their right to development.

RECOMMENDATIONS

TO THE US GOVERNMENT:

- The State Department must remove Sudan from the list of State Sponsors of Terrorism, and coordinate with the US Bureau of Industry and Security to increase the accessibility of items on the commerce control list, in order to translate existing norms to the digital age and to make it easier for both government and private companies to fully utilise the ICT infrastructure in developing the country.

17 U.S. Bureau of Industry and Security. (2015, 18 February). Revisions to License Exception Availability for Consumer Communications Devices and Licensing Policy for Civil Telecommunications-Related Items Such as Infrastructure Regarding Sudan. *Federal Register*. https://www.federalregister.gov/documents/2015/02/18/2015-03329/revisions-to-license-exception-availability-for-consumer-communications-devices-and-licensing-policy

18 https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations/sudan

19 https://www.take-profit.org/en/statistics/inflation-rate/sudan

- The US Bureau of Industry must announce and encourage the US tech companies to unlock online services in Sudan.
- The US Treasury must lift the remaining economic sanctions, to unlock the economy that has been long set in a stranglehold making it next to impossible for businesses to carry out US dollar transactions or to work with foreign banks and access loans from international institutions.

THE MINISTRY OF JUSTICE MUST:

- Implement the provisions of the Declaration of Principles on Freedom of Expression and Access to Information in Africa (the Declaration),[20] adopted in November 2019 by the African Commission on Human and Peoples' Rights. The Declaration requires states to adopt legislative, administrative, judicial and other measures to give effect to the provisions of the Declaration.

- Reform the ICT regulatory bodies' laws to be aligned with the Declaration, as well as giving the required privileges and authorities to the institution/ministry that will manage the sector.

THE TRANSITIONAL GOVERNMENT MUST:

- Address the equal representation of women, and establish a clear mechanism for hiring and selecting national talent from both women and men, especially while reforming the ICT sector where it is important to have female role models in technology.

- Reform the ICT sector to be supervised by the Council of Ministers, and consider the Declaration's principles 17 (regulatory bodies for broadcast, telecommunications and the internet), 36 (sanctions for withholding information), 37 (access to the internet), 41 (privacy and communication surveillance) and 43 (legislative and other measures to implement the Declaration).

- Ensure all regulatory bodies are independent and adequately protected from political, military or National Intelligence Services interference, including restructuring the Sudanese National Radio and Television Authority which is currently working under the Ministry of Media.

- Remove the Cyber Jihadist Unit from the NTC, and ensure that all remote control systems are removed, including the website that filters content or blocks access to websites and information.

20 https://www.achpr.org/presspublic/publication?id=80

- Develop open data policies that promote transparency and accountability, and allow citizens to create value from data provided.
- Develop and adopt ICT policies that will promote a conducive economic environment to foster an internet economy.

- Address the gaps that US sanctions caused in hindering the country's development, by 1) developing and integrating ecommerce policies and trade facilitation into its development agenda, to expand and diversify exports, and 2) ensuring simplified procedures using international standards and readiness of epayments infrastructure to stimulate cross-border ecommerce activity by Sudanese enterprises.

TO THE MINISTRY OF EDUCATION AND THE UNESCO SUDAN OFFICE:

- It is important that the Ministry of Education introduces ICTs in education to build capacity for the next generation that will equip them with digital literacy skills.

- The UNESCO Sudan office must support the efforts of the Ministry of Education to design and implement effective, evidence-based ICT programmes in education policies and master plans.

- The UNESCO Sudan office must support the ministry in effectively using ICTs to advance progress towards Education 2030 targets.

The shrinking of the digital space during the COVID-19 pandemic: Movement building and internet governance in North Africa

Authors: Sodfa Daaji And Rim Menia | Region: North Africa

INTRODUCTION

The analysis of the sphere of movement building and internet governance in North Africa leads inevitably to assess the shrinking of digital space and online mobilisation during the COVID-19 pandemic in the region.

North Africa – namely Algeria, Tunisia, Morocco, Western Sahara, Egypt, Libya and Mauritania – is a heated region of popular resistance and resilience movements. From the 1960s liberation wars against colonialism to the 2011 uprisings, and more recently the 2019 Algerian Hirak movement, the region has been characterised by a rise of popular pro-democracy movements.

Yet, the governmental response to this is usually characterised by oppressive mechanisms, repression against the freedom of speech and other violations of human rights. Despite the complexity of the North African civic space, these popular movements have been built online through information and strategy sharing, constructing the continuum of offline resistance in online spaces and drawing global attention and interest. However, the preventive measures due to COVID-19 are overturning, more than ever, the popular digital efforts aimed at maintaining the movements' continuum and momentum.

Analysis of the online movement building implies exposing the digital realities throughout the region. This assessment reveals that censorship of digital engagement still prevails, despite the pivotal role played by the internet in revealing the violation of human rights, and in providing an interactive platform for the people calling for freedom and dignity. During the preventive measures adopted throughout the region, the attempts at silencing the "dissidents" have risen.

Consequently, the most vulnerable individuals in a humanitarian crisis have been further exposed, while the fragile post-revolutionary settings are at risk of losing momentum, since the people have been disconnected from the political conversation. These failings are inevitably the result of an undefined judicial framework which does not fully protect the freedom of expression, resulting in several infringements of rights in the digital space.

Above: Sudanese activists protest in Khartoum demanding amendments of the Personal Status Law
Source: Aawsat

NORTH AFRICAN LANDSCAPE: BETWEEN A QUEST FOR DEMOCRACY AND AUTHORITARIANISM

North Africa is an interesting political, social and judicial contradiction that has been experiencing a shift in power dynamics since the 2011 uprisings in Tunisia, Libya and Egypt. Despite nine years of fervid socio-political resistance, the popular call for democracy, social justice and dignity has brought some horrific consequences to the region under oppressive regimes. A retrospective view would represent Libya as the common narrative regarding humanitarian catastrophes and armed conflicts and a peculiar situation of migrants and asylum seekers as well as a blurry political leadership. In another frame, Egypt has faced a failure paving the road to an authoritarian regime led by Abdel Fattah al-Sisi, after the removal of the long-time dictator Hosni Mubarak, worsening the socioeconomic situation.

If the shrinking of the civic space is a shared experience, two North African countries have remained passive to the popular uprisings. In fact, Mauritania's presidential transition in 2019,[1] the first in a decade, has raised hopes on ensuring human rights protection. However, persecutions of human rights activists and

1 Human Rights Watch. (2020, 14 January). Mauritania: Presidential Transition. https://www.hrw.org/news/2020/01/14/mauritania-presidential-transition

defenders and political dissidents is still frequent. In another context, the disputed Western Sahara, majoritarily occupied by Morocco and proclaimed as the Sahrawi Arab Democratic Republic by the Polisario Front, remains an unsolved political issue, as the referendums regarding its independence or integration with Morocco have always failed.[2] This conflictual situation threatens the stability of the region and results in a general atmosphere of suffocation as Sahrawi youth are severely affected by the lack of opportunities, violence and repression.

Despite the Sahrawi conflict, Morocco has been able to sedate internal uprisings in 2011 as well as the Rif Hirak Movement of 2016 while facing migrational issues reflecting diplomatic dynamics with neighbouring Spain. The successful democratic achievements of Tunisia's 2011 uprising have ensured major steps in the post-revolutionary context, including securing fair and free elections as well as accountability mechanisms and the reinforcement of civil society and online mobilisation at the forefront of organising and resisting against the leftovers of Ben Ali's regime. Similarly, the Algerian Hirak, a popular uprising of weekly protests since 22 February 2019 – which has been compared to the 2011 uprisings by Western media despite deep ideological and historical differences – has shifted power in the region and succeeded to remove the 20-year dictator Abdelaziz Bouteflika.

During the December 2019 electoral campaign, the newly elected president of Algeria, Abdelmadjid Tebboune, promised to revise the constitution. The constitutional amendments have been drafted and transmitted to political parties and representatives of pro-regime "civil society" for discussion while the country's political life is on standby due to the COVID-19 pandemic.

With common preventive measures among North African governments in response to the COVID-19 pandemic, a deteriorating trend has been identified with harmful consequences for digital engagement and activism. These responses have been shaped into coordinated guidelines towards repression and crackdown on opposition movements and activists in the region.

CENSORSHIP AND THE SHRINKING OF CIVIC SPACE DURING COVID-19

In the common narrative, the internet is considered as a window and a space for North African peoples, especially activists working in sensitive spaces of post-revolutionary and revolutionary dynamics. The role of the internet has been duly emphasised since the 2011 uprisings as the entire world has been "closely" watching the socio-political events in North Africa. From popular uprisings to identity and cultural struggles, the internet has been a pro-democracy mass mobiliser and a tool against censorship. It has seen the emergence of new forms and methodologies of engagement within the civic space, namely artivism and

2 https://www.unocha.org/middle-east-and-north-africa-romena/western-sahara

creative toolkits. These new forms and methodologies have been transformed into persecution tools serving power reinforcement and longevity of regimes, especially in the COVID-19 pandemic context.

On the national levels in Tunisia, Algeria and Morocco, the preventive health measures included the restriction of gatherings, including closing places of worship, restrictions on travel and imposing social distancing measures; a common effort within the global framework against the pandemic, including obligatory lockdowns and curfew. Ironically, only repression and oppression are not under lockdown, as the persecution of activists has increased drastically with the outbreak of the pandemic.

In Tunisia and within the economic measures that the government has designed to face the current health crisis, the internet has emerged in support of the people. In fact, in early April 2020, hundreds of people demonstrated in front of the local government offices across the country demanding the end of the lockdown and quick access to the promised governmental financial assistance. These protests have been documented by local activists and bloggers[3] who have later been arrested and detained. This was the case of the blogger and activist Anis Mabrouki, arrested on 14 April 2020 for live-streaming on Facebook a protest in front of the mayor's office in Tebourba, a town to the west of Tunis. Anis Mabrouki was charged with causing noises and disturbance to the public, and accusing public officials of crimes related to their jobs without furnishing proof of guilt, under Article 316 and Article 128 respectively of the Tunisian penal code.

In a similar experience, the activist Hajer Aouadi has been charged with insulting a civil servant under Article 125 and causing noises and disturbance to the public under Article 316 of the Tunisian penal code, following a video[4] posted on Facebook on 12 April 2020 accusing local authorities of corruption regarding the distribution of semolina, a staple food in North Africa. While Tunisia is nowadays shaped into a post-revolutionary democracy, the socio-political climate under the COVID-19 pandemic is similar to the one of the "ancien régime" under Ben Ali's rule. The government is allergic to criticism towards authorities' responses to the coronavirus, silencing journalists and online activists under the pretext of lacking patriotism or expertise. However, this is not a fresh approach in resorting to criminal laws; Amnesty International has documented a growing trend of violation of digital rights, threatening internet governance by using legislation that penalises freedom of speech – notably speech deemed to be offensive or defamatory not only towards individuals but also towards state institutions, as well as speech deemed liable to disturb the public order or morality.[5]

3 Noury, R. (2020, 21 April). COVID-19, Tunisia: Two Bloggers Arrested for Criticising Government. *Focus on Africa*. https://www.focusonafrica.info/en/covid-19-tunisia-two-bloggers-arrested-for-criticising-government and https://www.inhiyez.com/archives/2203

4 https://www.youtube.com/watch?v=VWEJznRo0KU

5 Amnesty International. (2020, 21 April). Tunisia: End prosecution of bloggers for criticizing government's response to COVID-19. https://www.amnesty.org/en/latest/news/2020/04/

If cultural practices, including traditions, social norms and taboos, are contagious in this multicultural region, this is also the case of repressive measures and oppression techniques. In fact, Algerian authorities have embarked on a campaign of arbitrary prosecutions aimed at silencing the Hirak movement and its activists, especially amid the COVID-19 pandemic.[6] Several arrests of online activists for Facebook posts have occurred since mid-March 2019, on charges such as encouraging illegal gatherings, insulting an official body, insulting the person of the president as well as attacking and threatening the territorial integrity of the state. Walid Kechida, a 25-year-old activist, has been arrested for creating a Facebook group named "Hirak memes" and charged with contempt and offending the person of President Abdelmadjid Tebboune, and attacking religious laws. In the same context, the pro-Hirak websites Maghreb Emergent, Interlignes Algérie and Radio M have been blocked during the lockdown period in contradiction of Article 50 of the Algerian constitution, which guarantees the freedom of print, audiovisual and online media.[7] Regarding this situation, Algerians question the efficiency of these repressive measures under the COVID-19 lockdown and remain uncertain regarding the future of the Hirak movement, at a time where online mobilisation and digital rights are endangered.

Meanwhile, the Moroccan government has drafted Bill 20.22 that punishes freedom of speech on social media platforms, including the calls to boycott products and spreading false information online.[8] The bill has been met by a total refusal from the Morocco online community regarding its content that restricts freedom of thought, opinion and expression guaranteed by Article 25 of the country's constitution.[9] Human rights defenders have criticised the government for failing to make clear the draft decree in an official statement, noting that Bill 20.22 could be used to "muzzle Moroccans' mouths" on social media, which were effectively used to organise the 2018 boycott campaign Moukatioun, which had been the largest action in Morocco's history in shifting political demands into a concrete call for actions targeting the economic sector. In response to this popular rejection, the Moroccan government has requested the postponement of passing the bill.

If the COVID-19 pandemic has been a political crackdown opportunity for North African governments, it has also highlighted the unequal effects of the pandemic on the most vulnerable members of the population, especially women. Soumeya Lerari Mouzai, an Algerian feminist activist and blogger, has emphasised:

> COVID-19 has exacerbated existing issues in North Africa, such as violence

tunisia-end-prosecution-of-bloggers-for-criticizing-governments-response-to-covid19

6 Amnesty International. (2020, 27 April). Algeria: End repression against Hirak activists and journalists amid COVID-19. https://www.amnesty.org/en/latest/news/2020/04/algeria-end-repression-against-hirak-activists-and-journalists-amid-covid19

7 Constitution of the People's Democratic Republic of Algeria, 2016.

8 Guerraoui, S. (2020, 30 April). "Fake news" draft bill sparks strong rejection in Morocco. *Middle East Online*. https://meo.news/en/%E2%80%9Cfake-news%E2%80%9D-draft-bill-sparks-strong-rejection-morocco

9 Constitution of the Kingdom of Morocco, 2011.

> against women and intrafamilial violence, including violence against minors. In addition, the loss and lack of revenue has reinforced several cases such as unwanted pregnancies and lack of access to birth control. Also, the lack of structures and shelters to host and support women, through psychological and legal support, is peculiar within the region, along to fast tracking measures to ensure full protection of victims.[10]

In this regard, the internet has been an amplifier calling to adopt an intersectional perspective, cognisant of the effects of COVID-19 on women and on the advancement of women's rights.

The COVID-19 measures, including repression, have endangered the civic space in North Africa and the freedom of expression as governments cross into digital censorship to ensure the continuity of authoritarian power in the online sphere. Yet, an interesting phenomenon is the frequent strategy of self-censorship in the absence of clear laws on media freedom, especially online and new media. This self-censorship may compromise the local narrative and lead to self-repression among online activists and creatives. Consequently, the reforms regarding freedom of expression in North Africa must arise from a political will permitting the population to hold opinions without interference, as emphasised by Principle 3 of the African Declaration on Internet Rights and Freedoms.[11] The radicality of these reforms must ensure open access to online information as a right guaranteed by the constitutions.

In the Tunisian context, for example, the contradiction lies within the legislative framework, as Tunisia's 2014 constitution guarantees the right of freedom of expression under Article 31,[12] further fostered by the country being a party to the International Covenant on Civil and Political Rights (ICCPR), which also guarantees the right to freedom of expression. However, Article 86 of the Telecommunication Code stipulates that anyone convicted of harming others or disrupting their lives through public communication networks may face up to two years of prison.

Furthermore, as previously mentioned, the penal code has provisions that criminalise defamation and the spreading of content liable to cause harm to public order or good morals. These contradictions expose critical questions about ensuring the continuity of the 2011 Jasmine Revolution's achievements but also the future aspects of the country's democratic transition. Additionally, these contradictions regarding the links between national and international internet governance mechanisms may lead to poor governance related to digital rights and the internet, and consequently a misuse of power among

10 Interview with Soumeya Lerari Mouzai, Algerian feminist activist and blogger at www.kalimateblog.wordpress.com, 2 June 2020.

11 https://engage.africaninternetrights.org/en/node/3

12 Constitution of the Republic of Tunisia, 2014.

democratic stakeholders.[13] Similarly, the Algerian Hirak movement is facing a shutdown which may disturb the continuity of its momentum in revolution and post-revolution contexts.

