





### **REGULATORY FRAMEWORK ANALYSIS:**

SELECT AFRICAN COUNTRIES COVID-19
REGULATIONS AND IMPACT ON DIGITAL
RIGHTS

### Disclaimer

The information in this Report has been compiled on the basis of publicly available information; internal data and other sources believed to be true. This Report is for general guidance only, and has not been verified independently. Whilst every effort is made to ensure the accuracy and completeness of information contained herein, we take no responsibility and assume no liability for any error/ omission or accuracy of the information provided. Opinions contained in this Report represent those of the author at the time of publication only. Forward-looking information or statements in this Report contain information that is based on assumptions, forecasts of future results, predictions not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of their subject matter, to be materially different from current expectations.

To the fullest extent allowed by law, the author and EndCode (Pty) Ltd shall not be liable for any direct, indirect or consequential losses, loss of profits, damages, costs or expenses incurred or suffered by you arising out or in connection with the access to, use of or reliance on any information contained in this Report.

The information that is contained in this Report should not be construed in any manner whatsoever as personalised advice.

TABLE OF CONTENTS

### **TABLE OF CONTENTS**

Disclaimer	2
TABLE OF CONTENTS	3
LIST OF ABBREVIATIONS/ACRONYMS	4
INTRODUCTION	5
EXECUTIVE SUMMARY	7
IMPACT OF REGULATIONS ON FREEDOM OF EXPRESSION	11
IMPACT OF REGULATIONS ON PRIVACY AND PERSONAL DATA PROTECTION	18
IMPACT OF REGULATIONS ON SECURITY, STABILITY AND RESILIENCE OF THE INTERNET	29
IMPACT OF REGULATIONS ON FREEDOM OF ASSEMBLY AND ASSOCIATION AND	
THE INTERNET	42
IMPACT OF REGULATIONS ON RIGHT TO DUE PROCESS	49
RECOMMENDATIONS	56
REFERENCES	63

LIST OF ABBREVIATIONS

### LIST OF ABBREVIATIONS/ACRONYMS

Abbreviation /Acronym	Meaning
AFDEC/Declaration	African Declaration on Internet Rights and Freedoms
APC	Association for Progressive Communications
AU	African Union
CIPESA	Collaboration on International ICT Policy in East and Southern Africa
COVID-19	Coronavirus Disease of 2019
ECOWAS	Economic Community of West African States
EFF	Electronic Frontier Foundation
HRDC	Human Rights Defenders Coalition
ІСТ	Information and Communications Technology
ICTA (Mauritius)	Information and Communication Technologies Authority
MACRA	Malawi Communications Regulatory Authority
MCS (Angola)	Minister of Social Communications
MFWA	Media Foundation for West Africa
MISA-ZIM	Media Institute for Southern Africa-Zimbabwe
OHCHR	Office of the High Commissioner for Human Rights
RSF	Reporters Without Borders
SADC	Southern African Development Community
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organisation
who	World Health Organisation
ZICTA	Zambia Information and Communications Technology Authority

INTRODUCTION

#### INTRODUCTION

The global spread and reaction to the COVID-19 virus, civil society organisations, human rights and digital rights activists have highlighted a range of potential and actual human rights violations as the continent responds to the COVID-19 pandemic. These include limitations to the exercise and/or facilitation of the enjoyment of rights through the internet or other digital mediums. These limitations are associated with new laws or amendments to existing laws which governments have relied upon as a direct response to the COVID-19 pandemic. - to reduce the spread of the virus, maintain track and trace databases of infected persons and curb the spread of mis- or disinformation.

The African Declaration on Internet Rights and Freedoms ("AFDEC"/"the Declaration") is a "pan-African initiative to promote human rights standards and principles of openness in Internet policy formulation and implementation on the continent". The purpose and intended use of the Declaration is to provide a tool and baseline of measurement to inform human rights on the Internet in order to "meet Africa's social and economic development needs and goals. The Declaration builds on existing human rights initiatives, reports and frameworks such as the African Charter on Human and Peoples' Rights, the Windhoek Declaration on Promoting and Independent and Pluralistic African Press, the African Charter on Broadcasting, the Declaration of Principles on Freedom of Expression in Africa, and the African Platform on Access to Information Declaration.

The AFDEC Coalition, consists of various individuals, from non-profit organisations and civil societies. The Coalition identified the significance of <u>digital rights and freedoms</u>, as societies and communities across Africa have become increasingly digital and reliant on the Internet for communication, education, work and social interaction. The Coalition supports and promotes safeguards for digital rights and freedoms with the intention of informing legal and policy development and practices ensuring that such rights and freedoms are protected from a grassroots level.

The Secretariat of the African Declaration on Internet Rights and Freedoms Coalition launched the COVID-19 & Digital Rights Rapid Response Fund. The Fund is an extension of the Strategic Advocacy Fund that forms part of the project aimed at "Securing human rights online in Africa through a strong and active 'African Declaration on Internet Rights and Freedoms' network. This emergency response initiative is aimed at ensuring the promotion and protection of human rights online in response to existing national internet-related policies and COVID-19 prevention, containment and treatment policies. The initiative facilitates strategic interventions by Coalition members as they monitor and respond to the implementation of existing internet-related

policies and national COVID-19 prevention, containment and treatment policies that involve digital technologies.

This Report is a strategic intervention facilitated by the AFDEC COVID-19 & Digital Rights Rapid Response Fund. The Report identifies regulations that Angola, Malawi, Mauritius, South Africa, Zambia and Zimbabwe have enacted in response to the COVID-19 pandemic with a view to considering the implications on select digital rights:

- the right to freedom of expression
- The freedom of assembly and association and the internet
- the right to privacy and personal data protection
- the right to the security, stability and resilience of the internet
- the right to due process.

The scope of this Report is limited to identifying and discussing the impact of regulatory measures adopted by select African governments as a response to the COVID-19 global pandemic on the selected set of rights above. The AFDEC is thus used as a baseline against which various regulatory interventions are measured in order to identify possible and actual digital rights violations. This is not to say that the remaining rights enshrined in the AFDEC have not been violated or otherwise affected by COVID-19, however, said impacts on the remaining rights falls outside of the scope of this Report.

Sources of information include governmental repositories of laws and regulations as well as secondary sources such as commentary and opinions of experts, academics, and civil society groups on the implications of the regulatory responses to the COVID-19 pandemic on the select digital rights.

Limited experts, knowledgeable within the digital rights space and who have an in-country perspective on the actual impact of the COVID-19 laws and regulations were consulted.

### FREEDOM OF EXPRESSION

Everyone has the right to hold opinions without interference. Everyone has a right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds through the Internet and digital technologies and regardless of frontiers. The exercise of this right should not be subject to any restrictions except those which are provided by law, pursue a legitimate aim as expressly listed under international human rights law (namely the rights or reputations of others, the protection of national security, or of public order, public health or morals) and are necessary and proportionate in pursuance of a legitimate aim.

# PRIVACY AND PERSONAL DATA PROTECTION

Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication. The right to privacy on the Internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law, (as specified in Article 3 of this Declaration) and are necessary and proportionate in pursuance of a legitimate aim.

# SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

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

# FREEDOM OF ASSEMBLY AND ASSOCIATION

Everyone has the right to use the Internet and digital technologies in relation to freedom of assembly and association, including through social networks and platforms. No restrictions on usage of and access to the Internet and digital technologies in relation to the right to freedom of assembly and association may be imposed unless the restriction is prescribed by law, pursues a legitimate aim as expressly listed under international human rights law (as specified in Principle 3 of this Declaration) and is necessary and proportionate in pursuance of a legitimate aim.

### RIGHT TO DUE PROCESS

Everyone has the right to due process in relation to any legal claims or violations of the law regarding the Internet.Standards of liability, including defences in civil or criminal cases, should take into account the overall public interest in protecting both the expression and the forum in which it is made; for example, the fact that the Internet operates as a sphere for public expression and dialogue.

**EXECUTIVE SUMMARY** 

-------

### **EXECUTIVE SUMMARY**

### Impact of Regulations on Freedom of Expression

With the understanding that African countries have an obligation to provide accurate reports, statistics, updates, contacts and health precautions during COVID-19 African countries have a corresponding obligation to ensure that false information harmful to the population regarding the pandemic is mitigated. This Report observes, however that under the auspice of controlling the spread of harmful or potentially harmful false news, Countries have installed or entrenched regulatory mechanisms that place limitations on the right to freedom of expression.

The spreading of false and misleading information, with intent or without, has been a global issue prior to the pandemic. This crisis has emphasised the prolific nature of the issue and concerns in regulatory responses. The primary concern being the response fails to adequately balance rights to freedom of expression. Whilst, the impact of unbridled dissemination of false information pertaining to the virus is clear, freedom of expression should be viewed as crucial in addressing and dealing with the COVID-19 pandemic.

Cases of excessively punitive measures for the spreading of false and misleading information, criminalising the offence or providing vague definitions of what constitutes misinformation, especially in the context of opinions are diagnosed in the Regulations under study. Whilst the Regulations may not be unlawful, these have the effect of regulatory over-step insofar as the restrictions on the freedom of expression are concerned. In the context of the Declaration the legitimacy of the restrictions is debated..

### Impact of Regulations on Privacy and Personal Data Protection

The Report observes that to varying degrees, the Countries COVID-19 Regulations limit the rights to privacy and personal data protection as defined in the Declaration.

Across the Countries, their Regulations envision compulsory screening, testing and medical examinations that place limitations on privacy in the offline realm and the resulting and the protection of personal data in the digital realm. Across the majority of the countries, the adequacy of safeguards and oversight measures ordinarily invoked to avoid possible encroachments into privacy rights is lacking. Regulations in Angola and South Africa, as positive measures, place notification and reporting obligations (to respective authorities) concerning the

processing of health status and other personally identifiable information of potentially infected persons.

The further (additional) processing of personal data by authorities for purposes of containing COVID-19 was identified as an area of potential risk. Limitations on the processing, safeguards and oversight mechanisms are inadequate, and Regulations include provisions that are ambiguous in intent or scope. In such cases, personal data handling during and post the pandemic will have varying impacts on the privacy of persons.

South Africa's Regulations as a positive example, does include safeguards and oversight mechanisms in respect of its Department of Health's COVID-19 Database and the tracking and tracing activities of its authorities.

In the context of the Declaration, and the conditions for legitimate restrictions on the right to privacy, Countries Regulations may on assessment be legitimate but the potential prejudice to the privacy rights of persons both during and post the pandemic is clear.

### Impact of Regulations on Security, Stability And Resilience Of The Internet

This Report points to the efforts of selected Countries through Regulations to endorse the benefits of an Internet that is secure, stable and resilient, that is supported by mutual cooperation between stakeholders particularly during the COVID-19 pandemic.

Malawi and South Africa have both taken steps, legislatively, to ensure that the stability of the Internet, in-country, is maintained during periods of national lockdowns and other times where freedoms such as the freedom of movement is restricted. The impact thereof being that from an infrastructural perspective, the propensity for internet disruptions due to technical or other reasons can be mitigated.

Considering the potential for unlawful surveillance and monitoring of individuals by State and non-State actors during the COVID-19 pandemic, all Countries under study indicated at least the capacity if not actual institution of a contact tracing system - tracking infected persons as well as those persons that may have reasonably come into contact with infected persons. Sensitive information such as infection status, name, identity number and address are generally captured by these systems. The key enquiry becomes the safeguards to ensure the legitimacy of the contract tracing system - does it go too far?

South Africa is the only Country that has expressly created an online COVID-19 database. The regulations establishing this database also provided for a number of strict data processing and

access requirements such as access logging and the use of encryption services. From the Regulations, the implications and methodology behind the system are clear and surveillance and monitoring made under this system can be interrogated during and post the pandemic to determine its lawfulness. The remaining Countries by comparison, do not expressly provide for the conditions to interrogate the lawfulness of the databases and systems that may be used to facilitate surveillance and monitoring for the purposes of contact tracing.

Finally, the nature of this right is predicated on accessing an Internet that is secure and stable. Access to the internet itself in the Countries under study are subject to socio-economic limitations. The persisting digital divide ultimately means that the meaningful exercise of this right is a fiction .

### Impact of Regulations on Freedom of Assembly and Association

The Declaration provides that "everyone has the right to use the Internet and digital technologies in relation to freedom of assembly and association, including through social networks and platforms". As a result of the COVID-19 pandemic, governments from the Select African Countries, which form the subject of this Report, have not been observed to have taken actions that expressly impact this right. In this Report, the focus was placed on examining regulatory limitations to the freedom of assembly or association online.

None of the Countries COVID-19 Regulations have an express provision that restricts the right to use the internet or digital technologies and association in relation to freedom of assembly and association. The freedom to form, join and associate with online communities, furthermore has not been expressly limited by the Regulations enacted or relied upon by the Countries under Study.

Importantly, all of the observed Countries adopted a form of national lockdown in response to the COVID-19 pandemic limiting the physical right to freedom of assembly and association by consequence. Zambia adopted a partial lockdown providing for the designation of infected areas, which allowed for free assembly outside of those areas. Lockdown regulations establish offences for violating acts of physical assembly and association but do not expressly restrict communications calling for potentially violating acts of assembly or association.

### Impact of Regulations on Right to Due Process

Key Principle 11 of the Declaration encompasses three themes of governance. The first is: how and when a person is arrested or detained. The second: do people have full access to courts and the third: do people have a guarantee to a lawfully and procedurally fair trial. If any of these three

forms of due process are infringed by any regulation, international standards require that the limitation be made clear based on a legitimate aim, necessity, and proportionality.

The practical importance of a public interest consideration in implementing arrests, access to courts and lawful trials has already been seen in Zimbabwe.

Moreover, if the law pertains to the limitation of internet activities – a space where a large population in Africa is already uninformed about, there is a greater call for regulations that consider public interest.

Research indicated that excessive penalties such as harsh prison sentences or fines would potentially infringe further rights as contained in the Declaration and should not be relied upon to curb issues such as the spread of mis- or disinformation during the pandemic. While there is a need to curtail the spread of misinformation it is worrying that, in Zambia for example, ZICTA is reverting to a law that was invalidated by the courts. It was observed that sufficient steps need to have been taken to make sure the public is aware of the reasons for the restrictions and the need to comply with them. States must also put in place measures for people to be able to comply with the restrictions, including by enabling them to satisfy their essential needs.

FREEDOM OF EXPRESSION

### 1. IMPACT OF REGULATIONS ON FREEDOM OF EXPRESSION

### 1.1. Introduction

In terms of Article 3 of AFDEC "everyone has the right to hold opinions without interference". This right provides everyone with the right to freely express themselves' "seek, receive and impart information and ideas", regardless of the kind of information or opinion. In terms of AfDec, this right should not be restricted except where such a limitation is in pursuance of a legitimate intention/aim that is listed under international human rights laws, in particular, the right to freedom of expression should not impact the rights or reputations of others, the protection of national security or public order, public health or morals. In addition, the limitation needs to be necessary and proportionate in pursuance of the legitimate aim.

In practice, AfDec's right to freedom of expression requires that there can be no "content blocking, filtering, removal and other technical or legal limits on access to content" as this would constitute a restriction on the right to freedom of expression and can only be justified if they strictly comply with international human rights, as mentioned above. Freedom of expression online calls for all peoples to be able to engage individually or collectively in expression of their views and opinions through the internet with respect and use the Internet as a "tool and platform for a protest action".

No-one should be held liable for content on the Internet of which they are not the author, accordingly, judgments to remove content from sites made by self-regulatory systems should be done so taking into account the need to protect the right to freedom of expression. Processes adopted by the regulatory bodies need to be transparent and include provision for appeals.

States are obligated to take positive steps to prevent violent attacks against any person in its territory, especially, when the people being attacked are being attacked for expressing their opinions online.

States are required by the AFDEC to create a favourable environment for "participation in public debate by all persons" where their opinions can be expressed without fear. Should an attack occur, the State is further required to launch an effective investigation and to bring the perpetrators and instigators to justice. Victims should be provided appropriate remedies for the harm suffered.

States are called on to review and reform legislation related to the right to freedom of expression online and to ensure that such legislation complies with international standards. Particularly,

criminal defamation, sedition and speech related offences should be abolished, including their application online.

### 1.2. Relevant Regulations

## 1.2.1. Regulations impacting the right to hold opinions without interference; and the freedom to seek, receive and impart information and ideas.

During the COVID-19 pandemic a number of Countries have enacted or enforced laws that prohibit the spreading of misinformation, disinformation and mal-information.

<u>UNESCO</u>, defines these terms as follows:

- "Disinformation: Information that is false and deliberately created to harm a person, social group, organisation or country"
- "Misinformation: Information that is false but not created with the intention of causing harm"
- "Mal-information: Information that is based on reality, used to inflict harm on a person, social group, organisation or country."

Below is a consideration of the regulations of misinformation, disinformation and mal-information, colloquially referred to as "fake news" with a view to assess any resulting limitation on freedom of expression. Excessive prohibitions or the lack of adequate definitions of what is "fake news" can result in an overstep in the regulations and direct or indirect restrictions on the right to hold opinions and freedom to seek, receive and impart information and ideas on the internet without interference and the legitimacy of such limitations.

#### 1.2.1.1. **Malawi**

In Malawi, section 21 of the <u>Public Health (Coronavirus Containment and Management) Rules 2020</u> provides that where a person furnishes or gives false or misleading information to an enforcement officer, he or she is liable for an offence. The scope of these Rules, as it pertains to Key Principle 3, is limited to the interaction between an individual and an enforcement officer. For reference, an "enforcement officer" includes, amongst other things, a health officer, a police officer or an immigration officer. The impact of this, on the right to freedom of expression, is that the Rules do not provide for the element of intention. This means that a statement could be construed as falling within the scope of the Rules even though it was not made with intent to mislead or knowledge of its falsity.

### 1.2.1.2. **Mauritius**

Mauritius passed the <u>Information and Communications Technologies Act</u>, 2001, which provides in Section 46 that:

"(f)forges a message or transmits or otherwise makes use of a message knowing that it has been forged;

(g) knowingly sends, transmits or causes to be transmitted a false or fraudulent message; (ga) uses telecommunication equipment to send, deliver or show a message which is obscene, indecent, abusive, threatening, false or misleading, which is likely to cause or causes annoyance, humiliation, inconvenience, distress or anxiety to any person;"

Although this Act was not passed during the COVID-19 pandemic, it has been used to combat the spreading of misinformation during the pandemic. Recently, <u>arrests</u> have been made in accordance with this Act due to actions taken by Mauritians with reference to COVID-19.

#### 1.2.1.3. **South Africa**

South Africa's <u>Regulation 11(5)</u>, published in terms of the <u>Disaster Management Act</u>, prohibits the publication of misinformation regarding COVID-19. More specifically, the Regulation provides that any person who publishes any statement, whether online or offline, with the intention to deceive any other person about COVID-19, the COVID-19 infection status of another person and any Government measure taken to address COVID-19, is guilty of an offence. Such a person is liable on conviction to a fine or imprisonment for a period not exceeding six months, or both. Misuse of this Regulation as well as the criminalisation of spreading information which may deceive impacts the right to freedom of expression, as contained in AFDEC.

### 1.2.1.4. **Zambia**

The <u>Public Health Infected areas COVID19 Disease 2019 Regulations No. 22 of 2020</u>, in Section 8, mandates any person who becomes aware or has reason to suspect that another person has died or is suffering from COVID-19 shall immediately inform the nearest authorised officer in a local authority or public health facility. The issue with this Section of the Regulations is that it creates an obligation to supply information, however does provide further guidance on what the details of said information must be. Thus the risk exists that unverified information or base opinions are communicated in both good and bad faith the result of which may be construed as

false or misleading ex post facto. This lack of clarity could have a negative impact on the exercising of the right to freedom of expression.

The Zambia Information and Communications Technology Authority (ZICTA), warned Zambians, during March 2020, not to circulate fake and unverified information regarding the Coronavirus using various ICT platforms. In its statement, ZICTA stated that it would support law enforcement agencies to ensure that those that violate the law by spreading false information on ICT platforms will be prosecuted. The law ZICTA refers to is Section 67 of Zambia's Penal Code which prohibits the spreading of false information likely to cause harm. Section 67 relieves the prosecution of its burden to prove the elements of a crime which could result in the conviction of an accused person despite the existence of a reasonable doubt of their guilt. This provision restricts the persons accused of breaching this provision an opportunity to prove lack of knowledge of the falsity of the information published or circulated or that reasonable measures were taken to verify the truthfulness of the information.

The provision was declared unconstitutional in the case of <u>Chipenzi vs The People</u> where it was found to extend beyond the permissible limitations to human rights established in Article 20(3) of the <u>Constitution of Zambia</u>. Under the Article, a restriction to the right to freedom of expression must be reasonable and for a legitimate aim. The Court found that liability for prosecution and conviction under Section 67 of Zambia's Penal Code did not appear to have a dependency on actual occurrence of public fear or alarm or disturbance of public peace - fundamental to the offence. Instead the State's perception of the possible impact of the expression may have on the public was the basis. Evidently, the risk this posed for misuse was obvious and unacceptable.

### 1.2.1.5. **Zimbabwe**

In Zimbabwe, <u>Statutory Instrument 83 of 2020</u> Public Health (COVID-19 Prevention, Containment and Treatment) (National Lockdown) Order, 2020 provides in Section 14 that false reporting during the national lockdown is prohibited. In particular, the Section states that any person who publishes or communicates false news about any public officer, official or enforcement officer involved with the enforcing or implementing of the national lockdown or about any private individual that has the effect of prejudicing the State's enforcement of the national lockdown, shall be liable for an offence. If found guilty, the individual shall be liable under <u>Section 31 of the Criminal Law Code</u> (the Section that provides for penalties for the publishing or communication of false statements prejudicial to the State). The penalty for this crime is a fine up to or exceeding ZWE\$ 5 000 000.00 or imprisonment for a period not exceeding twenty years or both.

The provisions of Statutory Instrument 83 and section 31 of the Criminal Law Code do not define what false information is or provide a presumption of innocence for a person that was reasonably unaware of the falsity of the information. This, therefore, creates the potential for unreasonable restriction on the right to freedom of expression online as there is no clarity on what statement would fall under the meaning of "false news".

1.2.1.6. The exercise of the right to freedom of expression should not be subject to any restrictions, except those which are provided by law, pursue a legitimate aim as expressly listed under international human rights law (namely the rights or reputations of others, the protection of national security, or of public order, public health or morals) and are necessary and proportionate in pursuance of a legitimate aim

Although AfDec provides for the protection and promotion of the right to freedom of expression online, it recognises that there are instances when the limitation to the right to freedom of expression may be necessary in pursuance of a legitimate aim and are necessary and proportionate to achieve said aim. The Regulations enacted, as a response to the COVID-19 pandemic, in Malawi, Mauritius, South Africa, Zambia and Zimbabwe, had varying degrees of impact on the right to freedom of expression, as contained in the AFDEC. In the observed Countries, the purpose of these Regulations was, in context, to curb and penalise the spread of misinformation concerning COVID-19. However, the definition of what constituted misinformation or what entailed misleading was not made clear or even provided in these Countries. In conjunction thereto, the harsh punishment and criminalisation of spreading misinformation could have a negative impact on the exercising of the right to freedom of expression. AFDEC provides for situations when the right to freedom of expression may be limited, on justifiable grounds. Taking steps to curb misinformation is not an automatically prohibited restriction on the right to freedom of expression as siad restriction is justifiable. However, it is the aforementioned overreaches or penalties that exceed the bounds of lawfulness and thus impact the right to freedom of expression.

### 1.3. **General Observations**

As the pandemic presented an unprecedented crisis which demanded a swift response, there may be cases where, even in Countries with generally robust protections for freedom of expression, governments may have inadvertently promulgated regulations which infringe fundamental rights. Not all Countries created new regulations – Zambia and Mauritius are examples where there was reliance on existing laws (from 1962 and 1925) to declare their States of emergency or disaster.

These Regulations in certain instances limit or prohibit freedom of expression, unlawfully. AfDec Article 3 provides that there are legitimate reasons for limiting the right to freedom of expression and governments must have applied their minds to this whilst considering the proportionality and necessity when passing the Regulations which affect the right. The limitation or prohibition across the Countries has been for a legitimate purpose (halting the spread of misinformation) and is necessary in the interest of public health.

It has, however, been noted that the Regulations restricting the spread of false information, as well as compelling people to provide requested information to law enforcement, carried with them criminal sanctions and heavy fines. Article 19, in its Policy Brief titled, <u>Viral Lies: Misinformation and the Coronavirus</u>, advised that states should refrain from criminal prosecution as a primary measure to stop the spreading of misinformation pertaining to COVID-19. Criminal sanctions should be reserved for more grievous infractions. In Zimbabwe for example, any person found liable for spreading false information may be found liable for a fine that may exceed ZWE\$ 500 000.00 or a sentence not exceeding 20 year. The criminalising of the actions of individuals who disseminate false and inaccurate information about COVID-19 should be proportional to the harm that can be caused to the public. In South Africa for instance, the regulations criminalised the spread of false news on the virus, punishable by up to six months imprisonment, a fine, or both. Although, the prison sentence is less than that provided for in Zimbabwe's regulations, criminal sanctions for the spreading of information negatively impact and limit the right to freedom of expression.

It has also been noted that, although States did not enact regulations that explicitly and unreasonably restrict the right to freedom of expression online, it was that application of these regulations that led to the restriction of the right. This is the case in Zimbabwe where it was reported that a Mr. Zvokusekwa allegedly caused the publishing and spreading of an announcement allegedly from President Mnangagwa that the national lockdown period would be extended. Mr. Zvokusekwa was arrested for infringing upon terms of Section 31 of the Criminal Law Code. However, after his arrest, President Mnangwagwa announced the extension of the national lockdown as per the "false" statement published. Further, the Media Institute of Zimbabwe - Zimbabwe has reported several people have been arrested and charged in terms of Instrument 83, with the matters pending in court. It stands to reason that should the circumstances be identical to that of Mr. Zvokusekwa, the arrestees may not be found guilty of spreading false information. In Zambia, the ICT Authority ZICTA, warned citizens that should anyone spread false news they would be prosecuted in terms of a provision in the Penal Code that had been declared unconstitutional.

With regard to the right to receive information, governments are demonstrating a proactive response in terms of communicating with the public on information regarding COVID-19. Angola released a communication strategy where the government detailed its plans to disseminate

information to inform the public. South Africa has an Emergency Hotline, Whatsapp support line and a Resource Portal to keep citizens informed.

### 1.4. Analysis of Impact of Regulations

Principle 3 of AFDEC, requires States to create safe spaces, online, for people to hold opinions without interference. Moreover, these online spaces should allow for people to seek, receive and impart information. This allows for people to participate in public discussions and debate, in a manner that does not infringe on others rights or cause public and national harm. However, Principle 3 also recognises that in accordance with international human rights laws, there are instances when the right to freedom of expression can be limited. This limitation should be reasonable and proportionate to the reason for the limitation. According to the <u>United Nations</u> it cannot be overemphasised that any limitation of human rights, with the appropriate justification must be done with a high level of fidelity and transparency.

Although the right to freedom of expression online has generally been preserved, States have had to combat the spread of misinformation and disinformation regarding COVID-19, which the <u>United Nations</u> has stated, has the potential to cause harm to the public. This has led to States enacting laws that may be used to infringe on the right to freedom of expression. It is important to reiterate that limiting freedom of expression for the purpose of curbing misinformation is not unlawful, unless the appropriate legal mechanisms are not followed. These regulations were further required because, according to <u>Gumede</u>, there is a need for accurate information that is accessible and evidence based to be disseminated, especially during a public health crisis.

However, Article 19, has observed that in an effort to combat the spread of misinformation and disinformation, States have taken advantage of the national emergency or disaster regulations to pass Regulations that repress and unreasonably limit the right to freedom of expression. Herein lies the true issue. It has been observed that many governments have used the COVID-19 pandemic as an opportunity to attack the right to freedom of expression and thereby the fundamental human rights granted to African citizens as per international human rights law as well as contained in the Declaration. This infringement on the right to freedom of expression has manifested itself in overbearing penalties or lack of clarity pertaining to the scope of what constitutes misinformation. Furthermore, the UN Human Rights Committee has stated that the use of criminal law as a means of restricting freedom of speech must only be used in the "most severe cases" and that ultimately a prison sentence is wholly unsuitable.

# PRIVACY AND PERSONAL DATA PROTECTION

## 2. IMPACT OF REGULATIONS ON PRIVACY AND PERSONAL DATA PROTECTION

#### 2.1. Introduction

Principle 8 of the Declaration concerning privacy personal data protection states that:

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

"The right to privacy on the Internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law, (as specified in Article 3 of this Declaration) and are necessary and proportionate in pursuance of a legitimate aim."

The wording of Principle 8 of the Declaration is strongly inclined towards privacy in the online context, on the internet. However, when reference is made to the application of Principle 8 in the Declaration, its scope broadens to apply to all processing of personal data, which must be processed "in compliance with well-established data protection principles".

In consideration of what would constitute legitimate aims, Article 3 of the Declaration points to: "the rights or reputations of others, the protection of national security, or of public order, public health or morals". In the context of a pandemic, these legitimate aims will need to be assessed on a case-by-case basis to determine whether they are proportional in the circumstances.