The Algerian government is taking advantage of the COVID-19 pandemic in an attempt to silence the movement that ensured a remarkable continuum for more than one year until its suspension due to the pandemic. This situation threatens the loss of momentum and prevents any recurrence as the crackdown continues on opponents, journalists, independent media and internet users. Algerians are currently scared by the signs of regression due to the oppression and dictatorship of the Bouteflikian era. Despite the efforts of the resistance movements to bring onto the table the idea of a parallel republic within a democratic framework, the Algerian government duplicates efforts to maintain the authoritarian regime even in the online sphere. However, Algerians continue to resist online, demanding mainly the release of prisoners of conscience. Under the banner of "Songs for Freedom",[14] Algerian artists took part in a virtual concert organised by Free Algeria on 23 May, calling for the freedom of prisoners of conscience, freedom of expression and media freedom. In fact, despite Article 36 of the Algerian constitution that stipulates that the freedom of conscience and the freedom of opinion are inviolable,[15] Drareni, Tabou and Kechida, to cite a few among the 63 prisoners of opinion as of 3 June, according to the non-exhaustive list of the National Committee for the Liberation of Detainees (CNLD),[16] remain jailed in silence.

While the draft Bill 20.22 has aroused an ardent debate on online freedom of expression, the online Moroccan sphere is also currently discussing privacy and personal data protection[17] issues. In fact, on 1 June, the Moroccan Ministry of Health launched Wiqaytna, a COVID-19 tracking application, as part of a national awareness campaign, after undergoing tests related to users' privacy from the National Commission for the Control of Personal Data Protection (CNDP). Wiqaytna compiles the list of people with whom the user has interacted through Bluetooth and notifies them if one of them has tested positive for COVID-19. However, human rights and digital rights defenders have raised concerns about potential violations of fundamental rights and freedoms, warning of the potential extension of this application into a model for a surveillance policy. As noted by the Moroccan Association for Human Rights, that may cause a wave of intimidation and arrests of online activists, even in the post-pandemic era.[18]

---

13 https://engage.africaninternetrights.org/en/node/42

14 https://www.youtube.com/watch?v=liwuU1AEqhE&feature=youtu.be&fbclid=IwAR3lzIcco05w2Hc4Q2uVPLQ3LetBycLjJo8XODCa16FJmso372HPp0Rc8ow

15 Constitution of the People's Democratic Republic of Algeria, 2016.

16 https://www.facebook.com/comitenationalpourlaliberationdesdetenusCNLD/posts/1640356882999904?__tn__=K-R

17 https://engage.africaninternetrights.org/en/node/38

18 Chahir, A. (2020, 29 May). Morocco's coronavirus surveillance system could tip into Big Brother. *Middle East Eye*. https://www.middleeasteye.net/opinion/risks-moroccos-coronavirus-surveillance-system

CONCLUSION

The interesting North African socio-political shift from offline activism to online movement building during the COVID-19 pandemic has exposed practices violating human rights, including digital rights, but also resulted in mechanisms of online repression omitting freedom of expression and digital rights and endangering sound internet governance principles as set out in the 2014 African Declaration on Internet Rights and Freedoms.[19] Consequently, it has deepened the shrinking of civic space, exposing an experience duplicated in different contexts throughout the African continent.

This assessment leads one to interrogate the future of movement building and internet governance in the region, and on the continent. Accordingly, it becomes imperative that North African governments fully implement concrete principles of online rights as set out in Part IV of the Declaration of Principles on Freedom of Expression and Access to Information in Africa,[20] issued in 2019 by the African Commission on Human and Peoples' Rights in recognition of the role of the internet as a tool to promote individual and collective participation in democratic processes.

This will be in line with international principles to ensure the right to freedom of expression and to receive and impart information, as duly stated in Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR), and to ensure that governments do not infringe on the right to privacy. In order to ensure that the right to internet freedom is universally recognised, the implementation requires a cross-sectoral approach between the governments, civil society organisations, the academic community and activists, to ensure mechanisms of accountability against states abusing laws on internet access.

Along with the digital divide and the current documented state abuses and infringement of digital rights, the internet is still an unequal space, with access still limited to a privileged population, leaving behind the most vulnerable, including the elders, the poorest and those living in remote areas who are consequently disconnected. Beyond the digital divide, women and other vulnerable individuals are targeted and abused on digital platforms, with devastating consequences for their mental well-being and safety.

To enable these marginalised groups to exercise their rights online, states need to act in line with Principle 43 of the ACHPR Declaration, which compels them to take legislative and other measures to implement the principles on freedom of expression and access to information rights.

19 https://africaninternetrights.org/articles

20 https://www.achpr.org/presspublic/publication?id=80

With the advancement of the internet and its growth as an essential service, new forms of digital abuse are established, reproducing the societal structures, such as so-called "revenge porn", or non-consensual sharing of intimate images. Therefore, it is pivotal that the cross-sectoral approach includes a feminist and pan-African perspective to ensure a just internet for all.

In addition, if the future of the internet is envisioned as a pro-democratic space, it should welcome democratic offline practices into the digital space and duplicate participatory practices including relevant stakeholders. Governments, civil society, marginalised groups and collectives, tech communities, academia and the private sector must take effective roles in the future digital realities. These roles must be clearly established, including accountability mechanisms and equal decision-making and leadership positions.

Therefore, these future digital realities must apply the learnings of the COVID-19 pandemic and become a showcase of human rights violations, exposing the misuse of power and corruption, holding dictatorial regimes accountable, and most of all, building trans-regional solidarity.

Digital divisions: COVID-19 policy and practice and the digital divide in Africa

Author: Charley Lewis

INTRODUCTION

The sudden and dramatic advent of the COVID-19 global pandemic caught the world by surprise and left many floundering for responses, none more so than those in the information and communications technology (ICT) sector: the policy makers, regulators and internet and other ICT service providers.

It was a few short weeks from the first reports of a strange new respiratory illness in faraway Wuhan (December 2019), to the first cases in Africa (late February 2020), the declaration of COVID-19 as a global pandemic (March 2020) and the imposition of the first full draconian lockdown on the continent (end of March 2020).[1]

The measures adopted by so many countries in Africa – the imposition of "social distancing" and stay-at-home strictures, the closure of businesses, shops and schools, travel bans and virus testing – had dramatic impacts on both economies and societies, on lives and livelihoods. And these measures, in turn, created a range of knock-on consequences for the ICT sector, its infrastructures and services, as access to the internet became both a key channel for authorities seeking to manage the crisis, and for citizens seeking to accommodate its exigencies. Thus was precipitated a flurry of ICT sector interventions – from policy makers, regulators and government entities.[2]

Many of these have been designed to increase access to the internet, to mobile telephony, and to a range of data-enabled ICT services. Many are aimed either

1 https://en.wikipedia.org/wiki/COVID-19_pandemic_in_Africa

2 Lewis, C. (2020, 3 April). ICT sector policy and regulation in the time of COVID-19. *ITWeb*. https://www.itweb.co.za/content/RgeVDMPYwGJqKJN3

at promoting the dissemination of public service information or at mitigating the impacts of lockdowns and social distancing on the economy and society, on how individuals and their communities live, work and play. Most depend on effective access to the internet and to data services for their efficacy and impact.

Indeed, the COVID-19 crisis has demonstrated in hard and practical ways that access to the internet, and the ability to benefit from its content and services, should now be considered a fundamental human right.[3]

In this article, we examine how policy makers, regulators and service providers responded to the COVID-19 explosion. The focus is specifically on the ICT sector, on telecoms and the internet, looking at some of the slew of ICT sector-specific measures, ranging from public service messaging, though temporary spectrum assignment and zero-rating of educational and health websites, to those actions intended to make access and services more affordable.

COVID IN CONTEXT

The eruption and rapid spread of COVID-19 found an ICT sector ill prepared to deal with the effects of a health pandemic, and with very limited guidance towards what should be the possible array of good practice responses.

It is true that the International Telecommunication Union (ITU) has since 2001 been working on good practice measures for telecommunications services in time of disaster, but the focus of this work has been on natural disasters, such as hurricanes and the 2004 Indian Ocean tsunami. It was therefore largely taken up with early warning systems and the coordination of post-disaster relief work.[4] And in a stroke of bitter irony, the ITU was to release a set of guidelines on how to develop a national emergency telecommunication plan in March 2020,[5] mere days after the World Health Organization (WHO) declared COVID-19 to be a global pandemic.[6] Despite being far too late to assist countries to formulate ICT sectoral responses to the rapidly escalating crisis, this new set of guidelines too remained centrally preoccupied with how to respond to natural disasters, without even a single mention of epidemiological outbreaks such as Ebola.

---

3 Berners-Lee, T. (2020, 4 June). Covid-19 makes it clearer than ever: access to the internet should be a universal right. *The Guardian.* https://www.theguardian.com/commentisfree/2020/jun/04/covid-19-internet-universal-right-lockdown-online

4 ITU. (2005). *Handbook on Emergency Telecommunications. Geneva: International Telecommunication Union.* https://www.itu.int/pub/D-HDB-HET-2004

5 ITU. (2019). *ITU Guidelines for national emergency telecommunication plans. Geneva: International Telecommunication Union.* https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/2019/NETP_Global_guideline.pdf

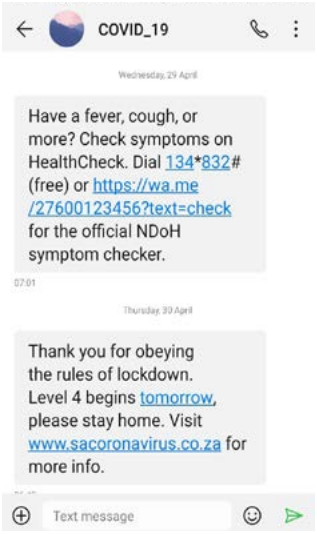
6 ITWeb. (2020, 20 March). ITU seeks to maintain vital communications during COVID-19. *ITWeb.* https://www.itweb.co.za/content/P3gQ2MGx8XKqnRD1

But it is in the responses to the Ebola epidemic that the roots of some of the good practice interventions discussed below lie, albeit not explicitly. For example, the GSM Association (GSMA) proposes the use of SMS and other messaging, along with anonymised contact tracing, based on call data.[7] A similar contemporaneous brief by USAID reviews a number of messaging and monitoring tools.[8]

On the one hand, some of the top-level Ebola lessons – for example, that speed of response trumps perfection[9] – drove the rapid move to impose lockdowns in so many jurisdictions. On the other, dramatically deadly though the outbreaks of Ebola may have been, those epidemics have been far more localised, making them an imperfect exemplar when it comes to identifying good ICT sector practices in response to the rapid sweep of COVID-19 across entire communities, countries and continents.

As a result, ICT sector policy makers, regulators and operators have largely been forced to fly by the seat of their pants when it came to devising appropriate responses to the exigencies of the crisis.

It is to a discussion of some of these responses that we now turn. The data and information available to record and examine them may be scant and patchy, reliant on the vagaries of press coverage. But the research and the analysis provide essential guidance for policy makers, regulators and practitioners attempting to deal with similar exigencies in the future.



Left: Public service SMS messages
Source: Charley Lewis

PUBLIC SERVICE COVID-19 CONTENT: SMS, WHATSAPP, RADIO AND TV

It is no accident that the provision of information about Ebola features prominently in the interventions endorsed above by the GSMA and USAID. Not only is access to information a fundamental human right, but empowering individuals and communities with information about an epidemic is critical to combat viral spread and to ensure popular support for other necessary public health emergency measures.

7 GSMA. (2014). *Blueprint: Ebola Mobile Response. London: GSM Association.* https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/10/gsma-Ebola-Mobile-Response-Blueprint.pdf The GSMA is the global umbrella body for mobile service providers. Contact tracing is a full subject in its own right, and will not be discussed here.

8 USAID. (2014). *Technical Brief: Use of Technology in the Ebola Response in West Africa.* https://www.msh.org/sites/default/files/technology_and_ebola_response_in_west_africa_technical_brief_final.pdf

9 https://www.youtube.com/watch?v=XEUwig1GkHo

Although radio and television are still the most common sources of information in Africa, cellular telephony ranks a close and growing third. Some 50% of the population now have access to a mobile phone, although a sizeable 40% of this number only have access via a basic 2G feature phone.[10] GSM telephony, therefore, offers a powerful tool to reach large numbers of people quickly and cheaply, by means of a structured campaign of SMS messaging as had been recommended by the GSMA in respect of Ebola.

Yet, despite a joint call from the WHO, ITU and UNICEF for countries to do just that,[11] drawing on a pre-provided database of messages in a number of languages,[12] actual deployment of this intervention appears to have been limited.

Left: South Africa's pioneering COVID-19 WhatsApp service
Source: www.iol.co.za

Kenya did move quickly in this regard, however, with the government sending out millions of informational COVID-19 SMSs to mobile subscribers in early March.[13] South Africa followed soon after, with a generalised injunction from the relevant minister to licensees requiring them to "receive and disseminate public information" and to provide "streaming of public announcements".[14] This was soon formalised in a notice from the regulator, specifying that all mobile licensees should transmit two SMSs daily to their customers.[15] However, no other regulators in Africa appear to have followed suit, although there have been rather less systematic claims of widespread COVID-19 SMS distribution by Vodacom Tanzania.[16]

---

10 GSMA. (2019). *The Mobile Economy: Sub-Saharan Africa 2019. London: GSM Association.* https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_SSA_Eng.pdf

11 ITU & WHO. (2020, 20 April). ITU-WHO Joint Statement: Unleashing information technology to defeat COVID-19. *World Health Organization.* https://www.who.int/news-room/detail/20-04-2020-itu-who-joint-statement-unleashing-information-technology-to-defeat-covid-19

12 Available via Google Docs at: https://docs.google.com/spreadsheets/d/1d4emD3Dpksns8mXTi22MTlyD2FeAz-U04PgWdKm4C3Y/edit#gid=1702826806

13 Xinhua. (2020, 11 March). Kenya uses mobile phones to spread awareness on Covid-19. *Independent Online.* https://www.iol.co.za/news/africa/kenya-uses-mobile-phones-to-spread-awareness-on-covid-19-44577955

14 RSA. (2020). Electronic Communications, Postal and Broadcasting Directions issued under Regulation 10(8) of the Disaster Management Act 2002 (Act No 57 of 2002). *Government Gazette, Vol. 657 No. 43164, 26 March 2020.*

15 de Wet, P. (2020, 6 April). You'll now be getting at least two Covid-19 SMSes a day, plus info on govt announcements. *Business Insider SA.* https://www.businessinsider.co.za/covid-19-regulations-require-daily-smses-from-south-african-cellphone-operators-2020-4

16 Telecompaper. (2020, 22 April). 'Vodacom Tanzania donates TZS 2 bln to support fight against Covid-19 pandemic. *Telecompaper.* https://www.telecompaper.com/news/vodacom-tanzania-donates-tzs-2bln-to-support-covid-19-pandemic--1335522

Other information dissemination measures adopted in South Africa included the development of a free national AI-enabled WhatsApp COVID-19 information service, a technological innovation later adopted and rolled out by the WHO itself,[17] and which has subsequently been rolled out in Nigeria and Zimbabwe, among others.

This was followed by a ministerial requirement that all websites registered under the national .za country domain add a link to the COVID-19 portal set up by the Department of Health[18] – a measure greeted with some confusion, but supported in principle.[19]

The efficacy and impact of the various measures discussed above remain unclear at this stage. There is limited reporting available on similar measures in African countries other than those specifically mentioned above.

Anecdotal accounts suggest that SMS overload quickly sets in, with subscribers moving to block the short code number being used. More importantly, it appears, unfortunately, that the messages have been circulated in English only. In both cases this would have limited both reach and impact. And, although compliance with South Africa's website linking requirement on the country's top 100 sites was reportedly around 80%,[20] the measure does not appear to have been widely emulated.

"DISINFODEMIC" IN THE PANDEMIC: DEALING WITH "FAKE NEWS"

The converse of the right of access to information lies in protection from exposure to incorrect, misleading or false information – of the kind that is often referred to as "fake news". Indeed, the prevalence and spread of misinformation and disinformation thrive in the vacuum left when the kind of public service messaging referred to above fails to find its audience.

The pervasiveness of such misleading and false information surrounding the COVID-19 pandemic has been so extensive that UNESCO has felt compelled to issue a number of guidance briefs for authorities attempting to deal with what it has characterised as a "disinfodemic" – the dissemination of "content that is false and [...] can have fatal consequences during a pandemic."[21]

---

17 Bloomberg. (2020, 26 March). SA WhatsApp service goes global in Covid-19 fight. *News24*. https://www.news24.com/citypress/News/sa-whatsapp-service-goes-global-in-covid-19-fight-20200326

18 McLeod, D. (2020, 26 March). All .za websites ordered to link to government Covid-19 portal. *TechCentral*. https://techcentral.co.za/all-za-websites-ordered-to-link-to-government-covid-19-portal/96874

19 Dundas, N. (2020, 27 March). COVID-19 Regulations Affecting ".ZA Domain Names". https://t.co/azzFLD8qB2?amp=1

20 Department of Communications and Digital Technologies. (2020, 4 June). Communications and Digital Technologies Sector Response: June 2020 (presentation).