### 2.2. Relevant Regulations

### 2.2.1. Regulations Impacting the right to privacy online

In South Africa, the right to privacy online, and the right to the protection of personal data, have been impacted by the <u>Disaster Management Act Regulations</u>, <u>Government Gazette</u>, <u>18 March 2020</u>, <u>No. 43107</u> ("The DMAR"), the amendments thereto, and Directions that have been issued in terms of the DMAR.

### The Disaster Management Act Regulations

Regulation 4 of the DMAR, prohibits any person from refusing medical examination (including the taking of any bodily sample by an authorised person). Importantly, this Regulation constitutes a direct limitation of the right to privacy and the protection of one's special personal information (health information, genetic data, etc).

Under the DMAR, as <u>amended</u> (25 June 2020), Regulation 8(2) entitles the National Department of Health to develop and maintain a national database to combat COVID-19, "including contact tracing and geospatial hotspot mapping". Regulation 8(3) allows the database to include all information necessary to guide appropriate responses to COVID-19, which information may include, but is not limited to: "first name and surname, identity or passport numbers, residential address and other address where such person could be located, and cellular phone numbers".

Additionally, the most recent amendments to the DMAR (25 June 2020) have added new sub-regulations which may impact privacy online. In particular:

- Regulation 8(20) entitles the National Department of Health to "develop and implement electronic systems or applications to be used on mobile devices or computers in order to collect, on a voluntary basis, information from members of the public for inclusion in the COVID-19 Database", subject to various additional requirements listed under Regulation 8(20); and
- Regulation 8(21) entitles the National Department of Health to receive, "on a voluntary basis, information regarding members of the public from electronic systems or applications operated by private entities for inclusion in the COVID19 Database", subject to various additional requirements listed under Regulation 8(21).

### The Electronic Communications. Postal and Broadcasting Directions

Regulation 10(8) of the DMAR expressly provides a catch all provision entitling any Minister to "issue and vary directions, as required, within his or her mandate, to address, prevent and combat the spread of COVID-19, from time to time, as may be required...".

In terms of Regulation 10(8), the Minister of Communications and Digital Technologies issued Electronic Communications, Postal and Broadcasting Directions on 26 March 2020. Under the initial Directions, Paragraph 8(1) required Electronic Communication Network Service (ENCS) and Electronic Communications Service (ECS) Licensees, as well as the "internet and digital sector in general", 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". On 8 May 2020, the original Directions were amended and Paragraph 8(1) was removed.

However, to date Paragraph 8(2) of the Directions remains, which requires the South African Post Office ("SAPO") to make available its national address system and any applicable database to assist the relevant authorities in their tracking and tracing efforts. Paragraph 8(2) goes on further to allow a database of the SAPO to be correlated with other sources from the Government and private sector.

### 2.2.2. Regulations Impacting the right to the protection of personal data concerning him or her.

Across the selected African countries, all have introduced some form of legal instrument to regulate national responses to the COVID-19 pandemic which have privacy implications. The legal instruments have varied from Regulations to Directives, Rules, Decrees and Orders, most stemming from a disaster management statute, or a public health statute.

### 2.2.2.1. **Angola**

The core regulatory instrument issued in Angola in response to the COVID-19 pandemic was Presidential <u>Decree 142/20</u>, 25 May 2020. Article 12 of the Decree (*unofficial translation*), provides that the competent authorities in Angola can determine that quarantine and testing be mandatory. Furthermore, Rule I (9) (*unofficial translation*) sets out a reporting obligation for persons to notify authorities of sick/infected persons.

### 2.2.2.2. **Malawi**

Malawi issued the <u>Public Health Act</u>, <u>Public Health (Corona Virus Prevention, Containment and Management)</u> Rules, 2020 (the "COVID Rules"). Under these Rules, Rule 6 makes testing for COVID-19 compulsory. In particular, an enforcement officer may order an individual to immediately submit to a medical examination, which "may include but not be limited to the taking of a bodily sample".

#### 2.2.2.3. **Mauritius**

In Mauritius, an Act of law was introduced alongside Regulations to deal with the COVID-19 pandemic in its country, both of which concern the protection of personal data for Mauritians.

### The COVID-19 (Miscellaneous Provisions) Act

Mauritius passed the <u>COVID-19</u> (Miscellaneous Provisions) Act No. 1 of 2020 ("the Miscellaneous Provisions Act") on 16 May 2020. Section 13 of the Miscellaneous Provisions Act has amended the Mauritian Data Protection Act, 2017 ("the DPA") through the addition of a new exception to the application of the DPA under Section 44(1)(f). Section 44(1)(f) states that the DPA will not apply where the processing of personal data is necessary for the issuing of "any licence, permit or authorisation during the COVID-19 period." The purpose of this amendment is to enable the issuing of licenses, permits or authorisations during the 'COVID-19 period', without being impeded by the provisions of the DPA.

#### The Public Health Act Regulations

Section 9 of the <u>Public Health Act Regulations</u> issued under Government Notice No. 58 of 2020 makes provision for screening assessments. Thereunder, a person being screened by a medical practitioner in Mauritius is required, under Regulation 9(2), to disclose "information about other persons with whom he may have travelled or had contact", "his contact details or such other sufficient information so that he may be contacted immediately" and must allow the practitioner to "take his biological sample". Similarly, under Regulation 9(3), a parent of a child is required to provide relevant information about persons whom the child has been in contact with, and allow the practitioner to take a biological sample of the child. Importantly, it is an offense under Regulation 19(1)(b) to refuse to undergo screening.

### 2.2.2.4. South Africa

Under South Africa's DMAR, Regulation 4 prohibits any person from refusing medical examination (including the taking of any bodily sample by an authorised person). Furthermore, Section 16.10 of the Department Of Employment and Labour COVID-19 Occupational Health And Safety Measures In Workplaces COVID-19 (C19 Ohs), 2020, requires employers of organisations to notify the Department of Health and the Department of Employment and Labour of any infected employees, as well as provide administrative support for contact tracing purposes.

### 2.2.2.5. **Zambia**

Regulation 4(2) of <u>The Public Health (Infected Areas)(Coronavirus Disease 2019)</u> Regulations, 2020 ("the COVID19 Regulations") prohibits a person from non-compliance with "any direction of an authorised officer" (which refers to listed health officers under Regulation 2 of the COVID19 Regulations). Regulation 4(2) does not provide further detail on what such a 'direction' may

include. If such a direction includes being subject to a medical examination, then Regulation 4(2) may constitute a limitation on the right to the protection of personal data belonging to Zambian citizens.

### 2.2.2.6. **Zimbabwe**

The Government of Zimbabwe has issued <u>Statutory Instrument No. 99 of 2020 - the Public Health (COVID-19 Prevention, Containment and Treatment) (National Lockdown) (Amendment) Order, 2020 (No. 5). Under Section 11F of the Order, all persons "operating or employed in a business or industry in the formal commercial and industrial sector" are required to submit to compulsory screening and testing for COVID-19, prior to resuming work. Section 11F(2) of the Order provides that persons may elect to be tested by way of a rapid results diagnostic test or through another other test approved by the Minister of Health.</u>

### 2.2.3. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication.

Whilst, Angola, Malawi, Mauritius, South Africa, Zambia and Zimbabwe have all passed COVID-19 related Regulations, none of them prohibit, encourage or contain any reference to interceptions of communications online, or monitoring of internet behaviour in their respective Countries.

There have been no Regulations in South Africa that allow the interception of electronic communications of South African citizens. Whilst South Africa's Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 may allow the lawful interception of electronic communications in certain instances, there have been no publicly reported cases of the use of the RICA for these purposes as of writing.

# 2.2.4. The right to privacy on the Internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law, (as specified in Article 3 of this Declaration) and are necessary and proportionate in pursuance of a legitimate aim.

The COVID-19 Regulations passed in Angola, Malawi, Mauritius, Zambia and Zimbabwe do not encourage or contain any reference to a restriction of the right to privacy on the internet. However, unlike these countries, South Africa has passed Regulations (described above) that may limit or restrict the right to privacy on the internet insofar as one's movement and location is concerned.

#### 2.3. General Observations

An observation of the regulatory developments in the selected African Countries insofar as they concern privacy and personal data protection has indicated the following:

- The most prevalent overarching limitation on the right to privacy has not been in an online context, but rather, in an offline context where persons have been required to submit to compulsory screening, testing and medical examinations, under which, their personal data and special personal data can be collected, processed and stored. Of the selected African countries, all six (6) Countries (Angola, Malawi, Mauritius, South Africa, Zambia, Zimbabwe) have made Regulations requiring mandatory screening, testing and medical examinations.
- It has been observed that three (3) of the selected African Countries (Malawi, Mauritius and Zambia) have provisions which are broadly drafted. South Africa and Malawi make provision for the taking of 'any' bodily sample and to submit to a medical examination which includes but is not limited to the taking of a bodily sample, respectively. Mauritius does not define 'the COVID Period' leaving room for an open-ended duration of exceptional processing, and Zambia provides for compliance with "any direction" of an authorised officer.
- Only one (1) of the selected Africa countries has introduced Regulations which impact the right to privacy in an online context South Africa. Whilst contact-tracing by public authorities may take place without the immediate knowledge or awareness of South African data subjects, the voluntary collection of information that has been envisioned in South Africa's Regulations has been drafted with data protection principles and safeguards in mind and may therefore be argued to be proportionate to the aim (securing public health).
- Mauritius is the only selected African country that has passed amendments to a national data protection law.

### 2.4. Analysis of Impact of Regulations

### 2.4.1. **Privacy Offline**

### Compulsory Screening, Testing, Medical Examinations and Reporting Obligations/Notification

As observed above, across all of the selected African Countries, compulsory screening, testing and medical examinations were provided for in national Regulations. The impact of these Regulations are that the right to the protection of one's personal data (including special personal data), in an offline context, are being encroached upon where one's consent is not required.

In other cases, reporting and notification obligations to authorities in Angola and South Africa that require the sharing of health status, name, location, identity number and other personally identifiable information of persons to authorities, directly impacts the privacy and protection of personal data belonging to such persons. The same concerns apply to the sharing and repurposing of State owned databases in South Africa's case.

When considering the context within which these Regulations were issued, it may be argued that each pursues legitimate aims of protecting the 'rights of others' (the rights to life and safety) and 'public health' - in accordance with the legitimate aims provided for in Principle 3 of the Declaration. However, caution should be exercised in cases where the wording in Regulations is open-ended or ambiguous, which may potentially enable state or private actors to misuse the personal data collected. In such cases (where personal data may be used for purposes that go beyond the original aim for collecting such data), the legitimacy of such conduct may be brought into question, which may in turn bring into question the legitimacy of the new aim. Accordingly, in cases of over-broad or ambiguous Regulations, the importance of oversight mechanisms cannot be emphasised enough.

An ancillary aspect of compulsory screening, testing and medical examinations is the further processing of collected personal data by authorities for purposes of containing COVID-19. In such cases, the manner in which personal data is handled will have varying impacts on the privacy of persons. In this regard, a <u>Guidance Note</u> issued by the Office of the United Nations High Commissioner for Human Rights has touched upon important considerations for the protection of personal data belonging to persons that have been subjected to compulsory medical examinations, or surveillance under the auspices of track and trace measures. Quoting from the Guidance Note:

"Health monitoring includes a range of tools that track and monitor the behaviour and movements of individuals. Such surveillance and monitoring should be specifically related to and used exclusively for public health-specific aims and should be limited in both duration and scope as required in the particular situation. Robust safeguards should be implemented to ensure any such measures are not misused by Governments or companies to collect confidential private information for purposes not related to the public health crisis" (Office of the United Nations High Commissioner for Human Rights, 2020, 6).

Considering the fact that legitimate aims exist in all of the above mentioned scenarios, the focus of attention should therefore be shifted from the 'collection stage' of personal data, to the 'processing stage' - in other words, how is the personal data being used, stored, shared, secured and ultimately de-identified or destroyed after it has been collected. Drawing from the Guidance Note, the duration and scope of processing of personal data are essential, as well as the presence and extent of safeguards to protect such sensitive information.

As a positive case in point, South Africa has, in accordance with its Regulations (Regulation 11H(13)), appointed a 'COVID-19 Designated Judge' to oversee the COVID-19 Database managed by the Department of Health. In terms of Regulation 11H(15), the Designated Judge "may also make such recommendations... regarding the amendment or enforcement of this regulation in order to safeguard the right to privacy whilst ensuring the ability of the Department of Health to engage in urgent and effective contact tracing to address, prevent and combat the spread of COVID-19" (Department of Justice and Constitutional Development, 2020). Regulations 11H (16) - (17) also provides express time periods for notifications to persons that have been tracked, and for the de-identification of the contents of the COVID-19 Database.

Conversely, the Regulations in the other Selected African Countries do not expressly require, or provide, any details on what kind of safeguards are to be put in place to protect personal data that is collected and processed through screening, testing and medical examinations, nor what steps will be taken to delete it after its purpose has been fulfilled. To illustrate the importance of adequate safeguards to protect personal data collected, in April 2020 the The International Criminal Police Organisation (Interpol) issued a statement advising that it "has detected a significant increase in the number of attempted ransomware attacks against key organizations and infrastructure engaged in the virus response" (Interpol, 2020).

Accordingly, where countries have not provided for adequate safeguards in line with data protection principles, the impact of their Regulations may be prejudicial to the privacy rights of persons. Therefore, whilst such actions may strive towards legitimate aims in terms of the Declaration, it is vital that governments in the Selected African Countries "ensure that patient"

confidentiality is protected even as authorities take steps to identify those who may have been exposed to the virus" (Human Rights Watch, 2020).

### Amendments to National Data Protection and Privacy Laws

In Mauritius, the implication of the Amendment to its DPA is that the rights, duties, obligations and various other legal restrictions which would usually be afforded to data subjects, will not apply to the processing of their personal data when required for the issuing of "any licence, permit or authorisation during the COVID-19 period." Of significance is that the Miscellaneous Provisions Act does not set out who may issue licenses, permits, or authorisation and does not define 'the COVID-19 period' both of which have been drafted widely - despite the scope of exclusion provided for in the amendment having been crafted with specificity.

It may be concluded that whilst legitimate aims exist to increase the speed at which licenses, permits and authorizations are issued in Mauritius (which are in the interest of protecting the rights of others and public health), these types of ambiguities in the drafting of Regulations should be avoided to guard against the misuse of such exclusions.

### 2.4.2. **Privacy Online**

### **Tracking and Tracing - Surveillance**

Civil advocacy groups such as the Electronic Frontier Foundation (EFF) have vocalized their stance on the use of tracking technologies, specifically during the COVID-19 pandemic, as they believe that the use of these technologies carries significant risks to "individual privacy and civil liberties" (Crocker, Opsahl & Cyphers, 2020).

In considering the impact of South Africa's <u>Regulations</u> providing for the tracking and tracing (surveillance) of persons in the country, it is important to firstly distinguish between those surveillance activities which are voluntary and those which are involuntary. By requiring the express opt-in consent of South Africans in certain scenarios (such as those relating to the use of both official and non-official contact tracing and other mobile applications and programmes), the impact on the right to privacy is to some extent mitigated. Saying that, both voluntary and involuntary forms of track and trace measures ought to integrate data protection principles and provide appropriate safeguards to meet best practice standards.

As put by the African Declaration on Internet Rights and Freedoms Coalition, "States and other relevant stakeholders should strictly implement the principles for the lawful processing of personal information set out in their domestic data protection laws or regional standards,

including the relevant time periods, the way in which the data will be handled, and the conditions of access, storage and security of the information" (African Declaration on Internet Rights and Freedoms Coalition, 2020, 12).

In South Africa's case, its Regulations clearly require compliance with data protection principles and the implementation of adequate safeguards when handling personal information processed in the context of COVID-19. In particular:

- **Regulation 8(20)(a)-(c)**: When collecting information from electronic systems or applications on mobile devices/computer, information may only be collected subject to various limitations which include specified purposes for processing, express opt-in consent, and transparency about:
  - which information will be collected and stored via the electronic system or application;
  - the means by which the information will be collected and stored;
  - the purposes for which any information will be collected and used;
  - the entities or persons to which that information will be transmitted, and under what conditions; and
  - whether the information will be kept on the user's mobile device or a centralised server;
  - the period for which the information will be retained; and
  - the notice that will be given to users when the information has been destroyed.
- Regulation 8(21)(a)-(c): When receiving information from electronic systems or applications operated by private entities for inclusion in the Department of Health's COVID-19 database, it must be on a voluntary basis and provided that:
  - The information may only be received and used in order to guide appropriate responses in addressing, preventing and combating the spread of COVID-19, including for the purposes of geospatial hotspot mapping;
  - The private entity concerned has obtained the information concerned from users of mobile devices and computers on a voluntary and opt -in basis; and
  - The private entity concerned has obtained the express consent of the user concerned to transmit the information to the National Department of Health for inclusion on the COVID-19 Database.
- The sub-contracting of the Department of Health's functions (to any other organ of State or private party) under the Regulation may only be undertaken in specific circumstances:

Regulation 8(23)-(24): "where it is not reasonably possible for the services to be performed by the Department of Health itself due to the Department of Health not having the necessary expertise, equipment or personnel available or due to the delays that would result from the Department of Health performing the services itself"), and subject to specific safeguards.

Accordingly, and on the basis of the content of its Regulation, South Africa's track and trace measures and their impacts on the privacy and protection of personal data online, may be deemed justifiable. Not only do they seek to achieve legitimate aims envisioned by the Declaration, but they reasonably provide for the protection of such personal data. As noted by CIPESA, "Covid-19 surveillance and data-based tracking interventions have been affected in haste, and with limited precedent and oversight mechanisms" (CIPESA, 2020). In practice, it will need to be seen whether such safeguards are complied with by relevant authorities and other actors involved, and enforced by those with oversight functions.

# SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

# 3. IMPACT OF REGULATIONS ON SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

#### 3.1. **Introduction**

Key Principle 9 of the Declaration states that:

"Everyone has the right to benefit from security, stability and resilience of the Internet. As a universal global public resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network.

Different stakeholders should continue to cooperate in order to ensure effectiveness in addressing risks and threats to security and stability of the Internet.

"Unlawful surveillance, monitoring and interception of users' online communications by state or non-state actors fundamentally undermine the security and trustworthiness of the Internet" (AFDEC).

The application of Principle 9 manifests in obligating governments to take the necessary steps to ensure that its citizens enjoy the Internet as a secure and stable resource. This would mean that legislative steps must be taken that promote minimum security measures such as encryption as a standard in information management. Additionally, governments must be persuaded from allowing the inclusion of "backdoors" that allow public and non-public access to citizen information who are using encryption services. Governments must refrain from unlawful surveillance or interception of citizen information, without due process. Additionally, there must be cooperation between the public and private stakeholders to ensure that the Internet and the services which it allows access to, are secure and stable.

#### 3.2. Relevant Regulations

3.2.1. Regulations impacting the right to benefit from security, stability and resilience of the Internet.

#### 3.2.1.1. **Angola**

In response to COVID-19 the Angolan Government released the Communication Strategy. The purpose of this Strategy is to maintain an open channel of communication between the Angolan Government, its departments and the Angolan people as it pertains to developments as a result of COVID-19. The Angolan Government has indicated that it will be using social media as a primary means of communication as well as SMS services. The Strategy, however, does not indicate whether the internet infrastructure or security on the Internet will be managed during the pandemic. The concern that this raises is that whilst social media support will be provided, the actual stability and security of internet services is not guaranteed. This Strategy disinvests the Government from maintaining its own communication services as it places a large reliance on existing platforms, all of which are based in foreign jurisdictions and thus susceptible to controls that do not fall under the Government's mandate or its own controls.

#### 3212 **Malawi**

The <u>Public Health (Coronavirus Containment and Management) Rules 2020</u>, specifically Section 10 and Part 1 of the Schedule attached thereto, provide for a list of services which are to continue to operate during COVID-19 national lockdown. Included in this list are communication, navigation and surveillance system services. If a service is declared "essential" it is allowed certain liberties such as its employees not being confined to private dwellings during a lockdown, so that the service may be provided during the pandemic.

#### 3.2.1.3. **Mauritius**

Despite enacting a number of laws and regulations as a response to the COVID-19 pandemic, these laws and regulations do not have a direct impact on the right to benefit from a secure, stable and resilient Internet.

#### 3.2.1.4. South Africa

The <u>Disaster Management Act</u>: Electronic Communications, <u>Postal and Broadcasting Directions</u> of 26 March 2020, establish the directions to facilitate the availability and use of digital technologies to combat the spread of COVID-19 in South Africa. Section 6.1 of the Directions obligates all service providers of electronic communications networks and services (telecommunications infrastructure and services) to ensure continuance of electronic communication services during the pandemic.

In terms of Regulations Issued In Terms Of Section 27(2) Of The Disaster Management Act, 2002 gazetted on 29 April 2020, as per Table 1, all information and communication technology services as well as those services required to maintain them, were declared "essential" under National Alert Level 4 lockdown. "Essential" in this context means that persons involved in providing these services are allowed to travel and not be confined to a private dwelling for work purposes. Please note however, that South Africa is currently in National Alert Level 3.

#### 3.2.1.5. **Zambia**

Despite enacting a number of laws and regulations as a response to the COVID-19 pandemic, these laws and regulations do not have an impact on the right to benefit from a secure, stable and resilient Internet.

#### 3.2.1.6. **Zimbabwe**

In response to the COVID-19 pandemic, Zimbabwe declared a State of Disaster as per the <u>Civil Protection</u> (Declaration of State of Disaster: Rural and Urban Areas of Zimbabwe) (COVID-19) Notice. The important aspect of this Notice and the declaration contained therein, is that the State of Disaster covered both urban and rural areas. Despite explicitly stating that the State of Disaster applied to both rural and urban areas, no differentiation was made, in the Notice, as to how these two types of areas would be affected. The impact that this may have on the right to a stable and secure internet, as per the Declaration, is that a blanket declaration of a State of Disaster, which impacts a number of liberties, including those exercised via the Internet or digital means, must take into consideration that this right is exercised to differently in rural compared to urban areas. This being due to unequal access to Internet and communication services in more rural areas. Which in turn means that those living in rural areas will have their right to benefit from a stable and secure Internet exponentially more impacted.

3.2.2. Regulations impacting stakeholders cooperating in order to ensure effectiveness in addressing risks and threats to security and stability of the Internet.

#### 3.2.2.1. Angola, Malawi and Zambia

Despite enacting a number of laws and regulations as a response to the COVID-19 pandemic, these laws and regulations do not have an impact on stakeholder cooperation.

#### 3.2.2.2. South Africa

The <u>Directions On Zero-rating Of Websites For Education And Health Issued Under Regulation</u> 4(10) Of The Regulations Made Under The Disaster Management Act, 2002 (Act No. 57 Of 2002) provide a framework for the zero-rating of websites subject to approval by the National Department of Basic Education. These include websites of educational institutions, local websites offering free access to educational content resources Department of Basic Education and Provincial Education Departments' websites or portals, all COVID-19 related websites identified by the Department of Health, and local websites offering free access to COVID -19 health content resources.

Furthermore, the Department Of Communications And Digital Technologies has provided technical parameters which need to be complied with prior to a website being zero-rated. These include: websites with missing technical information required by network operators for zero-rating, such as SNI (Server Name Identification), will not be zero-rated. The site owner or administrator must provide the network operator with default login details in order to facilitate zero-rating for websites that need to be zero -rated and are using login authentication.

Section 2 of the Regulations Issued In Terms Of Section 27(2) Of The Disaster Management Act, 2002 gazetted on 18 March 2020, mandate that the Department of Defence must, for the duration of the declared national State of disaster, release and mobilise any available resources ensure the delivery of essential services. Additionally, institutions within national, provincial and local government must make resources, other than funding, available to implement these Regulations. The Regulations Issued In Terms Of Section 27(2) Of The Disaster Management Act, 2002 gazetted on 29 April 2020 declared that all information and communication technology services are "essential" services.

#### 3.2.2.3. **Zimbabwe**

The <u>Statutory Instruments 83 of 2020</u>, specifically, Section 2, provides a list of "essential services". Included in this list are "communications and telecommunication services, including the Internet". Section 4 of the same Statutory Instrument states every other business establishment shall be closed except for every business establishment providing an essential service or services in support of such a service. The effect of this is that during the national lockdown, essential services and those supporting said services may continue to operate as well as being granted other allowances such less restricted travel obligations. As such, during the pandemic, the continued operation of the Internet and communication services can be guaranteed, as much as

possible, as those responsible for its upkeep and operation are provided the necessary freedoms to operate effectively.

## 3.2.3. Regulations impacting surveillance, monitoring and interception of users' online communications by State or non-State actors

#### 3.2.3.1. **Angola**

Article 34 of the <u>Angolan Constitution</u> grants individuals the inviolable right to secrecy of correspondence and other means of private communication, across various mediums such as postal, telegraphic and telephonic. Any interference of this right by a public authority can only be done if allowed, via a ruling by the competent judicial authority. This corresponds directly to Principle 9 as it protects individuals from unlawful interception of their online communications.

<u>Presidential Decree No. 142/20 of 25 May 2020</u>, has been issued by the Angolan Government in response to the continued effect of COVID-19 on the country. As such, the purpose of this Decree is to define and adopt a set of measures until the return to normality, in essence further disaster mitigation procedures and processes. Article 10 of the Decree provides for access control procedures to establishments as well as the duty, on identification, to report cases of infection to the health authorities. Article 11 of the Decree, provides for the reinforcement of active search and monitoring of contacts. This is expanded in Point 9 of the General Rules attached to the Decree, where the obligation to notify health authorities.

#### 3232 **Malawi**

The Public Health (CORONA VIRUS PREVENTION, CONTAINMENT AND MANAGEMENT) Rules, 2020, were enacted by the Malawian Government in order to enable the implementation of measures to prevent, contain and manage the COVID-19 pandemic in Malawi.

Section 16 of the Rules provides that where a person needs to travel to or from a restricted area, as defined in the Rules, that person must obtain a permit from an enforcement officer nearest to that person or at the point of entry into or exit from a restricted area, authorizing travel. The inference from the implementation of this process is to allow the Government to monitor the movement of persons who have reasonably come into contact with persons infected with COVID-19. The Rules do not indicate whether this data is used for monitoring purposes directly nor any further details on how it is stored, transmitted or accessed.

The possible impact that this law may have on Principle 9 is that it may give to a system which allows public authorities to monitor and surveil persons infected with COVID-19.

#### 3.2.3.3. **Mauritius**

In terms of the <u>Quarantine Act</u>, 2020, Section 9, creates the obligation that every person shall provide a quarantine officer with information that will allow said officer to determine whether a person may have reasonably come into contact with any person who has or may have a communicable disease. Additionally, the Act creates a duty on any person to disclose to a quarantine officer if they suspect that they have been in contact with a person who may have a communicable disease, such as COVID-19. The inference is that the Mauritian Government intends to create a contact tracing database in order to determine the possible spread of COVID-19.

The Act does not state how this information is gathered or whether electronic means will be used to monitor the movement of infected persons or possible contact with other people. Therefore, it is not determinable whether this provision will have effect on Principle 9 of the AFDEC.

The <u>COVID-19 (MISCELLANEOUS PROVISIONS)</u> Act, 2020 amends a number of Mauritian laws, including those pertaining to Data Protection and Information and Communications Technology, however these amendments pertain to permit issuing and authorisation and do not directly impact the rights contained in Principle 9.

#### 3.2.3.4. **South Africa**

In <u>Regulations</u> issued on 29 April 2020, under the Disaster Management Act, 2002, the National Department of Health was mandated to develop and maintain a national database 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.

The "COVID-19 Tracing Database", subsequently renamed "COVID -19 Database" by <u>Regulations</u> issued on 26 June 2020, may include all information considered necessary for the National Department of Health to guide appropriate responses in addressing, preventing or combatting the spread of COVID -19, including but not limited to:

the first name and surname, identity or passport numbers, residential address and other address where such person could be located;

- cellular phone numbers of all persons who have been tested for COVID19;
- the COVID -19 test results of all such persons; and
- the details of the known or suspected contacts of any person who tested positive for COVID-19.

According to the 26 June 2020 Regulations, the National Department of Health may develop and implement electronic systems or applications to be used on mobile devices or computers in order to collect, on a voluntary basis, information from members of the public for inclusion in the COVID -19 Database. The function of this Database is essentially to surveil infected persons in order to identify whether they have come into contact with non-infected persons, thereby potentially spreading COVID-19.

In terms of these Regulations, the Director-General of Health may, in writing, appoint any organ of State outside the Department of Health or private entities to provide services necessary for the carrying out of his or her powers and functions under this Regulation. Importantly information stored by the appointed entities or transferred to or from the appointed entities must be in an encrypted form, save where this is not possible in achieving the purposes of this regulation, and access must be subject to password protection. There is an understanding that sensitive information, such as health and location data must be protected via sufficient technological means.

Additionally, the Regulations create a number of security processes that must be adhered to during the course of the pandemic and thereafter. These include logging details pertaining to access made to data contained in the Database, the prohibition of retaining information, as a third party, derived from the Database either in original or duplicate form and the implementation of password protection measures.

#### 3.2.3.5. **Zambia**

Two Statutory Instruments have been issued in response to the COVID-19 pandemic in Zambia. The first, No. 21 of 2020, declared COVID-19 as a "notifiable infectious disease" in line with Section 9 of the Public Health Act. The second, No. 22 of 2020, set out measures aimed at controlling the spread of COVID-19. <u>Statutory Instrument No 22 of 2020</u>, provides for quarantine measures for possible infected persons. However, these Statutory Instruments do not make provision for a surveillance or monitoring of infected persons outside of quarantine.