21 Posetti, J., & Bontcheva, K. (2020). *Disinfodemic: Deciphering COVID-19 disinformation*. Paris: UNESCO. https://en.unesco.org/sites/default/files/disinfodemic_deciphering_covid19_disinformation.pdf

Above: Madagascar President Rajoelina punts COVID Organics
Source: www.newscientist.com

Examples of such fake news during the pandemic abound. Beyond the widely publicised and false fulminations emanating from US President Donald Trump, examples in Africa include:

- Malicious hoaxes, such as a viral video alleging that COVID-19 testing kits in South Africa were contaminated with the virus.[22]

- Deliberate phishing scams, such as the offer of free lockdown gas deliveries in Kenya in return for the payment of a "delivery fee".[23]

- Pseudo-science, such as the miraculous curative claims attached to the herbal tonic Covid Organics by Madagascar President Andry Rajoelina.[24]

- Conspiracy theories, such as the claim that 5G mobile technology is the source behind the spread of COVID-19.[25]

Dealing with disinformation and misinformation is not new – examples can be found from up to 200 years ago[26] – and so policy makers and regulators have had ample precedent upon which to base good practice responses.

---

22 Grobler, R. (2020, 6 April). Fake News: No, Covid-19 testing kits are not contaminated. *News 24.* https://www.news24.com/SouthAfrica/News/fake-news-no-covid-19-testing-kits-are-not-contaminated-20200406

23 Onamu, A. (2020, 18 May). No, Kenol Kobil Is Not Giving Out Free K-Gas Cylinders. Gadgets Africa. https://gadgets-africa.com/2020/05/18/k-gas-scam

24 RFI. (2020, 24 April). Two African leaders under fire for touting unproven Covid-19 'preventatives'. Radio France International. http://www.rfi.fr/en/africa/20200424-two-african-leaders-under-fire-for-touting-unproven-coronavirus-preventatives-madagascar-guinea-covid-organics-artemisia

25 Barlow, E. (2020, 6 April). 'Worst kind of fake news': 5G conspiracy theories run wild. *TechCentral.* https://techcentral.co.za/worst-kind-of-fake-news-5g-conspiracy-theories-runwild/97106

26 See, for example: Andrews, A. (2015, 25 August). The Great Moon Hoax. *History.* http://www.history.com/news/the-great-moon-hoax-180-years-ago?linkId=16545579

Reactions have ranged from the draconian to the collaborative. The disinformation dynamic in Africa during the COVID-19 pandemic has, however, been complicated by the fact that a number of political leaders (with Tanzania, Madagascar and South Sudan among the culprits) and politicians have themselves been involved in disseminating false information or manipulating the crisis for political ends.[27]

Whilst shutting down the internet, or blocking over-the-top (OTT) services, has been a widespread means of silencing political dissent in Africa over the years,[28] the fears that internet shutdowns might be used to silence opposition to government COVID-19 measures, or to limit the spread of bogus information,[29] appear to have been unfounded. Thus, the various calls to end such shutdowns in order to ensure the vital access to the key COVID-19 information discussed in the preceding section appear largely to have been unnecessary. Existing shutdowns in Ethiopia and Guinea, both political in intent, were ended in late March.[30]

However, in slightly less draconian vein, a number of jurisdictions – Kenya, Rwanda and South Africa among them – have criminalised the dissemination of "fake news", either in general, or specifically in relation to the COVID-19 crisis (as in the case of South Africa). Such measures are considered poor practice, and are both economically damaging[31] and widely condemned by human rights organisations, amidst concerns that responses to the "disinfodemic" can become excuses to erode key human rights.[32]

Most jurisdictions, however, rely on the self-regulatory codes of conduct adopted by OTT platforms such as Facebook, WhatsApp and Twitter – who themselves make use of artificial intelligence (AI) algorithms based on factors such as content or sharing patterns – or co-regulation with internet service provider associations. Of growing importance are the rising number of fact-checking entities, which identify, research and debunk (or occasionally verify) some of the vast range of claims made on internet-based platforms,[33] sometimes working in association with Facebook and others. These sites, therefore, play a valuable role in buttressing

27 Ncube, S. (2020, 26 May). Denial, opportunism and fakery muddy the waters in African campaign against Coronavirus. *Daily Maverick*. https://www.dailymaverick.co.za/article/2020-05-26-denial-opportunism-and-fakery-muddy-the-waters-in-african-campaign-against-coronavirus

28 Woodhams, S., & Migliano, S. (2020, 7 January). The Global Cost of Internet Shutdowns in 2019. *Top10VPN*. https://www.top10vpn.com/cost-of-internet-shutdowns

29 Human Rights Watch. (2020, 31 March). End Internet Shutdowns to Manage COVID-19. https://www.hrw.org/news/2020/03/31/end-internet-shutdowns-manage-covid-19

30 ACHPR. (2020, 8 April). Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Importance of Access to the Internet in Responding to the COVID-19 Pandemic. *African Commission on Human and Peoples' Rights*. https://www.achpr.org/pressrelease/detail?id=487

31 Woodhams, S., & Migliano, S (2020, 7 January). Op. cit.

32 Milo, D., & Thiel, J. (2020, 20 March). Fake news about Covid-19 now a criminal offence. *Daily Maverick*. https://www.dailymaverick.co.za/article/2020-03-20-fake-news-about-covid-19-now-a-criminal-offence

33 Examples, some of long standing, include https://africacheck.org and https://pesacheck.org in Africa – along with Media Monitoring Africa's recently launched and currently primarily COVID-19-focused https://www.real411.org – as well as https://www.snopes.com and https://www.hoax-slayer.com internationally.

the right of access to factual information. Many of them have been particularly busy in recent months dealing with the COVID-19 "disinfodemic". In Uganda, the regulator went one step further, launching its own fact-checking service.[34]

At the end of the day, however, it lies in the hands of public service media entities to ensure that accurate and factual information wins out. If they are proactive, transparent, accurate and authoritative, it is their news and information that will prevail, and that will make meaningful the right of access to information. In the long term this needs the support of the education system in order to promote digital skills, including informational skills, among citizens and the youth.

SPECTRUM: MEETING THE UPSURGE IN DATA DEMAND

Left: ICASA's Temporary covid-19 Spectrum Assignement
Source: ICASA

The dissemination of public interest information depends on service providers, and on mobile service providers in particular, as we have noted above.

Social distancing measures in general, and the imposition of lockdowns in particular, have led to a dramatic upsurge in network traffic, as people have been forced to work from home, communicate with family and friends from whom they are physically separated, access information over the internet, or make use of mobile money and e-commerce services. The resultant spike in demand for data and telephony services put pressure on the wireless networks that are the lifeblood of online content and services, as well as on the financial position of the operators.[35]

As a result, operators in many jurisdictions turned to their regulatory authorities, asking for access to additional electromagnetic spectrum in order to supply the necessary bandwidth, and for financial relief.

In Ireland, the regulator, ComReg, was quick to respond, running an expedited notice and comment process before issuing three-month temporary spectrum licences to several of its incumbent telcos.[36] Similarly, the FCC in the United

34 Ssebwami, J. (2020, 13 April). COVID-19 CRISIS: UCC launches fact-checking initiative to identify misinformation. *PML Daily.* https://www.pmldaily.com/news/2020/04/covid-19-crisis-ucc-launches-fact-checking-initiative-to-identify-misinformation.html

35 WIOCC. (2020, 2 June). Dramatic Surge in IP traffic due to Covid-19. *West Indian Ocean Cable Company.* http://wiocc.net/blog/dramatic-surge-in-ip-traffic-due-to-covid-19

36 ComReg. (2020). *Wireless Telegraphy (Temporary Electronic Communications Services Licences) Regulations, Statutory Instrument No. 122 of 2020. Commission for Communications Regulation.* https://www.comreg.ie/publication-download/s-i-no-122-of-2020-temporary-electronic-communications-services-licences

States granted temporary COVID-19 spectrum access to major providers AT&T and Verizon, and others.[37] New Zealand went one step further, simply allocating COVID-19 spectrum both directly and permanently.[38]

In Africa, the Independent Communications Authority of South Africa (ICASA) was quick to respond, first offering a temporary waiver of spectrum fee payments,[39] and then issuing the incumbent licensees with additional spectrum on a temporary basis.[40] While there has been some criticism of the move as having favoured incumbents and not sufficiently encouraging innovation,[41] it has nevertheless been widely welcomed[42] as providing much-needed relief for the incumbent networks that bore the initial brunt of the spike in traffic. Ironically and sadly, however, one of the dominant players turned its COVID-19 temporary spectrum allocation to the benefit of its most affluent customers, launching 5G services in several major metropolitan areas.[43]

A limited number of regulators elsewhere in Africa implemented similar measures, notably Ghana,[44] Zambia,[45] Zimbabwe,[46] the DRC and Morocco. These supply-side interventions were warmly welcomed by the global GSM Association as good COVID-19 regulatory practice.[47] But they are a measure less necessary in jurisdictions with lower levels of mobile penetration and fewer numbers of internet users, and where there is consequently less pressure on spectrum under the changed patterns of usage caused by COVID-19.

---

37 Welch, C. (2020, 19 March). Dish is letting the major US carriers borrow spectrum during quarantine data crunch. *The Verge.* https://www.theverge.com/2020/3/19/21187378/dish-letting-att-verizon-tmobile-use-spectrum-coronavirus

38 O'Neill, R. (2020, 12 May). NZ telcos welcome government's 5G spectrum direct allocation plan. *New Zealand Reseller News.* https://www.reseller.co.nz/article/679634/telcos-welcome-government-5g-spectrumdirect-allocation-offer

39 TechCentral. (2020, 30 March). Icasa grants 3-month spectrum break to operators. *TechCentral.* https://techcentral.co.za/icasa-grants-3-month-spectrum-break-to-operators/96944

40 ICASA. (2020, 6 April). Emergency release of spectrum to meet the spike in broadband services demand due to COVID-19. *Independent Communications Authority of South Africa.* https://www.icasa.org.za/news/2020/emergency-release-of-spectrum-to-meet-the-spike-in-broadband-services-demand-due-to-covid-19

41 Gillwald, A., Hadzic, S., & Aguera, P. (2020). *Temporary COVID-19 spectrum – a missed opportunity for some regulatory innovation? Cape Town: Research ICT Africa.* https://researchictafrica.net/wp/wp-content/uploads/2020/04/Covid-spectrum-brief-04-20.pdf

42 Stone, S. (2020, 15 April). 'Temporary spectrum relief a welcome step'. *City Press.* https://www.news24.com/citypress/Business/temporary-spectrum-relief-a-welcome-step-in-inevitable-evolution-of-human-connectivity-20200415

43 McLeod, D. (2020, 4 May). Vodacom unveils first 5G deals – 800GB for R1 499. *TechCentral.* https://techcentral.co.za/vodacom-unveils-first-5g-deals-800gb-for-r1-499/97785

44 Adepoju, P. (2020, 28 April). Ghana expands spectrum for MTN, Vodafone. *ITWeb.* https://itweb.africa/content/5yONPvEgAGGMXWrb

45 Malakata, M. (2020, 27 May). Zambia releases free additional spectrum. *ITWeb.* https://itweb.africa/content/KzQenMjVeXrMZd2r

46 Adepoju, P. (2020, 15 May). Zim telcos receive additional spectrum at no charge. *ITWeb.* https://itweb.africa/content/Olx4zMknepG756km

47 GSMA. (2020, 31 March). Keeping everyone and everything connected: How temporary access to spectrum can ease congestion during the COVID-19 crisis. https://www.gsma.com/newsroom/blog/keeping-everyone-and-everything-connected-how-temporary-access-to-spectrum-can-ease-congestion-during-the-covid-19-crisis

Perhaps of more interest in addressing the digital divide is South Africa's award of TV white space spectrum for rural connectivity to three licensees.[48] However, initiatives such as these – and there are a number, both in South Africa and elsewhere on the continent[49] – are highly unlikely to deliver results in the short time frames of the COVID-19 crisis. Rather than forming part of pandemic good practice, they need to be part of the long-term, multifaceted armoury of ongoing digital divide interventions.

ADDRESSING AFFORDABILITY: FROM MOBILE MONEY TO ZERO-RATING

The ability of poor individuals and remote communities to make use of the internet, and of data and messaging services, in order to mitigate the social and economic impacts of COVID-19 counter-measures is dramatically inhibited by the barrier of affordability.[50] The affordability-based digital divide, and its impact on lives and livelihoods, is an issue that has long been at the forefront of concern from many quarters[51] – all the more so now, given the fact that COVID-19 is a pandemic with deeply divided consequences for society.[52] On the one hand, the high-bandwidth, advanced-device access to the internet and data services enjoyed by the rich can palliate the most adverse consequences of COVID-19 strictures. On the other, those with limited data and basic handset devices have extremely limited access to the necessary data and services.

As a result, policy and regulatory interventions aimed at ensuring access to online data and services for the poorest households and most remote communities must surely be a key component of any good practice intervention during an emergency such as that occasioned by COVID-19.

Internationally, service providers adopted a number of measures aimed at poorer customers: they cut data prices, doubled data allocations, and promised not to disconnect those with payment arrears.[53]

---

48 Goldstuck, A. (2020, 10 May). TV white spaces change the rural Wi-Fi game. *Business Times*. https://www.timeslive.co.za/sunday-times/business/2020-05-10-tv-white-spaces-change-the-rural-wi-fi-game

49 Rey-Moreno, C., & Graaf, M. (2018). Map of the Community Network Initiatives in Africa. In L. Belli (Ed.), *Community Connectivity: Building the Internet from Scratch. Rio de Janeiro: FGV Rio Editions*. https://bibliotecadigital.fgv.br/dspace/handle/10438/17528

50 Turianskyi, Y. (2020, 14 May). COVID-19: Implications for the 'digital divide' in Africa. *Africa Portal.* https://www.africaportal.org/features/covid-19-implications-of-the-pandemic-for-the-digital-divide-in-africa

51 ITU. (2020). *Measuring Digital Development: ICT Price Trends 2019. Geneva: International Telecommunication Union.* https://www.itu.int/en/ITU-D/Statistics/Documents/publications/prices2019/ITU_ICTpriceTrends_2019.pdf

52 Jorge, S., Sarpong, E., & Nakagaki, M. (2020). *Covid-19 Policy Brief: Internet Access & Affordability. Washington, DC: Alliance for Affordable Internet and Web Foundation.* https://webfoundation.org/docs/2020/04/Covid-Policy-Brief-Access_Public.pdf

53 Ofcom. (2020, 1 April). How broadband and mobile firms are serving customers during the coronavirus pandemic. https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/broadband-and-mobile-firms-commit-helping-customers-during-coronavirus

In Africa, the response was rather more limited. While prices were cut in countries as far flung as Cameroon,[54] Mozambique and Cape Verde,[55] and while Egypt offered marginal increases to data bundle sizes,[56] other jurisdictions preferred to target the more affluent work-from-home contingent.[57]

South Africa had just emerged from a data services market review in which the Competition Commission had recommended a series of remedial measures which included substantial cuts in the retail price of data, provision of free lifeline data to poor consumers, zero-rating of public benefit websites, and abolition of price premiums on smaller bundles.[58]

In their settlements with the Commission (most of which were agreed just as the COVID-19 wave began to break), the dominant service providers agreed to implement some but by no means all of the findings. While prices were cut, and zero-rating agreed to, the tiered structure of bundle pricing remained,[59] and free data became camouflaged under free access to proprietary services and platforms.[60]

As a result, many were deeply disappointed at the limited extent of the settlements of the service providers with the Commission[61] – and no new concessions were made after the pandemic hit, despite encouragement by the regulator for providers to do so, leaving poor households severely constrained – aside from content on zero-rated websites (see discussion below) – in their ability to secure meaningful access to the internet during the crisis.

Some have pointed to South Africa's universal service fund and its provisions for funding the access of "needy persons" to ICT services, but nothing was ever attempted in this regard. This may be down to the March ministerial injunction

---

54 Atabong, A. (2020, 25 March). Orange Cameroun slashes prices in response to COVID-19. *ITWeb.* https://itweb.africa/content/KzQenqjVdKPqZd2r

55 Tsandzana, D. (2020, 3 April). Mozambique and Cape Verde's telcos offer affordable mobile internet as citizens urged to stay home. *Global Voices.* https://globalvoices.org/2020/04/03/mozambique-and-cape-verdes-telcos-offer-affordable-mobile-internet-as-citizens-urged-to-stay-home

56 Al-Youm, A. (2020, 16 March). Egypt's internet companies increases bundle quotas by 20% for free: Ministry. *Egypt Independent.* https://egyptindependent.com/egypts-internet-companies-to-increase-bundle-quotas-by-20-ministry

57 Oloo, V. I. (2020, 25 March). COVID-19: MTN Uganda Introduces Work From Home Data Bundle. *Dignited.* https://www.dignited.com/59266/mtn-work-from-home-data-bundles-uganda

58 McLeod, D (2019, 2 December). Free data for all South Africans in radical regulatory intervention. *TechCentral.* https://techcentral.co.za/free-data-for-all-south-africans-in-radical-regulatory-intervention/94444

59 For example, an MTN subscriber currently buying 1 GB of data in 100 MB chunks, still pays twice as much per GB as a subscriber who can afford to purchase a full 1 GB at a time.

60 BusinessTech. (2010, 20 March). MTN announces massive price cuts and free data. *BusinessTech.* https://businesstech.co.za/news/telecommunications/383443/mtn-announces-massiveprice-cuts-and-free-data

61 Shoba, S. (2020, 18 March). Are mobile network providers doing enough to keep South Africans connected? *Daily Maverick.* https://www.dailymaverick.co.za/article/2020-03-18-are-mobile-network-providers-doing-enough-to-keep-south-africans-connected

for the fund to prioritise broadband access to municipalities, although there is no evidence that that was done either.[62]

It is unfortunate that regulators in Africa were unable to secure the kind of substantive commitments elicited by Ofcom, the UK regulator, in support of those on the wrong side of the digital divide. ICASA did undertake such a written engagement with the sector early on in the pandemic,[63] but its impact and outcomes remain unclear.

Mobile money, however, proved rather more susceptible, as lockdown restrictions on movement curtailed the ability of individuals to access cash and to pay for goods and services. In a number of jurisdictions – Uganda, Malawi, Airtel and Safaricom in Kenya – m-money fees were waived or reduced, either on all transactions or low denomination ones. Even cash-critical Zimbabwe made some moves in this direction, albeit contradictory ones. The spike in mobile money transactions has been a global one,[64] and the eagerness of providers to facilitate the upsurge is likely due to a desire to leverage the COVID-19-driven demand for cashless transactions and cash transfers in order to achieve greater market share, as Kenya's Safaricom was historically able to do with M-Pesa.

FROM CLASSROOM COMFORTS TO E-LEARNING LAPSES

The widespread closure of schools and institutions of further education and training prompted a slew of responses intended to minimise the consequent disruptions to learning programmes,[65] but, as in many of the cases discussed here, there was little by way of a priori good practice guidance. Moves to replace face-to-face teaching with ad hoc e-learning, and by providing online access to educational resources, rapidly ran into the rocky ground of the e-learning ecosystem and foundered in the face of the digital divide.

A shift to e-learning is relatively easy for the affluent, with ready access to both the requisite user devices and connectivity, as well as the necessary digital skills to navigate the concomitant changes to facilities and behaviours.

---

62 USAASA has since issued a controversial tender to supply over 100,000 television sets to indigent learners in their final year of schooling –see Labuschagne, H. (2020, 15 June). Government plans to give free TVs to more than 100,000 matrics. *MyBroadband.* https://mybroadband.co.za/news/broadcasting/356259-government-plans-to-give-over-100000-matrics-free-tvs.html – a quixotic initiative whose chances of success in the absence of concomitant affordable access to online services, devices and content must surely be dismal.

63 ICASA. (2020, 19 March). ICASA engages with licensees to open their services to all South Africans as the country fights the scourge of the COVID-19 pandemic. *Independent Communications Authority of South Africa.* https://www.icasa.org.za/news/2020/icasa-engages-with-licensees-to-open-their-services-to-all-south-africans-as-the-country-fights-the-scourge-of-the-covid-19-pandemic

64 The Economist. (2020, 28 May). The covid-19 crisis is boosting mobile money. *The Economist.* https://www.economist.com/middle-east-and-africa/2020/05/28/the-covid-19-crisis-is-boosting-mobile-money

65 ITU. (2020, 31 March). COVID-19: Here's how some countries are addressing the digital education divide. *ITU News.* https://news.itu.int/covid-19-countries-addressing-digital-education-divide

But most learners from poorer households do not have either a laptop computer or easy access to their own smartphone, and many do not have ready access to the electricity needed to operate the devices. And then they are faced with the unaffordable costs of the data required for bandwidth-hungry e-learning content. Educators too are faced with a multitude of challenges as they seek to develop and deliver content that needs to be accessible and usable via a multitude of channels on a multiplicity of user devices.

The widespread adoption of zero-rating for educational content across the continent – an affordability proposal long punted,[66] often under the wider umbrella of public benefit content, and with antecedents in Facebook's "Free Basics" offering – was seen as a ready response to address the problems of affordable access for e-learning to take place. A number of operators, many with previous experience of using zero-rating as a marketing ploy, quickly moved to offer free access to educational websites. These included Airtel and Safaricom in Kenya, Orange and MTN in Liberia, Telekom Networks Malawi and all the major mobile operators in South Africa. Others, such as the Botswana Telecommunications Corporation, launched proprietary e-learning platforms. In some jurisdictions zero-rating has also been extended to health websites.

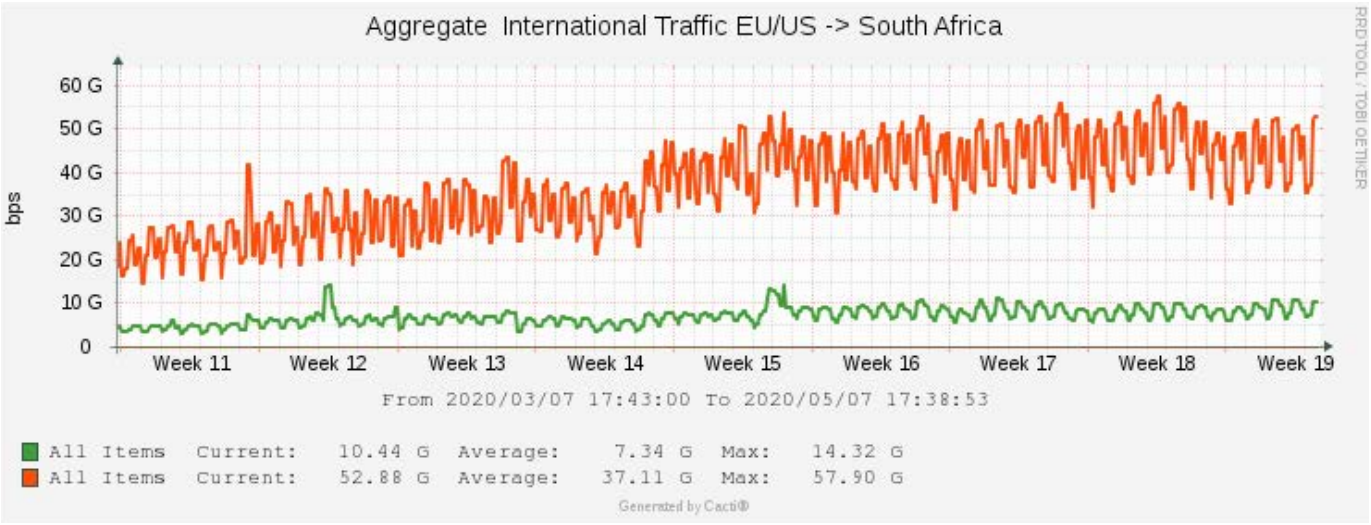
There have been a number of problems with this initiative,[67] not all of them fully documented and reported as yet. Firstly, there was often less than full unanimity on which of the many possible websites and online resources to zero-rate. This meant that some learner subscribers on one network were unable to secure free access to content that had been zero-rated by a different network. Secondly, websites often access breakout content, resources and JavaScript from external sources, which may not form part of the zero-rated walled garden, resulting in learners either unknowingly incurring unexpected data charges or being unable to load certain pages properly because they had run out of data. Thirdly, being classified as offering zero-rated content is a highly desirable status for providers seeking to maximise their exposure, creating a scramble for favourable classification.

Some have proposed a reverse billing model to resolve some of the problems with unexpected data charges. Meanwhile, universities in South Africa have struck agreements with service providers to provide free monthly data allocations to needy students as an alternative solution.

---

66 Mail & Guardian. (2020, 23 March). Zero-rate mobile services for health, education and development now. *Mail & Guardian.* https://mg.co.za/article/2020-03-23-zero-rate-mobile-services-for-health-education-and-development-now

67 Dell, S. (2020, 9 April). Zero-rating online learning – Not as simple as it sounds. *University World News.* https://www.universityworldnews.com/post.php?story=20200408201225155



Above: The upsurge in data traffic due to Covid
Source: Cacti

The resulting confusion has led South Africa recently to issue a comprehensive set of policy directions aimed at resolving these problems,[68] and, finally, publication of a long list of qualifying sites.[69]

But a further access challenge remains to be resolved: the provision of the necessary devices for learners to use. In South Africa, universities have offered loan laptops to students as a way of addressing the problem. The national student bursary scheme too has stepped into the breach, but its ability to supply laptops to needy students has been delayed by the decision to centralise the procurement process, and hence to put the project out to tender.[70]

Despite its intuitive appeal, zero-rating of online content has therefore proven to be a less than ready panacea for the challenges of e-learning access for disadvantaged learners.

THE DIGITAL DIVIDE AND THE FUNDAMENTAL RIGHT TO INTERNET ACCESS

As we have seen from the discussion above, the global COVID-19 crisis threw entire economies and societies into turmoil. It caught national governments across the board ill-prepared for the drastic, dramatic health and public safety measures that were required to combat the scourge of such an unprecedented global pandemic. But ICT sector policy makers, regulators, service providers and users were equally unprepared for the kinds of interventions that would be necessary if ICT infrastructure, services and content were to both manage and mitigate the consequences of social distancing and lockdowns.

68 Mzekandaba, S. (2020, 9 June). Zero-rating criteria for education, health sites gazetted. *ITWeb.* https://www.itweb.co.za/content/mYZRXv9aLQnvOgA8/2JN1gPvO29qjL6mO

69 McKane, J. (2020, 17 June). Here is the full list of zero-rated websites in South Africa. *MyBroadband.* https://mybroadband.co.za/news/internet/356371-here-is-the-full-list-of-zero-rated-websites-in-south-africa.html

70 Mzekandaba, S. (2020, 10 June). NSFAS students in laptop limbo as govt opens tender. *ITWeb.* https://www.itweb.co.za/content/lLn147mjEEDMJ6Aa/2JN1gPvO29qjL6mO

As a result, there were few if any good practice models that could be relied on for guidance.

Detailed research is required to track, delineate and analyse the interventions outlined above, and to assess the degree to which they may be considered to constitute an embryo of emerging international good practice. The ITU[71] and others[72] have commenced the work, but far more is needed to be done.

It is clear, however, that the ICT sector is a complex, dynamic and interlocking ecosystem, and that interventions need to be considered in the light of that complexity, so that they do not fail because of one or more overlooked critical success factors, or produce unintended consequences.

What is equally clear is that COVID-19 is a pandemic of two halves and two divergent outcomes, with socioeconomic disparities between rich and poor, between the connected and unconnected, both cruelly exposed and harshly magnified by ICTs.

For the connected few, with ready access to technology, information and the power of digital skills, COVID-19 has been a substantial inconvenience, but fundamentally a navigable circumstance. They have been able to adhere to lockdown measures, to work from home, and school from home, and shop from home, and live their lives from home.

But for those with limited or no access to ICT infrastructure, services and content, disabled by lack of technology and inadequate devices, and crippled by the high price of data, it has been a diametrically different story. They have been largely unable to work, or learn, or transact, or navigate daily lockdown life.

As the 2016 African Declaration on Internet Rights and Freedoms reminds us:

> Access to the Internet plays a vital role in the full realisation of human development, and facilitates the exercise and enjoyment of a number of human rights and freedoms, including the right to freedom of expression and information, the right to education, the right to assembly and association, the right to full participation in social, cultural and political life and the right to social and economic development.[73]

COVID-19 has demonstrated in ways beyond the cruel toll of those infected or killed, that access to the internet and its cornucopia of goods, services and

71 ITU. (2020). *First Overview of Key Initiatives in Response to COVID-19. Geneva: International Telecommunication Union.* https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/REG4COVID/2020/Summary_Key_Covid19_Initiatives.pdf

72 https://www.mobileworldlive.com/featured-content/home-banner/covid-19

73 http://africaninternetrights.org/wp-content/uploads/2015/11/African-Declaration-English-FINAL.pdf

content is, as its architect reminds us, a fundamental precondition for human welfare, for economic growth and for social development.[74]

This is a position that the 2019 Banjul Declaration reaffirms:

> [U]niversal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression, access to information and the exercise of other human rights.[75]

Resolute, concerted and urgent action is therefore required to deal with the digital divide, to mitigate its impact on individuals and communities, on lives and livelihoods, on health and happiness. It is a challenge that humanity dare not fail.

74 Berners-Lee, T. (2020, 4 June). Op. cit.

75 ACHPR. (2019). Declaration of Principles on Freedom of Expression and Access to Information in Africa. Banjul: African Commission on Human and Peoples' Rights. https://www.achpr.org/public/Document/file/English/Declaration of Principles on Freedom of Expression_ENG_2019.pdf

A provisional analysis of the impact of telecommunications policy and regulatory frameworks in Africa and COVID-19: A community networks perspective

Author: Josephine Miliza

INTRODUCTION

The COVID-19 pandemic has had a significant socioeconomic impact across the globe. To prevent the spread of infections, governments are implementing emergency measures, such as physical distancing and lockdowns, with some countries encouraging cashless transfers. Individuals, organisations and institutions are now leveraging internet connectivity and digital technologies for work, education, commerce and entertainment. However, for the privileged few with home internet service, this has not been designed for heavy usage, such as multiple live streaming connections and applications, which has resulted in a depreciation in quality of service. Slower speeds and internet outages are some of the effects of the sudden upsurge in internet uptake and digital platforms are straining the existing infrastructure capacity. For the economically and socially disadvantaged who are unable to access and use the internet, the impact goes beyond livelihoods to accessing critical information on the pandemic such as health and social connections.

This article seeks to examine the extent to which national and regional responses to the COVID-19 pandemic may have impacted on the regime of human rights online. The article also examines the widening digital divide and the role that telecommunication policy and regulatory frameworks play in closing this gap. The article is informed by two preliminary observations. First, regional state and non-state actors predominantly view the pandemic through clinical lenses, while largely projecting its current and anticipated impact in public health and socioeconomic terms. Second, the responses have been state-centred, resulting

in widening the digital divide and violating digital rights, such as the right to information and freedom of expression.

This article also discusses inequalities online and offline that have become apparent from the shift to online spaces, especially for work and education. Specifically, it will consider how this is impacted by the digital divide and the potential capacity of community networks in Africa to provide access during and beyond COVID-19. The article then discusses the importance of bottom-up approaches to fighting the pandemic and the role of community and community-based organisations such as community networks, radios and health centres.

CONTEXT

Africa reported its first case of COVID-19 in mid-February, and by the end of May 2020, the continent had over 100,000 cases reported.[1] Despite the initial fears about the continent's preparedness to deal with the pandemic, the reported mortality rate is not as high as that experienced in other parts of the world. However, the number of reported cases is still on the rise. Countries have implemented various emergency response measures to curb the spread of the virus, such as border closures, public health measures, and full and partial lockdowns. The implementation of physical distancing measures resulted in the shifting of work, education, commerce, public gatherings, family meetings and other day-to-day activities online. To some organisations and institutions, especially in the private sector, this was an almost easy transition. However, the operations of many public institutions, such as schools, and of those working in the informal sector, were curtailed.

The digitisation agenda has dominated conversations among governments, policy makers, businesses and civil society. African countries have made progress on digitisation in sectors such as financing and e-commerce. In 2019, Africa had over 122 million people using mobile financial services, which have been widely adopted due to penetration of mobile connectivity and basic phones.[2] The telecommunications sector has felt the impact of the pandemic as there has been an increased demand on mobile voice and messaging services and both mobile and fixed broadband, with accelerated internet and digital technologies adoption. The sector is now among those listed as essential services, and governments are exempting operators from some restrictions, such as movement within or outside cities.