The <u>Public Health Act</u> of originally of 1930 but subsequently consolidated and amended, under Section 30 empowers the Minister of Health, to establish through Statutory Instruments, mechanisms to ensure the removal of persons who are suffering from an infectious disease and

persons who have been in contact with such persons and more generally, for any other purpose, whether of the same kind or nature as the foregoing or not, having for its object the prevention, control or suppression of infectious diseases. From the aforementioned, the Minister of Health is enabled to install a system of surveillance of infected persons as a measure to prevent, control or suppress COVID-19 in Zambia.

#### 3.2.3.6. **Zimbabwe**

Whilst not enacted during the COVID-19 pandemic, the <u>Public Health Act</u>, specifically Section 35, empowers the Minister of Health to surveil persons suffering or suspected to be suffering from infectious diseases who are not quarantine or in hospital, the premises in which such persons are accommodated, those in charge of or in attendance on such persons, and other persons living in or visiting such premises or who may otherwise have been exposed to the infection of any such disease

#### 3.3. General Observations

#### 3.3.1. Expressly online databases for contact tracing

Only South Africa has established an expressly online database for COVID-19 tracking and tracing purposes. Where other countries gather sensitive information for the purpose of monitoring the virus, no further details pertaining to storage, access, deletion and so forth are provided in the corresponding laws.

This is <u>arguably</u> an issue that existed prior to the COVID-19 pandemic. Problem areas such as inadequate oversight by authorities and the lack of technical safeguards have been identified in the majority of the countries forming part of this Report. The concerns pertaining to unauthorised access, loss of data, and data misuse exist during the pandemic. However there is no indication what the process will be post pandemic.

Importantly, COVID-19 contact tracing and surveillance systems and databases, according to <u>CIPESA</u>, have "been affected in haste, and with limited precedent and oversight mechanisms".

Despite the focus on health information no country, but for South Africa, has included encryption or other security safeguards surrounding the storage, processing or accessing of health information. South Africa was the only country in this Report which provided very specific information pertaining to the use of technical safeguards such as encryption as it pertained to online contact tracing databases.

## 3.3.2. Communications, internet and telecommunications services classified as "essential"

In most of the select African countries forming this Report, essential services, which are allowed to operate during a national lock down, include those related to communication and telecommunication services. The positive impact thereof is that the propensity for disruption is lower.

#### 3.3.3. Impact on the digital divide

The <u>digital divide</u> is a term used to describe unequal access to or distribution of technology such as mobile phones, personal computers and the Internet. This is a global issue, however, its impact is acutely observable on the African continent.

In Zimbabwe, the Government instituted a State of Disaster which specifically applied to both urban and rural sections of the country, as a whole. With the distinction and specificity, no further information was provided to address how areas which fall under either urban or rural would be assisted and supported in terms of allowing access to an Internet and internet services that were secure.

#### 3.4. Analysis of Impact of Regulations

## 3.4.1. Regulations impacting the right to benefit from security, stability and resilience of the Internet

#### 3.4.1.1. **Angola**

The Communication Strategy does not make mention as to whether the internet infrastructure or security on the Internet will be managed during the pandemic. In fact, no mention of the infrastructure that these proposed means of communication operate on, was addressed.

The concern that this raises is that whilst social media support will be provided, the actual stability and security of internet services is not guaranteed. This Strategy disinvests the Government from maintaining its own communication services as it places a large reliance on existing platforms, all of which are based in foreign jurisdictions and thus susceptible to controls that do not fall under the Government's mandate or its own controls.

For this reason, this Strategy, whilst not a law, may have a negative impact on the individual's right to a secure and stable Internet as the means of accessing said Internet are not within the control of the Government.

#### 3.4.1.2. **Malawi**

By declaring communication, navigation and surveillance system services, through the <u>Public Health (Coronavirus Containment and Management) Rules 2020</u>, as essential during a period of limitations on freedoms, the Malawian Government strengthened the right for Malawians to benefit from a secure and stable Internet and internet infrastructure as allowing those services who support this right to operate regardless of restrictions lessens the propensity for technical or other issues from infringing on the benefits the right provides.

#### 3.4.1.3. South Africa

The Directions of 26 March 2020, are an example of possible positive impact that regulations promulgated as a response to the COVID-19 pandemic may have on Key Principle 9. These Directions specifically obligate service providers to ensure continuance of communication services despite the pandemic. In addition thereto, the Directions of 29 April 2020, established that information and communication technology services and those services required to support them, were "essential" and thus allowed to operate more freely.

SouthAfrican citizens were able to access an Internet and associated services that were maintained and secure as they had continued attention from those public and private entities which serviced them. In practice this meant that the propensity for internet disruption, due to technical reasons, was low, any security breaches or concerns could be addressed and the overall stability of the Internet in South Africa was preserved.

#### 3.4.1.4. **Zimbabwe**

By declaring a State of Disaster for, specifically, both urban and rural areas extends the protections as well as the limitations on freedoms that come with this declaration. In terms of the right to benefit from a secure and stable Internet, there will be a discrepancy on how this is enjoyed between rural and urban areas. The potential impact is that rural and urban areas will be treated similarly and thus those in rural areas, due to the digital divide, will not have full benefit of the Internet.

3.4.2. Regulations impacting the continued cooperation between stakeholders in order to ensure effectiveness in addressing risks and threats to security and stability of the Internet.

#### 3.4.2.1. South Africa

The <u>Directions On Zero-rating Of Websites For Education And Health Issued Under Regulation</u> 4(10) Of The Regulations Made Under The Disaster Management Act, 2002 (Act No. 57 Of 2002) provide a framework for the zero-rating of websites subject to approval by the National Department of Basic Education. These include websites of educational institutions, local websites offering free access to educational content resources Department of Basic Education and Provincial Education Departments' websites or portals, all COVID-19 related websites identified by the Department of Health, and local websites offering free access to COVID -19 health content resources.

Furthermore, the Department Of Communications And Digital Technologies has provided technical parameters which need to be complied with prior to a website being zero-rated. These include: websites with missing technical information required by network operators for zero-rating, such as SNI (Server Name Identification), will not be zero-rated. The site owner or administrator must provide the network operator with default login details in order to facilitate zero-rating for websites that need to be zero-rated and are using login authentication.

#### 3.4.2.2. **Zimbabwe**

The <u>Statutory Instruments 83 of 2020</u>, specifically, Section 2, provides a list of "essential services". Included in this list are "communications and telecommunication services, including the Internet". Section 4 of the same Statutory Instrument states every other business establishment shall be closed except for every business establishment providing an essential service or services in support of such a service. The effect of this is that during the national lockdown, essential services and those supporting said services may continue to operate as well as being granted other allowances such less restricted travel obligations. As such, during the pandemic, the continued operation of the Internet and communication services can be guaranteed, as much as possible, as those responsible for its upkeep and operation are provided the necessary freedoms to operate effectively.

3.4.3. Regulations impacting surveillance, monitoring and interception of users' online communications by state or non-state actors

#### 3.4.3.1. **Angola**

Articles 10 and 11 of the <u>Presidential Decree No. 142/20 of 25 May 2020</u> create the foundation of a contact tracing and infection surveillance system. That is to say, a system where notification of infection to health authorities and a system of searching and monitoring people who have become exposed to COVID-19. However, the Angolan Government has not provided details pertaining to how this information will be stored, used, accessed or deleted. The potential risk that this creates is that this system may fall victim to abuse or negligence and thus undermine a persons right to be protected against unlawful surveillance or monitoring should that data be stored online or accessed via the Internet.

However, the mitigating factor to the above is that the Angolan Constitution is robust and specifically protects people from unauthorised access by state actors to private communications. This Article of the Constitution should provide the vehicle against which any track and trace surveillance system can be criticised.

#### 3.4.4. **Malawi**

The <u>Public Health (CORONA VIRUS PREVENTION, CONTAINMENT AND MANAGEMENT)</u> Rules, 2020 do not indicate whether this data is used for monitoring purposes directly nor any further details on how it is stored, transmitted or accessed. The possible impact that this law may have on Principle 9 is that it may give to a system which allows public authorities to monitor and surveil persons infected with COVID-19 without proper oversight. Additionally, no technical information pertaining to how the data is protected is provided and thus it is not possible to determine whether safeguards such as encryption will be utilised.

#### 3.4.5. **Mauritius**

The inference is that the Mauritian Government intends to create a contact tracing database in order to determine the possible spread of COVID-19. The Act does not state how this information is gathered or whether electronic means will be used to monitor the movement of infected persons or possible contact with other people. Therefore, it is not determinable whether this provision will have effect on Principle 9 of the AFDEC. However, it is important to note that in the absence of directions, the propensity for mismanagement and misapplication rises. That is to say that if appropriate rules are established when such a system is created, issues such as unauthorized access and misuse of information may be protected against.

#### 3.4.6. **South Africa**

The South African National Department of Health has created a contact track and trace COVID-19 database. The purpose of this database is to enable the tracking of individuals who are or reasonably suspected to have come into contact with someone who has or is reasonably suspected to be infected with COVID-19.

On the whole, the system is comparatively speaking, a good example of government taking the necessary steps to ensure that its people are not victims of unauthorised or unlawful surveillance. In this particular instance, the laws that give rise to the Database cater for a number of security and personal data protection protocols such as encryption and user access logs.

#### 3.4.7. **Zambia**

The Zambian Statutory Instruments do not make provision for a surveillance or monitoring of infected persons outside of quarantine.

However, the <u>Public Health Act</u> empowers the Minister of Health, to establish through Statutory Instruments, mechanisms to ensure the removal of persons who are suffering from an infectious disease and persons who have been in contact with such persons and more generally, for any other purpose, whether of the same kind or nature as the foregoing or not, having for its object the prevention, control or suppression of infectious diseases. From the aforementioned, the Minister of Health is enabled to install a system of surveillance of infected persons as a measure to prevent, control or suppress COVID-19 in Zambia. Without proper controls pertaining to security and monitoring, the introduction of a system that monitors, especially in a public health crisis, can pose a serious threat to the right that peoples must be protected from unlawful surveillance and monitoring.

#### 3.4.8. **Zimbabwe**

Whilst not enacted during the COVID-19 pandemic, the <u>Public Health Act</u>, empowers the Minister of Health to surveil persons suffering or suspected to be suffering from infectious diseases and those who have come into contact with them. Similar to other jurisdictions, without the implementation of the necessary oversight structures, security safeguards and transparency, a system that surveils and monitors individuals may have a negative impact on the right to be protected from surveillance and monitoring that is unlawful.

# FREEDOM OF ASSEMBLY AND ASSOCIATION AND THE INTERNET

## 4. IMPACT OF REGULATIONS ON FREEDOM OF ASSEMBLY AND ASSOCIATION AND THE INTERNET

#### 4.1. Introduction

Key Principle 5 of the Declaration states:

"Everyone has the right to use the Internet and digital technologies in relation to freedom of assembly and association, including through social networks and platforms.

No restrictions on usage of and access to the Internet and digital technologies in relation to the right to freedom of assembly and association may be imposed unless the restriction is prescribed by law, pursues a legitimate aim as expressly listed under international human rights law (as specified in Principle 3 of this Declaration) and is necessary and proportionate in pursuance of a legitimate aim".

Principle 3 provides that the right should only be limited under a legitimate aim expressly 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 where such limitations are necessary and proportionate in pursuance of a legitimate aim.

#### 4.2. Relevant Regulations

#### 4.2.1. **Angola**

Angola enacted <u>Presidential Decree No. 81/20</u> on 25 March 2020 under which a State of Emergency was declared. Under <u>Presidential Decree 82/20</u>, Article 3 placed restrictions on the freedom of movement of persons in Angola (subject to exceptions provided in Article 3(2)), whilst under Article 20, political events and activities, and meetings and events that involve the concentration of more than 50 people were prohibited.

The State of Emergency ceased on 25 May 2020 and was succeeded by <u>Presidential Decree No. 142/20</u> in terms of which a State of Public Calamity was declared. Article 9 thereunder prohibited travel to the Capital of Luanda from other provinces with exception to obtaining or delivering essential services or the movement of patients. Article 27 prohibits public gatherings that are not for business or work purposes. Workplaces are restricted to 50% capacity with a maximum of 150 people allowed in any one place.

The <u>National Contingency Plan for the Control of the COVID19 Epidemic Communication</u>

<u>Strategy</u> which was instituted by the Ministry of Social Communication laid out Angola's plans to combat COVID-19 through the promotion and dissemination of information.

As part of the Communication Strategy, the Ministry provides for two separate communication techniques, internal and external communication. The former addresses standard communication techniques from within companies and State organs such as emails, circulars, letters and meetings. The latter addresses all other forms of communication external to a company or State organ and includes advertising, press briefings and social networks.

The Communication Strategy does not prohibit or disband any form of online assembly, however it does acknowledge that the dissemination of disinformation is a threat to the effective containment of the COVID-19.

Under the Contingency Plan, the Ministry established a Twitter page, Coronavirus Response Portal and multiple WhatsApp groups to encourage the spread of information. The Ministry's existing Facebook page is also regularly updated.

#### 4.2.2. **Malawi**

The Malawian government declared a national lockdown in terms of Section 11 of the <u>Public Health</u> (Coronavirus Prevention, Containment and Management) Rules, 2020. Under Rule 12 of the Rules, a prohibition against public gatherings in excess of 10 people was introduced. However, the Rules have not impacted on the use of the internet or digital technologies with regard to the freedom of assembly and association online.

Malawi underwent a round of presidential elections on 23 June 2020, which were originally postponed from 19 May 2020 over concerns of COVID-19.. The Rules are no longer valid under the new administration of President Lazarus Chakwera.

#### 4.2.3. **Mauritius**

Mauritius declared a nationwide lockdown on 20 March 2020 in terms of the <u>Prevention and Mitigation of Infectious Disease (Coronavirus) Regulations, 2020</u>. The lockdown saw strict limitations on all movement of people and the implementation of a curfew. Mauritians were only allowed to leave their homes in cases of emergency. Regulation 13 empowered the Minister to designate restricted areas which could not be accessed by anyone without prior approval.

This strict national lockdown was reduced in severity on 31 May 2020, allowing selected businesses to open and workers could travel without a permit while citizens could move freely for leisure. On 15 June 2020 the national lockdown was ended completely and Mauritius resumed normal operations, however international borders remain closed.

The strict lockdown did not affect the access to and use of the internet and digital technologies with regard to freedom of assembly and association. There has been no impact on the right by the COVID-19 Regulations. Mauritians are free to form, join and associate with online communities and groups.

#### 4.2.4. **South Africa**

A national lockdown was declared under the <u>Disaster Management Act Regulations</u>, 2020. Regulation 23 which prohibited all public gatherings has since been amended by <u>Regulation 4</u> of the <u>Amended Regulations</u> (25 June 2020). The Amended Regulations maintain a prohibition on all public gatherings with noteworthy exceptions including:

- Council and local government hearings, provided that such gatherings are restricted to allow for proper social distancing.
- Business conferences or meetings, provided such gatherings are limited to 50 people. This limitation does not apply for online attendees.
- Leisure activities including cinemas, theatres, sporting events, self care services and casinos provided that these events are limited to 50 people.

On 26 March 2020 The Department of Telecommunications and Postal Services passed the <u>Electronic Communications</u>, <u>Postal and Broadcasting Directions</u> under the Disaster Management Act Regulations, 2020. The Directions ensure that information and communication technologies are made available for use in combating COVID-19. Direction 2 states and includes "access to communications infrastructure and digital services."

Direction 4 states that the Directions shall among other things, ensure the smooth operation of the electronic communications industry as essential services during the State of natural disaster, and create an enabling licence environment for the rapid deployment of electronic communications infrastructure and services.

Direction 6.1 provides that all electronic communications service networks and providers must ensure the continued provision of services, whilst Direction 6.10 empowers the Regulator to temporarily assign a high demand spectrum to licensees that are capable of expeditious implementation.

#### 4.2.5. **Zambia**

The <u>Public Health (Infected Areas) (Coronavirus Disease 2019) Regulations, 2020</u> passed under the Public Health Act empowers the Ministry of Health to designate infected areas. Regulation 5 provides that no one may enter or exit an infected area without permission of the Ministry of Health or the local authority. Whilst Regulation 9 initially prohibited gatherings of over five persons who are not family in designated infected areas, this restriction was eased on 8 May 2020 to prohibit gatherings of more than fifty people.

#### 4.2.6. **Zimbabwe**

The <u>Public Health (COVID-19 Prevention, Containment and Treatment)</u> (National Lockdown <u>Order), 2020 (Statutory Instrument 83/20)</u> was adopted on 23 March 2020. Thereunder, a national lockdown was declared under Section 4, which prohibits public gatherings over two people with the following exceptions:

- Gatherings at a stop point for public transport provided that no more than 50 people may be present at any such stop;
- Gatherings at a funeral service which is limited to 50 persons
- Individuals who are in a public transport vehicle;
- Gatherings at supermarkets for the purpose of purchasing necessities;
- Gatherings at hospitals for the purpose of obtaining medical treatment;
- Gatherings at pharmacies for the purpose of obtaining essential medication; and
- Gatherings for the purpose of obtaining an essential service.

Further, <u>Statutory Instrument 83/20</u> prohibits all interprovince and intercity travel that is not for the purpose of procuring or delivering an essential service. Statutory Instrument 83/20 was subsequently amended by <u>Statutory Instrument 136/2020</u> which amendments provided for the Parliament of Zimbabwe as an essential service, and for an exception to the two persons gathering restriction - public hearings organised by a Parliamentary portfolio committee - provided such gathering is limited to 50 people.

#### 4.3. **General Observations**

None of the countries expressly prohibit the use of or access to the internet or digital technologies in relation to the freedom of assembly or association online in any provision or acknowledge the right in their respective COVID-19 regulations. As a result this right has not been guaranteed or infringed upon.

Online protest action against the regulations and adopted measures has been witnessed in South Africa particularly in the form of Facebook groups and trending Twitter hashtags (Mail and Guardian, 2020). However the digital divide remains a significant barrier towards the realisation of freedom of assembly and association online (CIPESA et al, 2019).

All of the countries adopted a form of national lockdown in response to the COVID-19 pandemic and each of them limited the physical right to freedom of assembly and association in order to control the spread of the Coronavirus.

All of the lockdowns were imposed in terms of a national law serving a legitimate purpose, namely the protection of public health. The imposition of lockdowns has widely been <u>regarded</u> <u>by experts</u> as a necessary step in containing the spread of COVID-19 and protecting public health (World Health Organisation, 2020). However, the intensity of lockdowns has varied significantly between the various countries which leaves the assessment of the proportionality test open to debate.

The type of lockdowns implemented has also been varied. Zambia adopted a partial lockdown providing for the designation of infected areas, which allowed for free assembly outside of those areas. The most severe national lockdowns were Mauritius and Zimbabwe, however it is worth noting that Mauritius has managed to keep <u>daily confirmed cases under 5 since 11 April 2020</u> and has since opened the country to normal functionality, with the exception that <u>international borders remain closed</u> (African News, 2020).

The effect of restricting physical freedom of assembly and association in the context of a participatory democracy has been significant in Malawi and Zimbabwe. Malawi postponed general elections in terms of the lockdown which resulted in <u>significant protests</u> across the country ultimately culminating in the rerun of the elections on 23 June 2020 and the election of President Lazarus Chakwera (All Africa, 2020). Zimbabwe prohibited the movement of persons across interprovincial and intercity borders, however parliamentary portfolio committee meetings continued under lockdown, including <u>hearings towards amending the Constitution</u> (All Africa, 2020).

Angola and South Africa were the only countries who explicitly made reference to online platforms, digital services and infrastructure providing for the establishment and increased penetration of these services and infrastructure.

#### 4.4. Analysis of Impact of Regulations

Although none of the countries expressly prohibited access to or the use of the internet or digital technologies, it would have been contentious to use social media, the internet or other communications services to promote, organise or encourage a physical assembly of any nature in any of the examined countries for the duration of their respective lockdowns.

All of the countries have limited the physical right to freedom of expression and association. All of these limitations have been necessary and lawful in terms of their purpose and enabling legislation. However, the test for proportionality is more vague owing to the varying levels of severity among the various countries lockdown measures.

In order to provide an understanding of how to apply the proportionality test, the <u>African Charter</u> on <u>Human and Peoples Rights</u> provides under Part 1 subsection (g):

"The principle of proportionality for the purpose of the guidelines (contained in the Charter) involves striking a fair balance between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights".

In applying the test, the results can vary depending on the importance of the right, the severity of the restriction and the necessity of the restriction.

Angola could be said to have passed the proportionality test as the demand for public health is vital especially amid the pandemic. The original national lockdown established in terms of the State of Emergency declared under Presidential Decree No. 81/20 was severe. When the extended State of Emergency lapsed on 25 May 2020 it was replaced by a partial less severe lockdown of the capital Luanda only under Presidential Decree 142/20.

Mauritius could also be said to have passed the proportionality test despite having a lockdown that was among the strictest of all the examined countries. Mauritius' strict lockdown resulted in a swift reduction in positive cases and has since allowed the country to emerge from lockdown and resume normal functions (VoxEu, 2020). It is noteworthy that Mauritius is the one of only two African countries to meet and exceed the <u>Broadband Commission's target for the cost of internet at 2% of GNI per capita</u>, making internet access in Mauritius more accessible than all other examined countries (IT Web, 2020). A more affordable internet may result in more Mauritians forming, joining and associating with online communities.

By comparison, Zimbabwe could be said to have failed the proportionality test as the national lockdown and restriction on movement and assembly was severe. The country has not faced

widespread coronavirus cases with just over 700 confirmed cases and 9 deaths. The further political implications for restricting freedom of assembly and association is limiting citizen participation in the <u>Parliamentary hearings on the controversial Constitutional Amendment Bill</u> which should weigh heavily against the assessment of proportionality (AllAfrica, 2020).

Although not expressly provided for, the Malawian Public Health (Coronavirus Prevention Containment and Management) Rules, 2020 could provide for the promotion of the use and access to online services. Section 11 empowers the Minister of Health to declare a lockdown in Malawi in order to prevent, contain and manage the virus. Section 11(2) mandates the form that any lockdown declared in terms of the Section should take and Section 11(2)(e) provides that access to essential services must be provided for for the duration of the lockdown. The Schedule to the Regulations establishes the forms of essential services and includes "information and communication" which is further defined as "communication and media services on screen, TV, radio, print, broadcast and online".

When read together with the Schedule, it is clear that access to the internet for both information and communication is protected under any COVID-19 lockdown.

The freedom to form, join and associate with online communities has not been expressly limited by any of the regulations as set out in the above Sections. However it is noteworthy that Zimbabwe under Section 14 of Statutory Instrument 83/20 and South Africa under the Disaster Management Act Regulations of 18 March 2020, both prohibit the publication of false or misleading statements regarding COVID-19. Zimbabwe goes as far as to criminalise false statements regarding a public official performing any function associated with the COVID-19 lockdown. Associating with any online group, social network or similar platform making such statements could result in criminal sanction which negatively impacts the freedom of assembly and association online (CIPESA, 2020).

## RIGHT TO DUE PROCESS

#### 5. IMPACT OF REGULATIONS ON RIGHT TO DUE PROCESS

#### 51 Introduction

The right to due process has been declared by the AFDEC as a key principle for the substantive transformation of Africa. This Principle states that:

"Everyone has the right to due process in relation to any legal claims or violations of the law regarding the Internet.

Standards of liability, including defences in civil or criminal cases, should take into account the overall public interest in protecting both the expression and the forum in which it is made; for example, the fact that the Internet operates as a sphere for public expression and dialogue"

In practice, and as the AFDEC principle alludes to, this right encompasses three central themes of governance:

- how and when a person is arrested or detained;
- do people have full access to courts; and
- do people have a guarantee of a lawfully and procedurally fair trial.

Should due process be infringed by any regulation, international standards require that the limitation be based on a legitimate aim, necessity, and proportionality. To this end, the following analysis will evaluate the right to due process in relation to the regulations enacted alternatively relied upon as a direct result of the COVID-19 pandemic.

#### 5.2. Relevant Regulations

#### 5.2.1. **Malawi**

Section 46 of <u>The Disaster Preparedness and Relief Act 1992</u> establishes the penalties for non-compliance with the remaining sections of the Act. The offender is described as, "any person, without lawful excuse...". This can be read in conjunction with the Constitution of Malawi's Article 43 Right to Administrative Justice, which affords lawful and procedurally fair administrative action in all cases of prospective regulatory violation (section 43). Moreover, the <u>Public Health (Coronavirus Containment and Management) Rules 2020</u>, which were enacted to give effect to the <u>Disaster Preparedness and Relief Act 1992</u> during the COVID-19 pandemic give further guidance on exercising this right. Section 18 of the Rule, dealing with Judicial

Proceedings, states that litigants will still have access to courts albeit through electronic means. If it is absolutely vital that the case be heard in a physical court or chambers, then provisions have been made to facilitate this subject to sanitary and hygiene requirements.

#### 5.2.2. **South Africa**

The <u>Constitution of the Republic of South Africa</u> establishes a number of rights which affect due process including Section 33 (Just administrative Action), Section 34 (Access to Courts), and Section 35 (Arrested Persons). The <u>Disaster Management Act 2002</u>, which gives effect to these Constitutional rights during a national emergency, states under Section 59 that any death, bodily injury or disablement that is a result of any regulation directed during the national emergency, will be entitled to compensation. Section 59 (2) then goes on to list the processes of claiming said entitlement. However, the condition is that the infringement has to have occurred in the State's performance of a Directive prescribed during the national emergency (Section 59 (1)(b)).

For general access to recourse, including violations on the internet, the <u>Directives Issued by Chief Justice Mogoeng Mogoeng in Terms of Section 8.3 b of The Superior Courts Act 10 of 2013 for the Management of Courts During the Lockdown Period impacts due processes exercisable. The Directive states that only urgent applications and urgent matters arising from the activities associated with disaster management may be heard in open court during the lockdown period, provided that the judge or magistrate may, if he or she deems it necessary, hear any such matter through video conferencing or other electronic means, after consultation with the parties concerned (Section 3).</u>

#### 5.2.3. **Mauritius**

The <u>Quarantine Act</u>, which was promulgated on the 16<sup>th</sup> of May 2020, directly impacts the right to due process as set out in Articles 10 and 17 of the <u>Constitution of Mauritius</u> as well as the right to due process as per the AFDEC. Under Section 11 of the Act, police are extended broad discretionary powers to enter premises and arrest a person without a warrant on grounds of reasonable suspicion of a violation. Moreover, Section 12 of the Act states that any resist, insult, or obstruction of said arrest will result in a further fine and/or imprisonment. Identically, the <u>Prevention and Mitigation of Infectious Disease (Coronavirus) Regulations 2020</u> extends the same discretionary powers to police officers. Section 12 affords officers the right to enter premises and arrest any person without a warrant, and Section 19 imposes penalties for any resistance to the arrest. Both Acts make no express mention of the right to recourse.

In terms of access to courts, the <u>COVID-19</u> (<u>Miscellaneous Provisions</u>) Act amended the <u>Court Act</u> to include Section 197H on practices and procedures to be upheld before any court during the COVID-19 pandemic period. Subsection 2(b) gives courts the option of hearing cases via telephone or other electronic means that the Chief Justice may deem fit.

#### 5.2.4. **Zambia**

Section 3 (f) of the <u>Emergency Powers Act</u> establishes a broad entitlement to compensation should any person be affected by the implementation of the Act. However, under its application sections, detailing the processes for claiming the compensation, any reference to compensation is expressly in relation to land or property possessed or acquired by the State during the period. The <u>Public Health (Coronavirus19) Regulations</u>, which was enacted on the 13<sup>th</sup> of March 2020 to address COVID-19 measures, allows for police to just enter premises and "search for a case of Covid-19" (Section 7). The Constitution affords rights to due process under Section 28 (Just Administrative Action), 18 (Access to Courts), and 25 (Arrested Persons).

#### 5.2.5. **Zimbabwe**

In matters of business operations, the <u>Statutory Instrument No. 99 of 2020 - the Public Health</u> (COVID-19 Prevention, Containment and Treatment) (National Lockdown) (Amendment) Order, <u>2020 (No. 5)</u>, adds a burden of proof to an accused's claim. Section 11F (5) states that businesses deemed "formal" may open after 08h00, which can also include those providing online services. Those that are deemed not "formal" are to remain closed. The potential impact on due process can be found under Subsection (6) which then adds the burden of motivating to an enforcement officer as to why a particular business is to be considered "formal".

In general, to address the COVID-19 pandemic the Government of Zimbabwe has enacted the following regulations: the Statutory Instrument 76 of 2020; the Statutory Instrument 82 of 2020; and the Statutory Instrument 83 of 2020. However, none of these in fact address affording due process regarding or resulting from internet activities, directly. The only mention made with regard to court processes is found under the penalty provisions (Sections 11 and 14). Section 11 of the Statutory Instrument 83 of 2020, refers to a fine and possible imprisonment for "obstructing or hindering" a police officer in the enforcement of the Regulation. Section 14 establishes the liability for disseminating misinformation is prosecution under Section 31 of the Criminal Law Code.

Conversely, the <u>Constitution of Zimbabwe</u> sets out detailed provisions on the right to administrative justice (Section 68), a fair hearing (Section 69), and the rights of the accused

(Section 70). Moreover, the Constitution underpins the <u>Access to Information and Protection of Privacy Act</u>, 2003, which explicitly affords access to the Administrative Court for cases that encompass potential internet and media violations under Section 90A.