Telecoms operators in Africa are implementing different response strategies. In Kenya, Safaricom, a telecoms operator, reported a 70% increased demand in

1 World Health Organization. (2020, 22 May). Africa COVID-19 cases top 100 000. https://www.afro.who.int/news/africa-covid-19-cases-top-100-000

2 Leke, A. (2019, 3 September). Why Africa's digital boom is only just getting started. *World Economic Forum*. https://www.weforum.org/agenda/2019/09/why-africas-digital-boom-is-only-just-getting-started/

April.[3] With the Kenyan government recommending the use of mobile money transactions to help reduce spread of the virus, Safaricom waived transaction fees for person-to-person transactions below 1,000 Kenya shillings (roughly USD 10). Daily transactions for small and medium-sized businesses were increased from 70,000 Kenya shillings (USD 700) to 150,000 Kenya shillings (USD 1,500).[4] Other telecoms operators across the continent have implemented responses as well: for example, Vodafone is sending COVID-19 health information via text messages at no cost to its subscribers; and MTN in Cameroon is providing communication services for the government's testing centres and dissemination of information.[5]

OFFLINE INEQUALITY MEETS ONLINE INEQUALITY

Africa's telecommunications sector is a key driver of socioeconomic transformation. The sector liberalisation and privatisation created an enabling environment for increased competition and foreign investment. In the last decade, the sector has advanced with varying degrees of structural and regulatory reforms starting in the 1980s and 1990s with the adoption of the structural adjustment policies.[6] These reforms have led to the privatisation of state telecommunications monopolies, the creation of regulatory agencies, national information and communication policies and master plans in several states. There has been a significant investment for undersea fibre optic from some governments and the private sector. For example, the Kenyan government launched The East African Marine System (TEAMS), a 5,000-kilometre fibre optic undersea cable, in October 2009.[7] Terrestrial fibre is also growing, and it is estimated that over 1.3 million kilometres have been rolled out with over 1 million kilometres being in operation in 2019.[8] Lastly, the number of internet exchange points (IXPs), which enable local internet traffic exchanges, continues to expand. Currently, there are 46 active IXPs in 34 countries.[9]

For the majority of end-users, mobile represents the primary means of connectivity. The network coverage in 2018 for 3G and 4G was 71% and 40% respectively.[10]

---

3 Miriri, D. (2020, 14 April). Kenya's Safaricom sees 70% jump in data usage during COVID-19 lockdown. *Reuters*. https://af.reuters.com/article/investingNews/idAFKCN21W1NH-OZABS

4 Bright, J. (2020, 16 March). Kenya turns to M-Pesa mobile-money to stem the spread of COVID-19. *TechCrunch*. https://techcrunch.com/2020/03/16/kenya-turns-to-its-mobile-money-dominance-to-stem-the-spread-of-covid-19

5 CIPESA. (2020, 27 March). How Technology is Aiding the Covid-19 Fight in Africa. https://cipesa.org/2020/03/how-technology-is-aiding-the-covid-19-fight-in-africa/

6 UN Economic Commission for Africa. (2017). *Review of the legal and regulatory frameworks in the information and communications technology sector in a subset of African countries: What lessons can we learn?* https://www.uneca.org/sites/default/files/PublicationFiles/review_of_the_legal_and_regulatory_framework.pdf

7 https://teams.co.ke

8 Hamilton, P. (2019, 19 November). Africa's Operational Fibre Optic Network Reaches 1 Million Route Kilometres. *Africa Bandwidth Maps*. https://www.africabandwidthmaps.com/?p=6158

9 https://www.af-ix.net/ixps-map

10 Broadband Commission Working Group on Broadband for All. (2019). *Connecting Africa Through Broadband*.

In 2019, talk of the "fourth industrial revolution" dominated conversations across all sectors and continents. There was excitement about the seemingly countless possibilities of these revolutionary technologies such as artificial intelligence, machine learning and robotics that would usher individuals, communities and organisations into a new era. These bandwidth-intensive initiatives would require even faster, more reliable and secure internet connectivity. The reality in many countries' focus on internet access has been on how to keep improving services for the connected, especially the economically advantaged in urban areas which are more commercially viable for telecom operators. According to the GSMA, although in 2018 mobile broadband coverage in Sub-Saharan Africa was at 30%, the mobile internet usage gap was at 46%. The two major barriers identified were the lack of digital and literacy skills, as well as affordability.[11] The majority of Africa's population live in the rural areas and the economies are primarily powered through the informal sector and agriculture. Unlike urban areas, rural and remote areas are usually sparsely populated with little disposable income. According to operators, high licensing and spectrum fees are some of the contributing factors to the high costs of the internet. Another challenge is the high backhaul costs due to local governments charging high right of way fees for telecommunications service providers. Early this year it was reported that in Nigeria, 14 state governments charged a 1,000% increase to operators laying fibre optic cables along state roads.[12] On the demand side, affordability of end-user devices and telecoms equipment is affected by high import and tax duties, the costs of which are transferred to the user. This results in economically disadvantaged people being left out.

Across Africa, telecommunication regulators are implementing temporary measures to help keep citizens connected during the pandemic. In South Africa, the Independent Communications Authority of South Africa (ICASA) temporarily granted additional spectrum to mobile operators at no additional cost. This was on condition that the operators would facilitate remote learning and free access to health-related websites. In Zimbabwe, the Postal and Telecommunication Regulatory Authority of Zimbabwe (POTRAZ) allocated additional spectrum to operators for 3G and 4G as well as wireless spectrum to the top telecom operators at no cost. Temporary free access to spectrum has also been offered to Vodafone and MTN by the regulator in Ghana. In Kenya, the Communications Authority of Kenya waived fees on toll-free numbers providing COVID-19-related advisories. However, these responses have shown little to no impact on the pre-existing barriers such as affordability and access to internet-enabled devices.

Broadband Commission for Sustainable Development. https://www.broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf

11 GSMA. (2019). *Mobile Internet Connectivity 2019: Sub-Saharan Africa Factsheet*. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/Mobile-Internet-Connectivity-SSA-Factsheet.pdf

12 Kolawole, O. (2020, 8 January). How increased Right of Way charges could raise data and voice call tariffs. *TechPoint Africa*. https://techpoint.africa/2020/01/08/increased-right-of-way-charges/

Offline and online inequalities have become more pronounced with COVID-19. Unfortunately, the implementation of responses has been top-down, missing critical realities faced by Africans and exposing the gaps in communication among governments, policy makers and citizens, especially those who are socially and economically disadvantaged. A key question to ask is to what extent the responses by both state and non-state actors have been inclusive of all groups in the society.

With COVID-19 responses being largely online, the unconnected are excluded not just from access to the internet, but also the much-needed information and services that affect livelihoods, education and health. Government recommendations during the implementation of the lockdown measures were that schools should find ways of ensuring that learning continued online. However, this would only be possible if students had access to the internet and internet-enabled devices from home. As it stands now, only about 10% of students can access computers from home, with over 80% being unable to get access to the internet, leaving over 330 million learners stranded and more than 8.5 million teachers unable to deliver online classrooms.[13] In Kenya, learning for private universities such as Strathmore University and United States International University-Africa continued, unlike in public universities, where attempts by lecturers were unsuccessful as learners were unable to get online.[14] Furthermore, misinformation and disinformation about the pandemic have been fuelled in online spaces, especially on social media. Hate speech especially has promoted both online and offline violence against foreigners and migrants, exposing the underlying inequalities.

Communities have an important role in curbing the spread of the virus, which means that emergency responses have to be created with communities. One of the key lessons learned from the Democratic Republic of Congo's fight against the Ebola virus was on the importance of communities owning the response measures. Due to the different economic, geographical and sociocultural contexts in countries, cities and villages, one-size-fits-all responses are already proving to be ineffective in some contexts. For example, implementing physical distancing or self-quarantine in informal settlements has not been successful due to the crowded conditions in which families live, as well as the sharing of amenities like public toilets.

From the onset of the pandemic, community organisations and leaders stepped in to provide accurate information on COVID-19, debunking myths related to the virus and translating and contextualising government guidelines. Community networks and community radios are contributing through the dissemination of context-relevant information. Community networks are a complementary

13 UN Sustainable Development Group. (2020). *Policy Brief: Impact of COVID-19 in Africa*. https://unsdg.un.org/sites/default/files/2020-05/Policy-brief-Impact-of-COVID-19-in-Africa.pdf

14 Kigotho, W. (2020, 21 May). COVID-19 – Fuelling a crisis already in the making. *University World News*. https://www.universityworldnews.com/post.php?story=20200518141038342

approach to connecting the unconnected. Unfortunately, the existing policy and regulatory environment does not support small and community-owned networks. Thus, grassroots communities, especially those in rural, remote and underserved areas, are viewed as having a purely passive role as customers. Community networks are telecommunication infrastructures built and operated by, with and for the community. [15] In Africa, these networks take different shapes in terms of their legal registration, some being cooperatives while others are started by not-for-profit or community-based organisations. The key thing is the active involvement and participation of the local community members in different aspects such as the governance and operations of the network. They exist to complement existing activities, and thus contribute to the development of local ecosystems both socially and economically. One of the advantages of these community-led initiatives is the holistic approach in addressing digital inclusion barriers such digital skills, locally relevant content and applications. They also contribute to local economies, workforce development and fostering social connections. In deploying of network infrastructure, these networks use Wi-Fi technologies due to the availability and lower costs of equipment.

During the pandemic, this holistic approach has been proven by the networks going beyond the provision of connectivity services to offering support in the making and distribution of locally made masks. Additionally, community networks like Zenzeleni[16] in Eastern Cape, South Africa and Tunapanda[17] in the Kibera district of Nairobi, Kenya are providing support in their communities through the customisation of health information to the community's local languages and contexts. In Uganda, several community radios continued using their platform to share updates from the Ministry of Health, as well as sharing public health information in the local languages.[18]

CONCLUSION

COVID-19 is a wakeup call on the importance of universal access for all. Internet access and affordability, one of the key principles of the African Declaration on Internet Rights and Freedoms,[19] advocates for affordable access for all Africans regardless of race, colour, sex, language, political or other opinion, national or social origin, property, birth or other status. As more people get online, the internet is now becoming an enabling platform for fundamental human rights such as the right to freedom of expression, freedom of assembly and political participation.

15 Rey-Moreno, C. (2017). *Understanding Community Networks in Africa*. Internet Society. https://www.internetsociety.org/wp-content/uploads/2017/08/CommunityNetworkingAfrica_report_May2017_1.pdf

16 https://zenzeleni.net

17 https://tunapanda.org

18 Myers, M., Harford, N., & Ssemakula, M. (2020, 19 May). Local Radio Stations in Africa Prove Resilient Amid COVID-19. *CIMA*. https://www.cima.ned.org/blog/local-radio-stations-in-africa-prove-resilient-amid-covid-19

19 https://africaninternetrights.org

Above: TunamapandaNET Network
Source: TunamapandaNET

The full impact of the pandemic is yet to be fully realised, as new cases are being reported daily and countries are yet to fully reopen. Although operators have had increased traffic, it is too early to determine if the sector will experience losses or make profits. The responses from regulators have been mainly towards large national operators, in effect leaving out end-users served by small-scale operators and community networks. A key question is how the experiences from the pandemic will shape the future of policy regulation in Africa.

During the pandemic, regulators in Africa have had a fast turnaround in terms of implementation of the emergency responses, which is quite commendable. This should continue post-pandemic. In the past, policy and regulation processes have lagged behind technological advancements. There needs to be a shift in the policy and regulatory frameworks in Africa to recognise the role of community-based operators in addressing geographic and sectoral connectivity gaps. The importance of creating an enabling regulatory environment that addresses digital inequalities cannot be overemphasised.

Communities can no longer be viewed as being on the receiving end of already preconceived policies and regulations. This can be achieved through actively involving community leaders, champions and members who understand local perspectives in policy and regulation formulation and implementation. Relief strategies such as licence or fee exemptions should not only be made available to large national operators, but also to community-based networks or small internet service providers.

In addition to bottom-up engagements with communities, regulators and policy makers should be open to alternative approaches to connecting the unconnected. The connectivity agenda should not only focus on commercially viable areas such as cities, but also consider rural and marginalised communities who require support beyond access. It is not enough to have access; users must have the right digital skills and tools that enable them to fully participate in the digital space.

RIGHT TO DEVELOPMENT

The "forgotten constituency": Making a case for digital rights for prisoners in Zimbabwe during and beyond COVID-19

Author: David Makwerere | Country: Zimbabwe

INTRODUCTION

The evolution of digital communications technology has changed our societies, many of our institutions and the way we live in profound ways. Internet access is now viewed as a basic requirement for many in society. Information on health, education, science, sports, etc. is now easily accessible on the internet. In some developed countries, public administration and bureaucratic communication have gone paperless. This evolution has also ushered in a growing discourse on digital (human) rights. These digital and technological advancements bring with them issues and dilemmas when engaging with certain constituencies in society, however. One such constituency is the prison constituency. In Zimbabwe, just like in many other parts of the world, prison is highly resented by society. Even the government and the ministry in charge of prisons do not seem comfortable to discuss the rights of prisoners, let alone digital rights.

This paper tackles this largely unexplored (at least in the Zimbabwean context) subject on digital rights for prisoners. The COVID-19 pandemic saw the proclamation of a decision by the government of Zimbabwe to limit visits to public spaces like hospitals, banks, colleges and prisons. For prisoners, it means very limited interaction, if any, with the rest of the world. Against this backdrop, this paper engages with the question of digital rights for prisoners and how these can play a part in keeping the prisoners connected to the rest of the world, while also arming them with necessary social, technological and economic skills for post-prison life. The reflections in the paper are based on the African Declaration on Internet Rights and Freedoms,[1] with particular attention

1 https://africaninternetrights.org

was given to Principles 1 (Openness), 2 (Internet Access and Affordability), 3 (Freedom of Expression), 4 (Right to Information), and 7 (Right to Development and Access to Knowledge).

BACKGROUND

Most studies on prisoners have focused mainly on their rights in general but are silent on digital rights and their importance.[2] Digital rights for prisoners remain largely unexplored as a discourse. Although there are a few studies that have explored the importance of digital rights for prisoners in the global North, the field remains embryonic.[3]

The Human Rights Forum reported in 2012 that the rights of prisoners in Zimbabwe are heavily compromised owing to several factors, among them overcrowding, lack of financial and material resources and general neglect.[4] On 27 March 2020, Zimbabwean President Emmerson Dambudzo Mnangagwa issued a presidential amnesty to qualifying prisoners. The reason for the early release of these prisoners was to decongest the prisons in light of the COVID-19 pandemic that has ravaged the world since the beginning of the year. Further restrictions were also made. One such significant pronouncement was the restriction of visits to prisons. What this effectively implies is that prisoners have been further alienated from the rest of the world.

According to the World Prison Brief, Zimbabwe had a prison population of about 22,000 inmates as of March 2020, as well as an overcrowded occupancy rate of 129.4%.[5] The decision to release some prisoners was thus intended to decongest the prisons. While this is commendable, questions should be asked about the welfare of the prisoners who could not qualify for the amnesty. What happens to their basic rights? Such rights as the right to information? Right to education? Right to entertainment? Could these be bridged through digital technologies, and to what extent? What type of digital rights do they have, and to what extent should they enjoy these? What is the role of the state in ensuring digital rights for prisoners? What efforts have been made to provide for the

2 Samanyanga, I. (2005). *A study to investigate the factors contributing to the increased rate of recidivism at Whawha Medium Prison*. Zimbabwe Open University; Human Rights Forum. (2012). *Human Rights Bulletin: March 2012*. http://www.hrforumzim.org/wp-content/uploads/2012/03/Bulletine-71-English.pdf; Human Rights Forum. (2018). *Rights Behind Bars: A Study of Prison Conditions In Zimbabwe*. http://www.hrforumzim.org/wp-content/uploads/2018/10/Prison-Report-2018.pdf; Rupande, G., & Ndoro, I. (2014). Challenges faced by the Zimbabwe Prison Service in implementing Prison Rehabilitation Programs. A Case of Marondera Prison. *International Journal of Innovative Research and Development, 3*(13).

3 Maass, D. (2015, 28 December). Defending Prisoner Rights in the Digital World: 2015 in Review. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2015/12/defending-prisoner-rights-digital-world-2015-review ;Mackey, A., & Maass, D. (2016, 20 January). The Federal Communications Commission Should Ensure Digital Rights for Prisoners and Their Families. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2016/01/fcc-should-ensure-digital-rights-prisoners-and-their-families

4 Human Rights Forum. (2012). Op. cit.

5 https://www.prisonstudies.org/country/zimbabwe

enjoyment of these rights? This paper discusses these questions to remind all relevant stakeholders of the need to uphold the digital rights of prisoners in these trying times and even beyond.

THE PROBLEM

Although human rights law is clear about the rights of prisoners,[6] there is no consensus regarding the extent to which prisoners should enjoy digital rights. The debate has been raging for years.[7] While significant headway has been made in the global North, the same cannot be said of countries in the global South. Nevertheless, it is an agreed fact that prisoners should, for the most part, enjoy human rights as much as any person in the world. The digital revolution also means that prisoners should be considered for digital rights and facilities. What can be debated, though, is the extent to which these can be enjoyed. The primary aim of this paper is to argue for some basic digital rights for prisoners. Such basic digital rights will enable prisoners to communicate, get information about the global COVID-19 pandemic and stay in touch with their families.

HUMAN RIGHTS REGIME FOR PRISONERS

Prisoners are meant to enjoy the generality of human rights, except for those rights, like freedom of movement, which are curtailed as a consequence of imprisonment. In 1990, the Office of the United Nations High Commissioner for Human Rights (OHCHR) provided some basic provisions for the treatment of prisoners. The emphasis is on ensuring the dignity of prisoners while also allowing them the exercise of most of the basic human rights.[8] At the continental level, the Kampala Declaration on Prison Conditions in Africa of 1996[9] is one of several important instruments aimed at ensuring decent conditions for prisoners across the continent. The declaration was passed against the backdrop of serious concern around overcrowding in African prisons.

Another key observation was that rights should be considered in the context of economic development, social and cultural values and social change. Emphasis should be placed on providing education, skills-based training and a work programme that is in the interests of the rehabilitation of the offender while incorporating elements of self-sufficiency and sustainability. The Kampala Declaration also emphasised the importance of protecting the human rights of

---

6 OHCHR. (1990). *Basic Principles for the Treatment of Prisoners*. https://www.ohchr.org/en/professionalinterest/pages/basicprinciplestreatmentofprisoners.aspx; OHCHR. (2005). *Human Rights and Prisons: A Pocketbook of International Human Rights Standards for Prison Officials*. https://www.un.org/ruleoflaw/blog/document/human-rights-and-prisons-pocketbook-of-international-human-rights-standards-for-prison-officials

7 Sawari, A. (2018, 29 August). Do prisoners have rights? *SawariMedia*. https://sawarimi.org/archives/2393

8 OHCHR. (1990). Op. cit.

9 https://cdn.penalreform.org/wp-content/uploads/2013/06/rep-1996-kampala-declaration-en.pdf

prisoners at all times. Of interest to this paper are recommendations (d), (e) and (i) of the Kampala Declaration, which state:

> (d) Urgent and concrete measures should be adopted that improve conditions for vulnerable groups in prisons and other places of detention; such as juveniles, women, mothers and babies, the elderly, terminally ill and very sick, the mentally ill, the disabled, foreign nationals. Procedures that take into account their special needs and adequate treatment during their arrest, trial and detention, must be applied to these groups.
>
> (e) Many prisoners require only minimal levels of security and should be accommodated in open institutions. Wherever possible, prisoners should be encouraged to involve themselves in educational and productive activities with the support of staff.
>
> (i) Channels of communication should be set up with the Special Rapporteur (SR) on Prisons and Conditions of Detention in Africa so that the SR can be assisted and supported in his important task.

The Kampala Declaration was later followed up by the 2002 Ouagadougou Declaration and Plan of Action on Accelerating Prisons and Penal Reforms in Africa.[10] The central theme of the Ouagadougou Declaration also resonated around making prisons more humane and platforms for personal development for inmates. In Zimbabwe, the Zimbabwe Prisons and Correctional Services (ZPCS) generally abides by the global and continental benchmarks, at least on paper. The Zimbabwe Prisons Act (Chapter 7:11) sets the rights of prisoners in line with international best standards and practices. On paper, the provisions are just as good as anywhere in the world, but in practice, life in Zimbabwean prisons is unbearable to many.

DIGITAL RIGHTS FOR PRISONERS IN ZIMBABWE?

The major problem with the laws and statutes on the treatment of prisoners is that the instruments are generally silent on digital rights for prisoners in Zimbabwe. The World Economic Forum has defined digital rights simply as human rights in the internet era.[11] Nitsche and Hairsine provided a more elaborate definition of digital rights when they stated, "Digital rights are considered to be the same fundamental human rights that exist in the offline world – but in the online world."[12] In a resolution on "The promotion, protection and enjoyment of human rights on the Internet", the United Nations Human Rights Council

10 https://www.achpr.org/legalinstruments/detail?id=42

11 Hutt, R. (2015, 13 November). What are your digital rights? *World Economic Forum*. https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/

12 Nitsche, L., & Hairsine, K. (2016, 9 December). What are digital rights? *DW Akademie*. https://www.dw.com/en/what-are-digital-rights/a-36703292

first declared in 2012 and reaffirmed in 2014, 2016 and 2018 that "the same rights that people have offline must also be protected online."[13] From the above definitions, it is clear that digital rights do not imply a reinvention of the meaning of human rights. It simply means enjoyment of the same rights via a variety of digital platforms. Considering that Zimbabwe is still a long way from realising availability of internet connectivity in its public spaces,[14] this paper adopts a working definition of digital rights that embraces the enjoyment of online rights by all members of society including those serving prison time.

What is, however, clear is that very little has been done to ensure that prisoners enjoy at least some basic digital rights. In years gone by, most prisons offered Zimbabwe Broadcasting Corporation Television (ZBC-TV) to their inmates. However, a combination of poor corporate governance practices within most government departments in Zimbabwe and a comatose economy has seen the television sets disappearing from the prison halls. This means that the only basic medium for the enjoyment of digital rights for prisoners has now been taken away. The idea of advanced technologies at this moment in time remains wishful thinking.

MAKING A CASE FOR DIGITAL RIGHTS FOR PRISONERS IN ZIMBABWE

The conditions in prisons across Zimbabwe are appalling, to say the least. They are overcrowded, filthy and poorly maintained.[15] The picture below provides a glimpse of what the internal conditions of a prison look like in Zimbabwe.

Conversations that were carried out in confidence with prison officials in Zimbabwe revealed that there are hardly any digital rights for prisoners in Zimbabwe. It was revealed that most of the facilities are run down and to think of digital rights when securing food for the prisoners is a nightmare is tantamount to daydreaming. First and foremost, prisoners are citizens and must be regarded as such at all times. Just like those citizens who are not serving prison time, they deserve to be kept informed on matters of common concern. The global COVID-19 pandemic is a matter of common concern to all citizens, including prisoners, and in such difficult times, digital platforms can go a long way in keeping the citizenry informed and thus reducing levels of anxiety. As Jewkes and Johnston argue, denying prisoners internet access could be seen "as an example of technology being used as a strategy of social exclusion."[16]

---

13 The 2018 resolution is available here: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/L.10/Rev.1

14 Freedom House. (2019). *Zimbabwe: Freedom on the Net 2019*. https://freedomhouse.org/country/zimbabwe/freedom-net/2019

15 Alexander, J. (2009). Death and Disease in Zimbabwe's Prisons. *The Lancet, 373*, 995-996;Home Office. (2017). *Country Policy and Information Note. Zimbabwe: Prison Conditions, Version 2.0*. https://www.refworld.org/pdfid/589d76684.pdf

16 Jewkes, Y., & Johnston, H. (2009). Cavemen in an Era of Speed-of-Light Technology: Historical and Contemporary Perspectives on Communication within Prisons. *The Howard Journal of Criminal Justice, 48*(2), 132-143.

Above: Source: Jekesai Njikizana /AFP

From a COVID-19 perspective, digital rights can contribute significantly to creating consciousness among the inmates. Inmates getting an opportunity to learn, first hand, from promotional materials from the Ministry of Health, Ministry of Information and the World Health Organization will surely go a long way in educating them about the best practices when dealing with the highly contagious disease. At least those who benefitted from amnesty will find information more readily available in the communities that they are being released into.

The situation is different for those remaining in prisons because they only look up to the prison officials (in most cases junior officers) who hardly have some training on communicating the characteristics of the disease. Although there are dedicated full-time health officers, they are likely to find it overwhelming to discuss the subject with all inmates and regularly. Denying prisoners their digital rights is certainly counter-productive because of the ravaging effects of COVID-19. The government and other stakeholders such as faith-based organisations and civil society should provide basics for the prisoners to allow them some standard of decency. The case for digital rights for prisoners is even more pertinent considering that on 1 June 2020, the ZPCS announced that novel coronavirus infections had been confirmed at two of its facilities, Plumtree and Beitbridge Prisons.

A key argument put forward by proponents of digital rights for prisoners is that the world has gone fully digital. A considerable degree of access to digital rights, especially the right to information, will go a long way in keeping the prisoners abreast with global trends so that when they are eventually released, they will find it easier to reintegrate into society because they already have an appreciation of what is happening in the world around them. Rehabilitation specialists in the ZPCS conceded that they have not considered the potential of digital rights in

facilitating effective rehabilitation. The writer also acknowledges that there is a need for an empirical study to establish the benefits of digital rights in the rehabilitation of prisoners. However, the case for mainstreaming digital rights in prison is one that resonates with global trends.

Beyond the COVID-19 pandemic, digital rights for prisoners can play an important role in addressing the needs of the inmates. For example, if inmates are seeking to continue with their education, whether academic or professional, access to digital rights will ensure that their desires to improve their qualifications are well catered for. Digital education in prisons could be a much more efficient, safe and cheap way of providing for the needs of the prisoners. This will also ultimately save a lot of taxpayers' money. In a world increasingly defined by technology, denying internet access makes it harder for inmates to prepare for life on the outside.

The current emphasis in Zimbabwean prisons appears to be on vocational skills for inmates. While this is commendable, as many of the prisoners get an opportunity to acquire technical and vocational skills necessary for their post-prison survival, this might not be enough. The world has gone digital, and allowing prisoners to enjoy their digital rights is a sure way of enabling their post-prison life adaptation and survival skills. Being internet savvy is rapidly becoming an essential survival skill. Samanyanga lamented that the rate of recidivism in Zimbabwe is very high,[17] although official figures are difficult to maintain.[18] While there is no evidence to show that digital rights can contribute to a reduction of recidivism, it is worth the while to begin to prioritise the provision of these rights for the prisoners.

Prisons must also ensure that inmates have at least some telephone access to their next of kin in these difficult times. This will lessen the anxiety levels among prisoners, since prison visits have been curtailed as part of the measures to keep COVID-19 away from the country's prisons. The enjoyment of digital rights will ensure that families are kept in touch with their loved ones who are serving prison time.

YET ANOTHER EMERGING CONCERN: CHILDREN ACCOMPANYING THEIR MOTHERS IN PRISON

Apart from the inmates, there are children who are accompanying their mothers in Zimbabwean prisons. These children are not offenders but rather victims of circumstances. According to Langa, "Children accompanying their incarcerated mothers in the country's prisons are reportedly suffering more than the offenders because of the harsh prison conditions in the archaic buildings

17 Samanyanga, I. (2005). Op. cit.

18 Rupande, G., & Ndoro, I. (2014). Op. cit.

that were constructed for male offenders only."[19] These children are not prisoners, and legally, they are not covered by international, continental, regional and national statutes for the treatment of prisoners. Nevertheless, they still need proper care and attention. They need to be nurtured properly and to enjoy their rights, particularly the right to education, entertainment and proper care.

Above: Source: Citizen journalist

The United Nations Convention on the Rights of the Child (1989) outlined civil, political, social, economic and cultural rights for children. Mtetwa found that the rights of children accompanying their mothers in Zimbabwean prisons are wilfully violated.[20] The situation is made worse by the fact that the children are not catered for on the food rations for their mothers. There are no proper childcare facilities for the children and their educational needs are not addressed.

Part of the efforts to create child-friendly facilities in prisons will be through advancing digital rights for these children, because their being in prison makes them a part of the "forgotten constituency" that requires attention. Their digital rights are being violated, particularly rights to entertainment and education. Provision of online learning and entertainment for these children will go a long way in ensuring rights for the children accompanying their mothers in prison.

CONCLUSION AND RECOMMENDATIONS

In a nutshell, this article argues that it is high time that national governments on the African continent seriously think of ways of respecting the digital rights of prison inmates. The COVID-19 pandemic has been a great cause of anxiety

19 Langa, V. (2018, 12 November). 'Children suffering more than incarcerated mothers'. *Newsday*. https://www.newsday.co.zw/2018/11/children-suffering-more-than-incarcerated-mothers

20 Mtetwa, P. (2018). *The Forgotten Victims in Zimbabwe's Prisons: Challenges Faced by the Children Accompanying Their Incarcerated Mothers*. Parliament of Zimbabwe.

and uncertainty among people across the globe and prisoners are not immune to this. Denial of digital rights is tantamount to the social exclusion of the prisoners. Providing for digital rights will ensure that prisoners are kept informed of global developments. After all, the Kampala Declaration on Prison Rights and the Ouagadougou Declaration and Plan of Action on Accelerating Prisons and Penal Reforms in Africa call for stakeholders to ensure that prisons are safe spaces for the rehabilitation of offenders. The paper, therefore, recommends that:

- Zimbabwe Prisons and Correctional Services ensure the provision of basic digital rights to prisoners so that they can at least communicate with their families

- To reduce stress and anxiety levels, ZPCS should at least ensure some basic digital entertainment for prisoners during and after the COVID-19 lockdown. This is a necessary consideration to manage the psycho-social effects of confinement among prisoners.

- Prisons should consider mainstreaming digital rights into rehabilitation programmes to effectively prepare prisoners for life after prison. This is a long-term consideration that goes beyond the current COVID-19 context.

- Global, continental, regional and national authorities should consider ways of strengthening the provisions of the African Declaration on Internet Rights and Freedoms to guarantee the rights of prisoners.

- There is a need to ensure that the rights of children accompanying their mothers in prison are met. They might be few in number, but still, their presence warrants a committed effort on the part of the responsible authorities to provide for their rights.

Digital-shy Zimbabwe's schools feel the brunt of COVID-19

Author: Kenneth Matimaire | Country: Zimbabwe

INTRODUCTION

The COVID-19 pandemic has exposed how citizens become vulnerable when governments do not protect and promote human rights in the online environment. The pandemic has critically affected the global education sector, potentially compromising the right to education.

Across the globe, over 1.2 billion children had their right to education infringed following enforced school closures as part of the measures to combat the spread of COVID-19. Most developed countries have turned to alternative means to deliver education through the use of online or electronic learning aided with digital technologies, thereby preserving learners' human rights to education and health. Italy, China and the United Arab Emirates are some of the states that are arguably doing significantly well on education delivery.[1]

However, in Africa, this has been a different scenario all together. African governments are battling over whether or not to reopen school premises, while those that had already taken the bold step to resume classes were forced to abruptly suspend lessons after they recorded a spike in new infections. Henceforth, e-learning has become a central talking point in African settings. In Sub-Saharan Africa, Zimbabwe is a typical example where debate is raging over the need for government to set up human and financial resources to address affordability, access and availability of infrastructure, devices, internet and content to aid e-learning.

1 Daniels, L. (2020, 20 May). Reopening of schools during Covid-19: How other countries have fared. *IOL*. https://www.iol.co.za/news/politics/reopening-of-schools-during-covid-19-how-other-countries-have-fared-48212849

TEACHERS UNIONS TAKE AIM AT PREMATURE REOPENING

In disregard of submissions from various quarters, the government of Zimbabwe announced a phased approach to reopen primary and secondary schools with effect from 28 July 2020, starting with learners writing exams. Ministry of Primary and Secondary Education Permanent Secretary Thumisang Thabela also said mid-year examinations will run between 29 June and 22 July 2020. Thabela said there was enough time to address outstanding health concerns before schools open.

Teachers unions have, however, warned that a rushed approach would be catastrophic at a time when the country's COVID-19 infections are increasing. The infection rate had reached 340 people by 11 June from 149 on 28 May.[2] Health Minister Obadiah Moyo also warned of a major surge.

It must be noted that the COVID-19 outbreak forced schools to prematurely close on 24 March instead of the scheduled term ending date of 2 April. Classes were expected to resume on 5 May. Technically, both teachers and learners lost teaching and learning time, respectively, in terms of syllabus coverage and preparation for June and November examinations.

Teachers unions acknowledge the government's bid to ensure the right to education, but lamented that this is being done at the expense of the right to health. Also, nine schools are operating as quarantine centres,[3] which would disadvantage learners and teachers of occupied schools in the event that classes resume in the given timeline. But the government hinted that it will no longer use schools as quarantine centres and they are set to be rehabilitated and disinfected upon being vacated.[4]

The Progressive Teachers Union of Zimbabwe (PTUZ) has argued that the government – which had over the past two months struggled to test 40,000 people – had no capacity to periodically test 4.6 million students, 136,000 teachers and 50,000 ancillary staff by July 28. Furthermore, according to the PTUZ, the procurement and delivery of test kits, thermometers, sanitisers and personal protective equipment is yet to be done at the 10,000 schools, making an early reopening impossible.[5]

---

2 Xinhua. (2020, 29 May). Zimbabwe's COVID-19 cases climb to 149, adding 17. *XinhuaNet*. http://www.xinhuanet.com/english/2020-05/29/c_139098680.htm

3 ZimFact. (2020, 6 May). Zimbabwe COVID-19 isolation and quarantine facilities. *ZimFact*. https://zimfact.org/factsheet-zimbabwe-covid-19-isolation-and-quarantine-facilities

4 Mashininga, K. (2020, 6 May). Use of colleges as quarantine centres exposes system decay. *University World News*. https://www.universityworldnews.com/post.php?story=20200506085705742

5 Interview with Takavafira Zhou, president of the Progressive Teachers Union of Zimbabwe, 28 May 2020.

Moreover, there is a need to design the school transportation programme, recruit an additional 50,000 teachers, and carry out the infrastructural development to allow physical distancing for a teacher-pupil ratio of 1:20.
"The reopening of schools is not advisable and has no merits whatsoever. Fundamentally, there has been no task force to carry out COVID-19 risk assessment in schools involving teacher unions, health and education officials," said PTUZ president Takavafira Zhou. "We have also recently witnessed a quantum leap of COVID-19 cases in Zimbabwe and opening schools would be against WHO recommendations."[6]

E-LEARNING IN ZIMBABWE

Dr Zhou said solutions to the education crisis posed by COVID-19 must ensure two key human rights, which are learners' right to education with equal measure applied to their right to health. The Parliamentary Portfolio Committee on Primary and Secondary Education concurs and recommends e-learning as the most suitable solution under such circumstances.