#### 5.2.6. **Angola**

Article 29 of the Angolan Constitution, not only entitles its subject to fair processes, but goes further to require that laws enacted in effect of the Constitution's mandate clearly outline and define adequate protections for the "secrecy of legal proceedings".

The National Contingency Plan for the Control of COVID-19 establishes how the State will utilize the dissemination of information to combat COVID-19. However, the Plan makes no mention of the legal recourse available if violations occur. The Communication Strategy indicates how the government will disseminate information on the pandemic through internal and external communication mediums, including social media. Similar to the National Contingency Plan for the Control of the COVID-19, the Communication Strategy does not outline how the information will be handled nor what constitutes mishandling of said information. Importantly, it does not set out the remedies for any infringement nor rights of recourse in this event.

#### 5.3. **General Observations**

#### 5.3.1. Addressing the three Due Process Themes

Of the selected African countries, only two (2) countries (Malawi and South Africa) have enacted regulations protecting the right to due process. However, only one (1), Malawi, addresses all three themes related to due process: arrests; access to courts; and the guarantee of a lawful and procedurally fair trial. Although all the selected African countries' Constitutions envision some form of public interest element, none of the regulations expressly addressed this as either a founding value of their implementation or a consideration in penalising violations.

#### 5.3.2. Sanctions: The Appropriate Standard of Liability

Of the selected African countries, regulations in four (4) countries (Mauritius, Zambia, Zimbabwe, and Angola) did not protect the right to due process. In three (3) countries (Mauritius, Zambia, Zimbabwe) of these four (4), there is mention made with regard to court processes found under the penalty provisions of the regulations. Although the fines varied, the general imprisonment penalty was consistently between 1 – 2 years across all countries. A Zimbabwean regulation

reverts liability for disseminating misinformation and the prosecution thereof to the country's Criminal Law Code.

#### 5.3.3. Coping with Dispute Resolution Alternatives

Generally, access to courts has been limited to telephonic and electronic hearings. Mauritius and South Africa have had to amend their respective laws governing court procedures in order to achieve this. The police have been afforded broad discretionary powers to enter premises and arrest a person without a warrant on grounds of reasonable suspicion of a violation.

#### 5.4. Analysis of Impact of Regulations

#### 5.4.1. Addressing the Three Due Process Themes

The practical importance of a public interest consideration in implementing arrests, access to courts and lawful trials has already been seen in Zimbabwe. There, without public interest guiding the enforcement efforts, reports have indicated how the State has used the regulations to stifle free speech.

Just as there is a legitimate expectation for a country's Constitution to underpin public Interest in its mandate, regulations governing a vital right such as that of due process also carry this expectation. Moreover, if the law pertains to the limitation of internet activities, a space where a large population in Africa is already disadvantaged, there is a greater call for regulations that consider public interest.

To this end, the AFDEC COVID-19 Position Paper recommends that "States should safeguard the right to due process in all forms while taking measures to address the COVID-19 pandemic, and any restrictions should comply strictly with the three-part test for a justifiable limitation" (AFDEC. pg 10). The Paper further suggests that without this public interest consideration the regulation enacted in response to the COVID-19 pandemic would have failed to demonstrate the necessity element of limiting the right under international human rights law. In line with this approach, the UN High Commissioner for Human Rights encourages governments to inform the affected population of what the emergency measures are, where and how they apply and for how long they are intended to remain in effect and should update this information regularly and make it widely available.

#### 5.4.2. Sanctions: The Appropriate Standard of Liability

The determinant of the appropriateness of sanctions that limit the right to due process is proportionality. Proportionality is generally regarded as the last leg of a three-part test for a justifiable limitation. As discussed above, most of the selected countries would fail at the necessity stage (part 2) of the inquiry. However, an evaluation of the sanctions enforced by regulations during COVID-19 provides insights that can improve ongoing due diligence to determine the impact of regulations on the right.

In this regard, Zimbabwe provides a good example. Section 14 of the <u>Statutory Instrument 83 of 2020</u> states that the liability for disseminating misinformation is prosecution under Section 31 of the Criminal Law Code. The Section allows for imprisonment of up to twenty (20) years. As a bar, twenty years may seem excessive, especially considering that AFDEC's envisions "states responding to misinformation and disinformation relating to COVID-19 with approaches that promote transparency and media freedom, rather than relying on criminal sanctions." (AFDEC, pg 10).

International law implores the imposition of penalties as enforcement measures to be the last resort where alternatives have proven unsuccessful or if it becomes clear that the objective cannot be achieved by such other means (<u>UN</u>). While there is a need to curtail the spread of misinformation it is worrying that, in Zambia for example, ZICTA is reverting to a law that was invalidated by the courts (<u>MISA-ZIM</u>). Section 67 of Zambia's Penal Code outlawed the spreading of false information likely to cause fear and alarm. However, in the case of *Chipenzi vs The People*, a High Court found that the Section was unconstitutional. It is thus quite surprising that the ZICTA would allude to this Section of the Penal Code. Sufficient steps need to have been taken to make sure the public is aware of the reasons for the restrictions and the need to comply with them. States must also put in place measures for people to be able to comply with the restrictions, including by enabling them to satisfy their essential needs, and take into account the situation of marginalized groups who may require support in order to be in a position to comply with the restrictions (<u>HRW</u>).

#### 5.4.3. Coping with Dispute Resolution Alternatives

As a measure to reduce contact amongst people, limiting court access to hearings held electronically or telephonically is justified. However, given the economic frailties, this fails as a practical solution in Africa. South Africa, which is one of the selected countries, is one of the few African countries with over half the population online (RIA). The inevitable result is that the

regulation will only benefit the wealthy. This discriminatory element directly opposed the ideals of the AFDEC set to empower African people.

The other common theme that we note is the broad discretionary powers afforded police officers. Mauritius' Public Health (Coronavirus19) Regulations, allows for police to just enter premises and "search for a case of Covid-19" (section 7). The ambiguousness of the provision, especially without any other provision expanding on it, can be abused to infringe a person's right to due process. If contact tracing is employed, then it means the State can track a person suspected of being infected by the virus, and the police can just detain the person – all without due safeguards, notification procedures and knowledge of the person. Kaye, a UN Special Rapporteur on freedom of expression, has cautioned against such ambiguous provisions because they essentially allow enforcement to make public interest decisions based on political motives (Kaye).

In Zambia, Lusaka Province Minister Bowman Lusambo was reported to have threatened people with whipping if they did not respect the Presidential Directive, while police have been beating people with baton sticks on the streets. National police spokesperson Esther Katongo said in a television interview that police in Zambia had adopted a strategy to "hit and detain" anyone found on the streets. In Zimbabwe, police officers raided a vegetable market, forcing more than 300 vendors to flee and leave behind their produce. Police carried out the raid despite the agriculture sector being flagged as an "essential service" during the 21-day lockdown. They later disposed of the food, and vendors are yet to be compensated.

All decisions taken in response to the COVID-19 pandemic should be implemented in a transparent manner. South Africa is a good example as they have placed a Designated COVID-19 judicial authority who is "impartial and can enforce due process safeguards that are justifiable and compatible with international human rights law and standards" (AFDEC, pg 10).

RECOMMENDATIONS

#### **RECOMMENDATIONS**

Regulations to define the meaning and scope of what constitutes disinformation and misinformation and not stifle the right to hold and disseminate opinions and information unduly.

The implementation of misinformation laws and regulations, under the auspice of curbing misinformation pertaining to COVID-19, must not be used as a thinly veiled guise for governments to stifle freedom of expression that may be <u>critical of government actions</u> during and post the pandemic. That is to say that any limitation on the right to freedom of expression must only be effected within what is permitted by national and international standards (<u>Human Rights Watch. 2020</u>).

The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has <u>published</u> a report to the Human Rights Council on disease pandemics and freedom of opinion and expression. The report makes the following recommendations:

- Provide the public with accessible and understandable information pertaining to the crisis
- Allow the independent media to perform its function of providing information to the public.

  There should be as little government interference as possible;
- Provide the public with tools and understanding to mitigate the impact and spread of misinformation:
- Implement the necessary systems to track and trace the spread of the virus. However, said systems must not infringe on existing fundamental human rights nor should any information gathered by these systems be used for any other purpose but for tracking and tracing the impact and spread of the virus; and
- Maintain accountability to prevent any abuses of power and authority that were ostensibly made under the auspice of disaster management.

#### Overbearing, overly harsh or frivolous penalties to be avoided

Measures such as censorship or overbearing misinformation penalties that result in the limitation of the right to freedom of expression are to be avoided. Sanctions should <u>meet</u> existing national and international standards of necessity and proportionality. Importantly, "any attempts

to criminalize information relating to the pandemic may create distrust in institutional information, delay access to reliable information and have a chilling effect on freedom of expression".

Essentially, public bodies developing laws, regulations and policies, in response to the pandemic should be tested against national and international standards regarding the protection of freedom of expression.

### Data protection principles should be integrated into the processes of relevant authorities in the Selected African Countries

In the first instance, countries are to ensure that data collection and processing activities including those of government authorities are compliant with national data protection laws. As well as the rights contained in the AFDEC as it relates to privacy and personal data protection. Considering that many national data protection laws contain exceptions for the processing of personal data by governments (i.e for national security), it is important for national authorities to be clear on what obligations they have in law towards data subjects in their jurisdiction.

In addition to pre-existing national data protection laws, (or in some cases, in place thereof), authorities in the Selected African Countries should consider best practices in the context of a pandemic. On this note, the EFF has highlighted a number of safeguards that ought to be addressed when any public or private body wishes to implement a track and trace application, programme or database (the "EFF Data Protection Safeguards") which in turn strengthen the affected individuals right to privacy and personal data protection especially in light of a public health crisis. These safeguards may be summarised as follows:

#### 1. Consent

individuals must p[rovided informed, voluntary, and opt-in consent

#### 2. Minimisation

- The least possible information must be collected.
- Information must be retained for the least possible amount of time.
- All data that is no longer relevant must be automatically deleted.
- Information must be collected solely for the purpose of contact tracing

#### 3. Information Security

International best practices in terms of information security must be applied

#### 4. Addressing Bias

Do not directly or indirectly leave out marginalized groups.

#### Regulatory restrictions on service providers with access to personal data

Other best practices have been highlighted for mobile network operators who are, under certain Regulations, required to provide government authorities with the location data of persons. Some of these best practices include (GSMA, 2020):

- Being transparent with the public about the sharing of their data with government authorities (unless prohibited by law);
- Prohibiting the re-identification of individuals;
- Only sharing metadata with government authorities where it is lawful to do so; and
- Seeking assurances from government authorities concerning their processing practices and accountability mechanisms..

#### Providing for the expiration of track and trace systems and personal data access

When the purpose for the system is no longer applicable, in this case, when the threats posed by the COVID-19 pandemic are mitigated, systems built to track and trace the spread of the virus must be decommissioned and provisions for the expiry of rights to process the personal data contained in such systems must be provided for.

#### Privacy-centric technologies should be utilised, where possible

Whilst not always available or accessible (especially in countries with lower levels of internet penetration, connectivity and smartphone adoption), the use of privacy-centric technologies to collect, process, store, distribute and retain personal data should be utilised where possible. In particular, the use of bluetooth proximity tracing technologies may be considered, which has been adopted by research groups in Singapore (TraceTogether), Cambridge (the Private Automated Contact Tracing (PACT) group) and in Europe (Chukwuma Muanya, 2020). Whilst bluetooth-based tracing applications are not without their flaws, the nature of their functionality is privacy enhancing in that "[a] smartphone regularly broadcasts a random string of characters that serves as a pseudonym to other phones using Bluetooth's low-energy specification for sending short bursts of data... [a]t the same time, it logs every 'chirp' it hears from other phones, as well as information about the signal strength to estimate how close they are." (Chukwuma Muanya, 2020).

#### Adopt Regulations on Security, Stability And Resilience of the Internet

In order to ensure a secure and stable Internet, States must adopt the necessary Regulations that support both the maintenance and development of infrastructure as well as promote the adoption of security best practices. The purpose of which, with stakeholder cooperation is to allow individuals in said countries to benefit from an Internet that is robust and free from unlawful surveillance and monitoring,

#### ICT declared essential services in Regulations

During times of national lockdowns and many liberties are restricted, it is advisable that certain industries or sectors be declared "essential". In a number of jurisdictions, this is included in regulations enacted in conjunction with the COVID-19 associated national lockdowns. In such instances, information and communications technology service providers were expressly declared "essential". The result of which was that these services continued to operate and thus maintain the services and infrastructure that allowed for continued benefit of a safe and stable Internet despite the implementation of a national lockdown. This in turn affects the chances or internet disruptions and shutdowns. For this reason, it is advisable that the aforementioned services are expressly categorised as "essential" in order to operate effectively and without limitation as the impact of this limitation will in turn have a negative impact on the right to a secure and stable Internet.

#### Implementing COVID-19 data protection standards

Details pertaining to movement, infection status and possible physical contacts are being recorded in both offline and online databases. The purpose of these databases is to monitor and surveil individuals for the purpose of mitigating or analysing the spread of COVID-19. Some jurisdictions have provided for strict terms on how this information is to be used, who has access to it and what happens to this information post pandemic.

The Electronic Freedom Foundation (EFF) stated that "this crisis will end, but new tracking technologies tend to stick around" (EFF). This is a poignant reminder that systems that have been implemented to mitigate and manage a particular problem and in doing so infringe on fundamental rights, justifiably so, do not necessarily disappear when their use has expired. It is the nature of data and digital systems that they may be accessible after the fact.

The impact of such must be mitigated as much as possible by introducing and applying standards that pertain to the collection, use and deletion of personal information gathered under the auspice of disaster and emergency management.

In order to address the above, the following recommendations are made:

- When a system is introduced that has the propensity to disrupt or otherwise impact the right to a safe and secure Internet as as well as the protection against unlawful surveillance, said system must require the input, oversight and approval of the local data protection authority (ELI, 2020)
- The source code or other technical information on any such system, if managed through digital mediums, must be made available and disclosed to independent stakeholders in order to create a degree of third party review and auditing (Massé, 2020). This will dissuade the inclusion of any technical backdoors which would allow unregulated and possibly unlawful access.
- Any data that is collected during the COVID-19 pandemic for the purpose of lawful monitoring and surveillance, must be deleted or otherwise anonymised, permanently.
- Research and apply best practice security safeguards which can be applied to any system maintained on the Internet as a response to COVID-19. This may include decentralised protocols (Massé, 2020), encryption technology and security-by-design processes.

The above recommendations are applicable both during and post the pandemic period, as they incorporate best practices that if applied generally can bolster the right to benefit from a technical safe and secure Internet and related services.