"School premises should reopen when it is safe for pupils and teachers. Government should in the meantime focus on e-learning," said the committee chairperson Priscilla Misihairabwi-Mushonga.[7]

Telecoms giant Econet Wireless Zimbabwe has taken the lead as it introduced online learning tailor-made for Zimbabwe's education system. Through its subsidiary Cassava Smartech, Econet launched Akello Digital Classroom[8] and Akello E-Library,[9] which allow students to have online classes and access to hundreds of school curriculum books online approved by the Zimbabwe School Examinations Council and international examination boards. Tertiary institutions had already been making use of Skype and email to foster distance learning, which can be adopted to further learning in junior schools. Zoom and Google Classroom are also among the many platforms recommended by UNESCO's COVID-19 Education Responses.[10]

Misihairabwi-Mushonga said there are other basic e-learning initiatives readily available and already in use such, as the WhatsApp Messenger application, where a parent can help a child follow through educational modules.

---

6 Ibid.

7 Interview with Priscilla Misihairambwi-Mushonga, chairperson of the Parliamentary Portfolio Committee on Primary and Secondary Education, 25 May 2020.

8 Mudzingwa, F. (2020, 28 May). Cassava Launches Akello Digital Classroom With Free Education Content For 1st Month. *Techzim*. https://www.techzim.co.zw/2020/05/cassava-launches-akello-digital-classroom-with-free-education-content-for-1st-month

9 The Herald. (2020, 9 June). Boost for learners as Cassava Edutech launches an e-library. *The Herald*. https://www.herald.co.zw/boost-for-learners-as-cassava-edutech-launches-an-e-library

10 https://en.unesco.org/covid19/educationresponse/solutions

"We should also look at the opportunities brought by e-learning with or without COVID-19. If we invest in information technology, it will help children, even those who have been walking long distances to school," she said.

Several primary school teachers have opened classes through WhatsApp Messenger groups with parents, in which work is given to pupils through their parents. At secondary schools, classes are conducted either directly with students or through their relatives via the same social media platform.

E-LEARNING AND ICTS AS A HUMAN RIGHTS-BASED APPROACH TO EDUCATION

The director of the Zimbabwe Internet Governance Forum, Cade Zvavanjanja, has explained that "the internet and ICTs [information and communications technologies] have a significant role and are relevant in addressing the COVID-19 education challenges, though not a panacea on their own."[11] Zvavanjanja said that although there were various bespoke, free and commercial tools that could be used for e-learning, keys to harness these platforms were access, affordability, availability of infrastructure, digital gadgets, internet and content.

He further stressed that as Zimbabwe leverages the use of technology in response to the COVID-19 crisis, the use of technology must be in line with the African Declaration on Internet Rights and Freedoms.[12] The African Declaration is a pan-African initiative that seeks to give guidance to governments and other public stakeholders in the regulation of the internet and the use of communication technologies. It contains 13 principles to promote internet rights and freedoms.

The Media Institute of Southern Africa (MISA) Zimbabwe, which deals with media and internet rights, has identified principles 2, 4 and 10 as of particular importance to guarantee e-learning.[13] Principle 2 calls for accessible and affordable internet; principle 4 is based on the right to information; and principle 10 focuses on promoting internet access to marginalised groups and those at risk.

The outlined principles set the tone and basis of where Zimbabwe should start from in order to implement e-learning effectively. The African Declaration advocates for internet rights and freedoms as human rights, which dovetails with the trajectory that Zimbabwe is pushing for under e-learning. Therefore, it is imperative that Zimbabwe borrows from these principles to ensure that the process and fruits of e-learning are not compromised.

11 Interview with Cade Zvavanjanja, director of the Zimbabwe Internet Governance Forum, 3 June 2020.

12 https://africaninternetrights.org

13 Interview with Nompilo Simanje, legal and ICT policy officer at the Media Institute of Southern Africa Zimbabwe, 9 June 2020.

Key principles such as wide internet access are essential, as this will avoid a situation where there is wide internet coverage that is, however, beyond the reach of many, or cheap internet charges hamstrung by limited accessibility. Most importantly, the majority of Zimbabwe's schools are in the rural areas that are highly underdeveloped in terms of internet accessibility, infrastructure and power generation – requisites that are essential to e-learning. Therefore, the principles of the African Declaration give Zimbabwe a solid model to adopt when it implements e-learning, considering that various shortcomings have been identified.

SHORTCOMINGS

In the current situation, Zimbabwe cannot fully embrace e-learning, as it would prejudice and be discriminatory to persons without internet access or those who cannot afford access to the internet. Students in rural and marginalised communities do not have the capacity in terms of hardware (mobile phones or other devices that facilitate access to the internet), infrastructure and finances to access the e-learning portals.

Some cannot even afford to purchase the subsidised or discounted data offered by the internet service providers for e-learning. In light of the above, students' access to information continues to be infringed during this time, said MISA Zimbabwe legal and ICT policy officer Nompilo Simanje. According to Simanje, data charges, internet coverage and technical skills required by teachers and students to utilise digital platforms and tools for e-learning remains a stumbling block towards the advancement of the edutech revolution.

MISA Zimbabwe is currently spearheading a #DataMustFall campaign against telecommunication companies that pegged data charges beyond the reach of many. A snap survey indicated that unlimited monthly data costs an average of USD 50 across internet service providers.[14] This technically infringes on affordability of internet, which is a key element towards the e-learning matrix, considering that civil servants who constitute the bulk of Zimbabwe's formal employees earn a paltry ZWL 2,800 (USD 40) as at 12 June.[15]

Zhou concurred and added, "Other than WhatsApp, e-learning is out of reach for many students due to challenges with internet connectivity, let alone affordability."

14 Masarakufa, C. (2020, 2 May). Comparative analysis of internet connectivity options In Zimbabwe. *StartupBiz Zimbabwe.* https://startupbiz.co.zw/comparative-analysis-of-internet-connectivity-options-in-zimbabwe

15 Vinga, A. (2020, 31 January). New Civil Servants Wages To Wipe Out Budget Surplus – Economists. *New Zimbabwe.* https://www.newzimbabwe.com/new-civil-servants-wages-to-wipe-out-budget-surplus-economists

The veteran educationist said e-learning currently has limited applicability due to limited power in rural Zimbabwe coupled with incessant power cuts in major cities.

"Currently more than 65% of secondary schools are not electrified, while more than 75% of primary schools are not electrified. Several schools have no single computer or laptop and it will take a responsible government to ensure that these challenges are addressed," said Zhou, adding that in-service training for the teaching staff is a necessity.[16]

LEGAL AND ADMINISTRATIVE SOLUTIONS

Notably, the Zimbabwean Constitution has a declaration of rights, which suffices as a foundational basis for digital rights. There should be no demarcation as to rights that are exercised online and those that are exercised offline. In terms of a resolution by the UN Human Rights Council, the same rights exercised and protected offline should also be exercised and protected online.[17] Taking note of the supremacy of the Constitution, the foundational framework is present for the exercise of digital rights in Zimbabwe.

However, Simanje highlighted the need to address challenges to do with e-learning from a legal and administrative perspective, taking advantage of the recently gazzetted Cybersecurity and Data Protection Bill[18] that must give direct impetus to the protection and promotion of human rights online.

"The objective is therefore to ensure that online spaces are safe for communication and for transactions as well," she said. "With regards to the educational sector, seeing that children or students will be resorting to the internet for their learning, research included, there is definitely a need to ensure that the online space is safe for them."

GOVERNMENT'S COMMITMENT QUESTIONED

However, Misihairambwi-Mushonga argued that and e-learning enabling environment needed to be available regardless of the COVID-19 pandemic.

"It's sad that government is now contemplating on the possibilities of utilising e-learning now that COVID-19 threatens the education sector," she commented. "If there is anything that the COVID-19 pandemic has done, it has exposed

16 Interview with Takavafira Zhou, president of the Progressive Teachers Union of Zimbabwe, 28 May 2020.

17 ARTICLE 19. (2017, 14 June). ARTICLE 19 at the UNHRC: "The same rights that people have offline must also be protected online". *ARTICLE 19.* https://www.article19.org/resources/article-19-at-the-unhrc-the-same-rights-that-people-have-offline-must-also-be-protected-online

18 Runyanga, N. (2020, 6 June). Cybersecurity Bill: Joining global cybercrime fight. *The Herald.* https://www.herald.co.zw/cyber-security-bill-joining-global-cybercrime-fight

government's reluctance to expedite online learning, which was recommended by Dr. (Caiphus) Nziramasanga back in 1999," she said as she questioned the government's will to embrace the internet.

Veteran educationist Caiphus Nziramasanga, through his 1999 Nziramasanga Commission, recommended the need to digitalise education, but it was not given priority.

Though the late former president Robert Mugabe launched the National Schools Computerisation Programme the following year, it must be noted that the National e-Learning Programme was launched 12 years later. Since then, the Ministry of Primary and Secondary Education has only managed to install internet facilities in 50% of the country's primary and secondary schools as part of its snail-paced efforts to enhance e-learning.[19]

The government signed a memorandum of understanding (MoU) with three contractors, namely ZARNet, e-Learning Solutions and the country's third-largest mobile operator TelOne Zimbabwe. ZARNet was tasked to install internet facilities and services to 1,300 schools at a cost of USD1.1 million, while TelOne was allocated 2,500 schools, and e-Learning Solutions was expected to deal with the remainder. However, the Ministry heaped the slow pace of the e-learning exercise to the contracted players.

"Of the three companies we signed MoUs with, only ZARNet has done something, the rest have not really taken off," said former education minister Paul Mavima.

It should be noted that the ruling party, ZANU-PF, has strong reservations toward the promotion of online spaces, which they describe as advancing a regime change agenda through social media platforms such as Twitter and Facebook. The social media platforms have been used by dissenting voices to expose misrule and corruption in government.

SIX-STEP PLAN TO ENABLE E-LEARNING

Nevertheless, the education sector has clearly illustrated how the country stands to benefit from online spaces, as it has become apparent that reopening school premises exposes not only teachers and learners but their contacts to the deadly COVID-19. Therefore, the government should adopt already existing solutions gathering dust in its archives in the form of the 1999 Nziramasanga Commission recommendations, and expedite school computerisation and e-learning programmes. Pursuant to this, Zimbabwe can follow at least six prerequisites to successfully digitalise education.

19 Matimaire, K. (2019, 20 September). 50% of Zim Schools Connected to WiFi - Govt. *The Industry and Trade Expert*. https://theindustrytrade.com/2019/09/20/50-of-zim-schools-connected-to-wifi-govt/

This starts by respecting the 2000 Dakar Declaration that stipulates that the educational budget must be above 22% of the total national budget. Other complementary funding sources such as the Universal Services Fund administered by the Postal and Telecommunications Regulatory Authority of Zimbabwe could also be utilised to develop ICTs in the sector. The same goes for funding that is currently being channelled into the country for COVID-19 responses.

Second, mobilised funds must be invested in wide internet coverage through infrastructure development. Third, the government must scrap duties on ICTs in order to lower the prices of digital devices such as desktop computers, laptops, tablets and smart phones to make them available at affordable prices, considering that they play a key role for one to connect to the internet.

Fourth, there must be skills enhancement programmes to ensure digitally literate adults targeting teachers, learners and parents to help children cope with their lessons. Fifth, there must be a relevant e-learning course that aligns with the syllabi. Equally important is the need to develop digital literature accessible online and offline. Lastly and most importantly, there is a need to align laws that infringe internet use to the 2013 Constitution and ensure that the Cybersecurity Bill conforms to Southern African Development Community (SADC), African Union and African Declaration principles.

In essence, the COVID-19 pandemic has reawakened the debate on the importance of the internet, which has not been prioritised in Zimbabwe. As the debate rages on, there is a clear indication that Zimbabwe is evolving into the cyberspace as means to circumvent the effects of COVID-19, with the education sector set to become a top beneficiary through e-learning. This cannot become a reality without adhering to the African Declaration principles. Principles 2, 4 and 10, which by and large speak to accessibility and affordability of the internet for all groups, can be safely guaranteed when the Zimbabwean government follows the six-step plan.

Compulsory e-learning in Namibia's public schools: A commendable idea marred by the digital divide?

Author: Nashilongo Gervasius | Country: Namibia

INTRODUCTION

Like much of the rest of the world, Namibia too came under a total economic and social shutdown, due to the global COVID-19 pandemic. A national state of emergency was declared, and the nation joined the rest of the world in a sit and wait-it-out situation.

With this situation, citizens experienced a sheer dilemma in every area of life – at a personal level, economic and survival matters, as well as their health and the education of their children.

The effects of COVID-19 were felt the most at the industrial and informal sector levels, where many were forced to close operations, leaving thousands without the security of a job and unexpected disruptions to livelihoods.

From the flourishing sectors such as agriculture to mining, fisheries to tourism, health to education, all had to shut down. Namibia had suspended operations and joined the rest of the world in a wait-and-see approach.

Two weeks into the national shutdown, the government, through the Ministry of Education, Arts and Culture (MoEAC), in an effort to salvage the educational calendar year and potentially avoid a setback of at least a year or two, called for the implementation of virtual learning in all Namibian public schools, for the duration of the lockdown and beyond.[1]

1 Shikololo, A. (2020, 15 April). Ministry of Education establishes e-learning in schools. *New Era*. https://new-eralive.na/posts/ministry-of-education-establishes-e-learning-in-schools

The directive was that schools would reopen on 20 April 2020, but that no learners would return to school premises, hence the implementation of elearning, where lessons were to be conducted via televisions, radios, print media as well as mobile phones.

Though the directive was vague and with no clear guidelines, a national committee was convened in the Khomas region to come up with ideas on how teaching and learning would take place as an interim solution, until a point where learners and teachers could resume physical contact throughout the country.

Cracks within the education system would soon be exposed by COVID-19, and the detrimental effects they pose to the right to development and access to knowledge, as set out in Principle 7 of the African Declaration on Internet Rights and Freedoms,[2] would become apparent.

E-LEARNING IN A LOW-TECH ENVIRONMENT

The Namibian education system is especially fragile. After 30 years of independence, a journey littered with experimenting with different educational systems, the country had just begun implementing a new national system.

This new system had recently been reviewed and accepted to meet the needs of the country and position the educational system towards meeting global trends. Most importantly, the new system was adopted with the hope of turning around the dismal performances of previous systems, which left thousands of young people out of the educational system altogether, resulting in a staggering youth unemployment rate of 49%.

Being unemployed and without a chance to pursue tertiary education means the inability to self-develop, but also, the community and nation would miss out on access to further knowledge and the income gains these would eventually bring about. This view was supported by Mulama and Nambinga who reported that youth unemployment in the country appears to be on the rise. The two researchers had noted that "high rates of youth unemployment represent both widespread personal misfortune for individuals and a lost opportunity for critical national and global economic development."[3]

The picture of education in Namibia looks as follows: the country has about 30,000 teachers in formal schooling and a population of 800,000 pupils who are teaching and learning in just over 1,900 schools countrywide. A compulsory

2 https://africaninternetrights.org/articles

3 Mulama, L, & Nambinga, V. (2017). *Namibia's Untapped Resource: Analysing Youth Unemployment. National Planning Commission.* https://www.npc.gov.na/download/pbriefs/Analysing-Youth-Unemployment.pdf

education system has been free from primary to secondary school for the last five years now and the free education policy has earned former President Hifikepunye Pohamba a Mo Ibrahim Award for making it an implementation priority during his term of office. Though it has been faced with a number of challenges, there have been benefits too, such as a higher enrolment rates as well as allowing pregnant learners to attend school and allowing them back to continue with studies when they feel safe to do so.

In the higher education segment, there are 16 institutions of higher learning, both private and public. There are also 86 Technical and Vocational Education and Training (TVET) institutions, both public and private. Roughly 67,000 youths are enrolled in universities, while 35,000 are enrolled in TVETs.

In exploring the challenges of the sector in relation to e-learning, it is important to present the picture of technological advancement and most importantly the issue of internet connectivity nationally.

The Ministry of Education, in a circular that made the rounds on social media, indicated that telecommunication infrastructure remained the biggest challenge, with 32% of schools (614) currently having no access to telecommunications. The ministry also noted that 32% of students in the higher education sector had no access to computers or data. The national internet penetration rate is 31%.

While it is plausible that throughout the pandemic, the government acted trying to ensure progress in the education sector, the hasty introduction of e-learning had possibly disadvantaged those without connectivity, consigning them to a future without knowledge and little hope of development.

This has been worsened by a lack of realistic planning that consequently resulted in a situation where there is no progress with a governance framework that clearly articulates the importance of the internet in education and the lives of its people, such as:

- A working information and communications technology (ICT) policy in the education sector.
- A strategic national ICT policy that is inclusive of all aspects of ICT.
- Implementation of a Broadband Policy and a Communication Act which are pro-people.
- A regulatory environment that prioritises access to the internet ahead of licensing fees.
- Government, industry and regulatory sectors which value access to the internet to fully operationalise the Universal Access and Service Fund.

With these challenges in mind, it is clear that free education and e-learning are interdependent and only possible with the required connectivity and ICT infrastructure in place. As set out in the African Declaration on Internet Rights and Freedoms, the internet is vital for giving everyone the right to development and access to knowledge[4] – especially in unprecedented times such as those presented by COVID-19.

PROBLEMS WITH INTERNET ACCESS, AFFORDABILITY AND INFRASTRUCTURE

Thanks to COVID-19, the Namibian education sector was forced into a position that it never even imagined. While this is not just unique to Namibia, the situation presented by the pandemic has probably brought some good and bad.

The good is that it disrupted the everyday dealings of the education system and also unsettled the bureaucracy that sometimes seemed detached from the realities of the education system, such as the fact that not all government schools have access to ICTs. Another good stemming from the COVID-19 situation is that it directed attention to what is important and has been overlooked for so long, namely e-education. While this is positive, the flipside is that there are chronic issues related to ICT access, technological infrastructure and internet affordability in the country.

The Ministry of Education could, however, be lauded for its honesty in highlighting challenges as follows:

- Access to ICT infrastructure and capacity of teachers and learners to access e-learning is limited to predominantly urban schools.
- Public higher education institutions have basic e-learning infrastructure in place, although bandwidth and student capacity to access teaching and learning might be a challenge.
- Private higher education institutions lack infrastructure and capacity to migrate programmes to online learning.
- 28,133 students at higher education institutions do not have access to laptops or tablets and are affected by the cost of data packages.
- E-learning for TVETs is not a plausible option due to the practical nature of training (70% practical and 30% theory); however, e-learning is being explored as an option for education and training delivery of theory in the medium to long term.

4 Principle 7 of the African Declaration.

- The cost implications associated with providing equitable access to all learners are high (a survey and costing are still to be done).[5]

Given these self-defined categories of challenges, it would, perhaps, make it easier to categorise them into three areas which are key in determining the success of e-education and demonstrate its reliance on ICTs and the internet.

ACCESS

Due to a dominance of urban connectivity and a digital divide that for years has been giving urban areas an advantage, rural schools generally are left in the dark by e-education. This challenge is confirmed by the Inclusive Internet Index, which in 2019 reported that only 29.5% of households in Namibia use the internet.[6] With less than 30% of households using the internet, this translates into about 70% to 90% of learners and students with limited or no access to education for the duration of the school closure due to COVID-19. Confirming this, Minister of Education Anna Nghipondoka revealed that only 13,000 learners were able to access the ministry's e-learning platforms during the national lockdown. "This is less than 2% of the total population of 804,000 pupils in state and private schools in the country," she said.[7]

Other proposed means of providing e-education and distance education through traditional media such as radio, television and newspapers also pose further challenges for rural communities. For instance, the usage of radio in an everyday rural household is usually confined to on-the-hour listening to news, given the cost of batteries and availability in certain areas.

This puts learners in rural areas at a further disadvantage, because, unlike at schools where a learner has access to a book and a teacher, at home radios belong to parents or guardians who may prioritise their own access, in addition to factors such as breakage, reception problems and battery costs. A 2019 study published by the Institute for Public Policy Research on media and digital challenges[8] revealed that only 11.8% of Namibian households had a TV set. Given the fact that TV sets are largely electricity operated, the lack of electricity in rural areas further marginalises school communities in rural areas. While many newspapers in Namibia have terminated operations or gone digital, those still operating usually reach remote areas three days to a week later.

---

5 Ministry of Education, Arts and Culture MoEAC. (2020). *Draft Calendar, April 2020.*

6 Smit, E. (2019, 5 March). Namibia's internet costs are too high. *Namibian Sun.* https://www.namibiansun.com/news/namibias-internet-costs-are-too-high2019-03-05

7 Bayer, R., & Nembwaya, H. (2020, 24 April). The glaring digital divide … two worlds of e-learning. *The Namibian.* https://www.namibian.com.na/200377/archive-read/The-glaring-digital-divide--two-worlds-of-e-learning

8 Remmert, D. (2019). *Namibia's Media: Facing the Digital Challenge. Institute for Public Policy Research.* https://ippr.org.na/wp-content/uploads/2019/04/Media_Report-small.pdf

Albertina Isaias, a pre-primary teacher at Oshitudha Combined School in the Omusati region, confirmed that at school level, they were hesitant in "sending school materials home" because care is generally lacking, as most children live with elderly grandparents. These guardians in many cases have a low level of literacy and are unable to pay close attention to school work.

Isaias further noted that a proposed alternative of sending video/audio recordings of teachers to parents and guardians via platforms such as WhatsApp is completely futile because "data prices are too high" and "smartphone devices are completely useless in rural areas," as these use 3G or 4G signals, which are generally not available in wider rural areas. At the same time, the cost of these smartphone devices is quite high and they need to be constantly charged with electricity, which is a luxury in many rural communities.[9]

Further concerns of teachers were captured by Paheja Siririka in an article in the newspaper *New Era*: "It has been a roller-coaster in the world of academics since the ministry decided schools resume as planned but via e-learning platforms. The worries were mostly centered on those students and parents who do not have access to the requisite means."[10]

In this article, Siririka captured various teachers' sentiments. "Our kids cannot do anything in class without first explaining the work in a vernacular; they are still going to fail. Maybe other students across the country can manage but ours need us, and being physically present is more crucial for them," said one teacher.

Another teacher cited lack of technology usage as a barrier to effectively conduct e-learning, and was quoted as saying, "I don't think I am ready. In as much as I am well equipped, I know how to operate all the gadgets, but my main concern is the recipients of this work mode; my learners are not ready and these are the most important custodians."

It is clear that e-learning and distance learning are futile for many rural learners, with only a 2% success rate.[11] This is supported by the secretary general of the Teachers Union of Namibia (TUN), Mahongora Kavihuhua, who condemned the implementation of e-learning, saying the system is not inclusive and many learners and teachers are going to be left out, since not all of them have access to electricity, gadgets or the internet.[12] He was quoted as saying, "As a union, we are repeating that the introduction of elearning is premature and not a solution to the problem. E-learning is a good thing but it should have been implemented years ago for every teacher and learner to be conversant with the system."

---

9 Interview with Albertina Isaias, May 2020.

10 Siririka, P. (2020, 22 April). Teachers worry about e-learning efficacy. New Era. https://neweralive.na/posts/teachers-worry-about-e-learning-efficacy

11 Bayer, R., & Nembwaya, H. (2020, 24 April). Op. cit.

12 NAMPA. (2020, 24 June). TUN slams principals for permitting schooling amidst challenges. *NBC*. https://www.nbc.na/news/tun-slams-principals-permitting-schooling-amidst-challenges.33284

His sentiments are backed up by the unwillingness of teachers and school management, driven by fear and worry, leading to absenteeism and a slow pace of uptake of e-learning while reportedly causing animosity in some districts.[13]

Access to e-learning as well as distance education in higher education is at least available to a certain degree. However, the government has confirmed that exactly 28,133 students at higher education institutions have no access to laptops or tablets and are affected by the cost of data packages too. In trying to remedy this situation, the government, in the heat of COVID-19, hastily committed NAD 9 million (USD 541,000) to boost e-learning.[14]

Some tertiary institutions have gone to the extent of negotiating with telecommunications companies to acquire data devices and packages for students. While the student financial assistance fund made efforts to avail extra funding for its recipients to acquire technological equipment,[15] these efforts could not fully salvage the situation, as many students still had no access to laptops to properly engage with course content. Additionally, the negotiated data usage has also been a headache for certain students, as it is largely inaccessible due to data not being loaded on time or not at all, rendering this exercise as mere tokenism. The issue of data packages and availability will be dealt with in more detail under infrastructural analysis below.

AFFORDABILITY

The cost of data, as reflected on above, is a core determining factor for the success of e-learning and distance education during COVID-19.

In 2018, *The Patriot* reported that Namibia ranked as one of the top 10 countries globally with the highest costs of data, and that Namibians continue to decry the cost of accessing the internet.[16] This survey of 196 countries found that many of the world's poorest consumers are being forced to pay sky-high costs for fixed broadband services, especially in sub-Saharan Africa.

According to the 2019 Affordability Index of the Alliance for Affordable Internet (A4AI), the cost of one gigabyte of internet data in Namibia is USD 8.45.[17] This translates into about 150 Namibian Dollars (NAD). However, for a week of me-

13 Jason, L. (2020, 15 June). Education inspector, principals cross swords. *New Era.* https://neweralive.na/posts/education-inspector-principals-cross-swords

14 Ngutjinazo, O. (2020, 18 June). Ministry to boost e-learning. *The Namibian.* https://www.namibian.com.na/91965/read/Ministry-to-boost-e-learning

15 Kandovazu, E. (2020, 8 April). NSFAF to pay 10k per student to tackle e-learning. *Informante.* https://informante.web.na/nsfaf-to-pay-10k-per-student-to-tackle-e-learning

16 The Patriot. (2018, 5 May). Namibia amongst most expensive globally for day. *The Patriot.* https://thepatriot.com.na/index.php/2018/05/05/namibia-amongst-most-expensive-globally-for-data

17 https://a4ai.org/affordability-report/data/?_year=2019&indicator=INDEX&country=NAM

aningful connectivity, inclusive of online engagement and learning, on average a student household would need more than that.

A National Labour Force Survey conducted during October 2014 indicated that the average monthly household income in Namibia then was NAD 6,626. If we are to imagine accessing at least four gigabytes or more data per month per household, data would cost at least 10% of household income.

With data seemingly this unaffordable, and public libraries and multipurpose centres closed during COVID-19, this means even students who had access to laptops, phones and gadgets could face further challenges in accessing e-learning to its fullest extent. As a result, the majority of students would not be able to complete course assignments and cover all course content, leading to potential failure and possible repetition of courses, perhaps setting students back by a year or more. It may be for such reasons that the second national and largest university has given students an option to cancel their studies for the first semester of 2020.[18]

INFRASTRUCTURE

The Ministry of Education and Culture, on behalf of the government, had explicitly made it clear that "access to ICT infrastructure and capacity of teachers and learners to use e-learning is limited to predominantly urban schools." This has placed students in rural areas at a disadvantage,[19] for instance, because ICT infrastructure depends on electricity and 346 schools (18% of schools nationally)[20] are without electricity and therefore without e-learning.

The government further noted that "public higher education institutions have basic e-learning infrastructure in place although bandwidth and student capacity to access teaching and learning might be a challenge." This concern has been consistently reflected in student complaints on accessing the Moodle platform, a virtual learning management system used by universities to deliver e-education. For instance, at the University of Namibia (UNAM), where e-learning has been in place for about two years prior, the platform capacity became totally overwhelmed during the COVID-19 shutdown, to a point where it was consistently inaccessible for prolonged periods of time.[21]
While UNAM's director of online and distance learning has confirmed readiness to kickstart e-learning amidst the highlighted challenges,[22] the second main

18 https://twitter.com/NUSTFM/status/1277859900710965249

19 Nakale, A. (2020, 15 April). 32% of public schools not equipped for online learning. *New Era.* https://newera-live.na/posts/32-of-public-schools-not-equipped-for-online-learning

20 MoEAC. (2020). Op. cit.

21 Siririka, P. (2020, 15 April). Students weigh in on e-learning. *New Era.* https://neweralive.na/posts/students-weigh-in-on-e-learning

22 Nakale, A. (2020, 8 April). Universities ready for e-learning. *New Era.* https://neweralive.na/posts/

university, the Namibia University of Science and Technology (NUST), was not able to begin immediately, as its elearning platforms were not fully in place. It was perhaps for this reason that the latter offered students a choice to cancel the semester as referred to above. Despite having reported readiness, the challenges in higher education were confirmed through a ministerial document that highlighted that "private higher education institutions lack infrastructure and capacity to migrate programmes to online learning" and that "e-learning for TVETs is not a plausible option due to the practical nature of training (70% practical and 30 % theory)." Consequently, the two main universities have cancelled semester examinations.[23]

E-educational infrastructure aside, ICT and connectivity infrastructure became a real challenge during COVID-19. With more people staying at home during lockdown, this meant driving data usage to towers in residential areas. This has led to user frustration as they became unable to use their data in residential areas because telcos prioritise their services in industrial and business areas. Many students, too, especially those in urban areas, could hardly access e-learning platforms as ICT tower capacities became overwhelmed and upgrades during the first stage of lockdown proved impossible.

For mobile connectivity, Namibia is only 39% covered by 4G (the highest generation of internet connectivity available in the country), according to the Inclusive Internet Index of 2019.[24] The Index further indicates that 3G is only available in 53% of the country, while 2G is available in 100%. This brings about some challenges, including that not many students and teachers are able to do much via WhatsApp platforms as an alternative form of learning, especially for video/audio conferencing or file sharing.

Broadband infrastructure remains a dream in Namibia. With a broadband policy only recently unveiled and broadband coverage still very low, institutions of higher education and schools that are connected could not meaningfully make any impact during COVID-19, as the lockdown meant everybody is working and studying at home. At household level, only 2.53% are covered by fixed-line broadband, according to the Inclusive Internet Index.[25]

CONCLUSION

The challenges posed by COVID-19 regarding e-education during this time are many. The infrastructure problems cause e-learning in Namibian schools to fail, while posing serious challenges to Namibian learners, denying them access to

universities-ready-for-e-learning

23 Iikela, S. (2020, 6 May). Unam, Nust suspend June exams. *The Namibian.* https://www.namibian.com.na/200684/archive-read/Unam-Nust-suspend-June-exams

24 https://theinclusiveinternet.eiu.com/explore/countries/NA

25 Ibid.

knowledge and education as well as a chance to develop themselves and contribute to the development of Namibia in the long run. These challenges have been confirmed by parents, teachers, teacher unions[26] and the student union.[27]

To make it worse, the infrastructural realities discriminate against communities faced with high poverty levels and where internet access is only a dream.

Left: Afraid that teachers would be receiving pay for no work, teachers like Ester Kadhila (seen here) returned to schools to plan how classes will be conducted when they eventually open, but mostly spend their time folding study materials that come as newspaper inserts. Source: Nashilongo Gervasius

To fully embrace and benefit from the internet, Namibia has to be more deliberate in providing a quality e-learning services. This needs to be supported by timely policies, accompanied by budget allocations and clear guidelines and investment in ICT infrastructure.

While implementation of e-learning countrywide was driven by the COVID-19 emergency, it showed 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.[28]

While the free education policy in Namibia should be commended, the COVID-19 scenario exposed that without tangible ICT policies and infrastructure in place and a lack of implementation of the Universal Access and Service Funds, many schools remain left out and learners are disadvantaged.

Namibia's willingness to work with stakeholders and development partners during the COVID-19 pandemic to publish school materials for students who have internet access is also commendable and is a basis for an even further drive to use the internet for general development.

The executive director of the Ministry of Education's acknowledgement of the challenges regarding e-learning is also laudable. It shows that there is hope to

26 Rasmeni, M. (2020, 19 June). Suspend face to face classes for 14 days – NANTU. *Namibia Economist.* https://economist.com.na/53763/health/suspend-face-to-face-classes-for-14-days-nantu

27 Cloete, L. (2020, 16 April). Nanso in //Kharas wants suspension of online Unam classes. *The Namibian.* https://www.namibian.com.na/200157/archive-read/Nanso-in-Kharas-wants-suspension-of-online-Unam-classes

28 https://africaninternetrights.org/about

turn the situation around, acknowledges that individuals and communities have the right to development and that the internet has a vital role to play in the full realisation of nationally and internationally agreed sustainable development goals.

Internet access is a vital tool for giving everyone the means to participate in development processes. For this reason it is important for Namibia to acknowledge and comply with the Declaration of Principles on Freedom of Expression and Access to Information in Africa, as adopted by the African Commission on Human and Peoples' Rights in November 2019.[29]

Principle 37.2 of the Declaration should be prioritised by the Namibian government: "States shall recognise that universal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression, access to information and the exercise of other human rights."

Namibia should also work to improve "information and communication technology and internet infrastructure for universal coverage" as stated in 37.3.b of the Declaration; as well as "promoting local access initiatives such as community networks for enabling the increased connection of marginalised, unserved or underserved communities" (37.3.d); and "facilitating digital literacy skills for inclusive and autonomous use" (37.3.e).

Finally, to ensure successful implementation of e-services such as e-learning, as covered in this article, Namibia should implement Principle 43.1 of the Declaration, to "adopt legislative, administrative, judicial and other measures to give effect to this Declaration and facilitate its dissemination."

29 https://www.achpr.org/presspublic/publication?id=80

https://africaninternetrights.org/