It is important to read the above in conjunction with the recommendations made under the Privacy and Personal Data Protection section of this Report as surveillance is inextricably intertwined with privacy, and as such, the contents of the recommendations provided for under privacy and personal data protection should be given due consideration by the selected countries.

## Regulatory steps to improve regulatory responsiveness to a pandemic such as COVID-19

The Countries under study provide for the rights to freedom of assembly and freedom of association in their respective constitutions. A legal lacunae is the extension of such freedoms to the digital sphere. This is supported by the joint submission to the United Nations Special Rapporteur on the Right to Peaceful Assembly and of Association where CIPESA, the International Centre for Not for Profit Law and the Civil Society Reference Group recommends that existing laws should be strengthened to protect freedom of assembly and association in the digital age (CIPESA, ICNL & CSRG, 2019). The UN Human Rights Committee is revisiting the

regulation of assemblies. The European Union is developing a digital policy to improve the responsibilities of internet intermediaries. The opportunity for African Countries to advance the respect for digital rights including freedoms of assembly, association, expression online and free from state interference should not be missed.

## Measures to to assess and address disproportionate limitations on freedom of assembly and association online in Regulations

On the other hand and in the current times, there remains an opportunity to assess and redress the limitations to freedom of assembly and association online arising from Regulations in effect in the Countries. OHCHR released detailed <u>Guidelines</u> governments and law enforcement agencies that in the main pertain to the right to freedom of assembly in the traditional sense. However the OHCHR notes that during COVID-19 countries have also implemented response measures that limit access to the internet or information - and limitations on access to the internet or information including censorship measures have restricted freedom of assembly and association. Civil society in particular has faced several constraints. The <u>fifth Guideline</u> places emphasis on guarantees for freedom of association and assembly online recommends:

"The rights to freedom of peaceful assembly and of association apply online just as they do offline. In this time when physical assemblies are restricted, it is all the more necessary that access to and use of the internet be ensured. In addition to refraining from restrictions such as internet shutdowns or online censorship, States should take measures to ensure access to the internet extends to the entirety of the global population, and that it is affordable. In the context of civil society organizations specifically, States should ensure that they may complete their registrations online, and should provide opportunities for them to participate, via online fora, in policy development. In all cases, ensuring the rights to peaceful assembly and association online requires that individuals' rights to privacy are fully respected and protected."

#### Meaningful exercise of rights

- Selected African Countries should establish a designated Covid-19 judicial authority who can independently enforce due process safeguards, during the pandemic and for a reasonable period of time after, to ensure all violations and notifications are addressed.
- All actions and decisions should be transparently implemented. If the person is accused of violating an internet regulation, officials may request a court for enforcement, but only if: there is persuasive evidence, put in writing, and the subject is afforded the judicial chance to be provided a lawyer.

Selected African Countries should establish partnerships with community centres that can assist those without electronic devices or the means to meaningfully participate in a court hearing.

#### Regulatory amendments for express due process and recourse during and post the pandemic

- The Selected African Countries should consider best practices in the context of a pandemic. On this note, the following is a definitional suggestion by the UDHR which in Article 10 states that "everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him".
- Regulations should have express due process sections that outline how the process of enforcement; what constitutes violation of the regulation; as well as setting out the recourse available to subjects.
- Regulations should expressly encourage implementation of the regulations in line with public interest. Furthermore, public interest has to be developed by courts in the Selected African Countries as a founding value and construct an objective test by which can be collectively decided on, rather than an individualised formulation.

REFERENCES

#### **REFERENCES**

Abdu Rahman Alfa Shaban and Yasine Mohabuth (2020) Mauritius ends virus lockdown, beaches open, borders still closed accessed on 08 July 2020, available at

https://www.africanews.com/2020/06/15/mauritius-coronavirus-no-new-case-in-8-days-amid-lock down-extension/

African Charter on Human and Peoples Rights (1981) accessed on 08 July 2020, available at <a href="https://treaties.un.org/doc/Publication/UNTS/Volume%201520/volume-1520-I-26363-English.pdf">https://treaties.un.org/doc/Publication/UNTS/Volume%201520/volume-1520-I-26363-English.pdf</a>

African Declaration (2020) African Declaration on Internet Rights and Freedoms accessed on 08 July 2020, available at <a href="https://africaninternetrights.org/articles/">https://africaninternetrights.org/articles/</a>

African Declaration (2020) About the Initiative accessed on 08 July 2020, available at <a href="https://africaninternetrights.org/about/">https://africaninternetrights.org/about/</a>

African Declaration (2020) Position paper in Response to the Covid-19 Pandemic accessed on 08 July 2020, available at

https://africaninternetrights.org/wp-content/uploads/2020/06/AfDec\_COVID-19\_Position-paper\_E\_ng.pdf

All Africa (2020) How COVID-19 crisis united Malawians against Mutharika accessed on 08 July 2020, available at <a href="https://allafrica.com/stories/202006270271.html">https://allafrica.com/stories/202006270271.html</a>

All Africa (2020) Zimbabwe: Bill amendment hearings begin accessed on 08 July 2020, available at <a href="https://allafrica.com/stories/202006170171.html">https://allafrica.com/stories/202006170171.html</a>

All Africa (2020) Zimbabwe: stop mutilation of constitution accessed on 08 July 2020, available at <a href="https://allafrica.com/stories/202006220883.html">https://allafrica.com/stories/202006220883.html</a>

Alice Hazelton (2020) How to read the news like a scientist and avoid the COVID-19 infodemic accessed on 08 July 2020, available at

https://www.weforum.org/agenda/2020/03/how-to-avoid-covid-19-fake-news-coronavirus/

Ashwanee Budoo (2020) Controls to manage fake news in Africa are affecting freedom of expression accessed on 07 July 2020, available at

https://www.chr.up.ac.za/opinion-pieces/2084-controls-to-manage-fake-news-in-africa-are-affect ina-freedom-of-expression

Article 19 Viral lies: Misinformation and the Coronavirus accessed on 08 July 2020 available at https://www.article19.org/wp-content/uploads/2020/03/Coronavirus-final.pdf

BBC News (2020) Malawi presidential election:Polls close in historic re-run accessed on 08 July 2020, available at <a href="https://www.bbc.com/news/world-africa-53136963">https://www.bbc.com/news/world-africa-53136963</a>

Chipenzi and Others v The People (HPR/03/2014) ZMHC (3 December 2014) accessed on 08 July, available at <a href="https://zambialii.org/node/3585">https://zambialii.org/node/3585</a>

CIPESA (2020) Restrictions to freedom of assembly and association in Africa in the wake of COVID-19 accessed on 08 July 2020, available at <a href="https://cipesa.org/?wpfb\_dl=330">https://cipesa.org/?wpfb\_dl=330</a>

CIPESA. (2020) COVID-19 in Africa: When is surveillance necessary and proportionate?, accessed on 08 July 2020, available at

https://cipesa.org/2020/03/covid-19-in-africa-when-is-surveillance-necessary-and-proportionate

Civicus Concern as government punishes free expression accessed on 08 July 2020, <a href="https://monitor.civicus.org/updates/2020/06/30/concern-government-punishes-free-expression/">https://monitor.civicus.org/updates/2020/06/30/concern-government-punishes-free-expression/</a>

CNBC (2020) Coronavirus: Zambia situation report (2020) accessed on 08 July 2020, available at <a href="https://www.cnbcafrica.com/africa-press-office/2020/06/15/coronavirus-zambia-situation-report-152020/">https://www.cnbcafrica.com/africa-press-office/2020/06/15/coronavirus-zambia-situation-report-152020/</a>

Contact Tracing. Centers for Disease Control and Prevention. (2020). Retrieved 9 July 2020, from

https://www.cdc.gov/coronavirus/2019-ncov/php/open-america/contact-tracing-resources.html.

COVID-19 Occupational Health and Safety Measures in workplaces C19 OHS 2020 accessed on 08 July 2020 available at

https://www.gov.za/sites/default/files/gcis\_document/202004/43257gon479.pdf

Criminal Law (Codification and Reform) Act 23/2004 accessed 08 July 2020, available at https://zimlii.org/zw/legislation/num-act/2004/23/Criminal%20Law%20%28Codification%20and%20Reform%29%20Act%20%5BChapter%209-23%5D.pdf

Department of Communications and Digital Technologies (2020) Directions on zero-rating websites for education and health under Regulation 4(10) of the Regulations made under the Disaster Management Act 57 2002 accessed 08 July 2020, available at

https://www.gov.za/sites/default/files/gcis\_document/202006/43411gon651.pdf

Department of Health COVID-19 Online Resources and News Portal (2020) accessed on 08 July 2020, available at <a href="https://sacoronavirus.co.za/">https://sacoronavirus.co.za/</a>

Department of Justice and Constitutional Development (2020) COVID-19 Justice related Information accessed on 08 July 2020, available at <a href="https://www.justice.gov.za/">https://www.justice.gov.za/</a>

Disaster Management Act 57 20002 accessed on 08 July 2020, available at <a href="http://www.cogta.gov.za/cgta-2016/wp-content/uploads/2016/06/DISASTER-MANAGEMENT-ACT.pdf">http://www.cogta.gov.za/cgta-2016/wp-content/uploads/2016/06/DISASTER-MANAGEMENT-ACT.pdf</a>

Disaster Management Act, 2002 (Act No. 57 of 2002) Amended Regulations accessed on 08 July 2020 available at

https://www.iustice.gov.za/legislation/notices/2020/20200625-gg43476gon714\_Cogta.pdf

Electronic Communications, Postal and Broadcasting Regulations made under the Disaster Management Act, 2002 (Act No. 57 of 2002) Amended Regulations accessed on 08 July 2020 available at <a href="https://www.gov.za/sites/default/files/gcis\_document/202003/43164gon-417.pdf">https://www.gov.za/sites/default/files/gcis\_document/202003/43164gon-417.pdf</a>

Erica Penfold (2020) Has COVID-19 changed the narrative on press freedom in Africa? Accessed on 08 July 2020, available at

https://www.africaportal.org/features/has-covid-19-changed-narrative-press-freedom-africa/

EURACTIV (2020) UN Post-coronavirus world will be even more digital accessed on 08 July 2020, available at

https://www.euractiv.com/section/coronavirus/news/un-chief-post-coronavirus-world-will-be-even-more-digital/

GSMA COVID-19 Privacy Guidelines accessed on 08 July 2020, available at https://www.gsma.com/publicpolicy/wp-content/uploads/2020/04/The-GSMA-COVID-19-Privacy -Guidelines.pdf

Information and CommunicationTechnologies Act 44 2001 accessed on 08 July 2020, available at <a href="https://www.icta.mu/docs/laws/ict\_act.pdf">https://www.icta.mu/docs/laws/ict\_act.pdf</a>

INTERPOL (2020) Cybercriminals targeting critical healthcare institutions with ransomware, accessed on 08 July 2020, available at

https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

Lovina Sophie (2020) Fake news: Jahmeel Peerally arrested accessed on 7 July 2020, available at <a href="https://www.lexpress.mu/article/373277/fake-news-iahmeel-peerally-arrete">https://www.lexpress.mu/article/373277/fake-news-iahmeel-peerally-arrete</a>

Masse, E. (2020). Privacy and public health: the dos and don'ts for COVID-19 contact tracing apps - Access Now. Access Now. Retrieved 8 July 2020, available at:

https://www.accessnow.org/privacy-and-public-health-the-dos-and-donts-for-covid-19-contact-tracing-apps/.

Media Institute of Southern Africa (2020) COVID-19, fake news laws being used to stifle free speech accessed on 08 July 2020, available at <a href="https://zimbabwe.misa.org/2020/06/01/covid-19-fake-news-laws-being-used-to-stifle-free-speech/">https://zimbabwe.misa.org/2020/06/01/covid-19-fake-news-laws-being-used-to-stifle-free-speech/</a>

Michael Sean Pepper and Marietjie Botes (2020), Balancing privacy with public health during COVID-19: how well is South Africa doing?, accessed on 08 July 2020, available at <a href="https://www.up.ac.za/news/post\_2906497-analysis-balancing-privacy-with-public-health-during-covid-19-how-well-is-south-africa-doing">https://www.up.ac.za/news/post\_2906497-analysis-balancing-privacy-with-public-health-during-covid-19-how-well-is-south-africa-doing</a>

National Contingency Plan for Controlling Covid-19 (2020) accessed on 08 July 2020, available at <a href="https://www.masfamu.gov.ao/VerPublicacao.aspx?id=3928">https://www.masfamu.gov.ao/VerPublicacao.aspx?id=3928</a>

Penal Code Act Chapter 87 accessed on 08 July 2020, available at

http://www.parliament.gov.zm/sites/default/files/documents/acts/Penal%20Code%20Act.pdf

Public Health (Coronavirus Prevention, Management and Containment) Rules 2020 accessed on 08 July 2020 available at

https://www.manaonline.gov.mw/index.php/national/general/item/13931-public-health-corona-virus-prevention-containment-and-management-rules-2020

Presidential Decree no. 81/20, of 25 March accessed on 08 July 2020, available at <a href="https://cms.law/pt/prt/publication/meet-the-law-covid-19-state-of-emergency-in-angola-restrictive-measures-approved">https://cms.law/pt/prt/publication/meet-the-law-covid-19-state-of-emergency-in-angola-restrictive-measures-approved</a>

Prevention and Mitigation of Infectious Disease (Coronavirus) Regulations 2020 accessed on 08 July 2020, available at <a href="http://extwprlegsl.fao.org/docs/pdf/mat194896.pdf">http://extwprlegsl.fao.org/docs/pdf/mat194896.pdf</a>

Ramanand Jeeneea and Kaviraj Sharma Sukon 92020) The Mauritian response to COVid-19: rapid bold actions in the right direction accessed on 08 July 2020, available at <a href="https://voxeu.org/article/mauritian-response-covid-19">https://voxeu.org/article/mauritian-response-covid-19</a>

Regulation of Interception of Communications and Provision of Communications Act 70 2002 accessed on 08 July 2020, available at

https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13?gclid=EAlalQobChMlq86BzcvA6gIVA-ztCh0cuQavEAAYASAAEg Kh9vD\_BwE

Simnikiwe Mzekandaba (2020) Internet uptake lags despite falling broadband prices accessed on 08 July 2020, available at <a href="https://www.itweb.co.za/content/xnklOvzLAo3M4Ymz">https://www.itweb.co.za/content/xnklOvzLAo3M4Ymz</a>

Statutory Instrument 83 of 2020 Public Health (COVID-19 Prevention, Containment and Treatment) (National Lockdown) Order 2020 accessed on 08 July 2020, available at <a href="https://zimlii.org/zw/zw/subleg-consol/S.I.%2083%20of%202020%20Public%20Health%20%28COVID-19%20Prevention%2C%20Containment.pdf">https://zimlii.org/zw/zw/subleg-consol/S.I.%2083%20of%202020%20Public%20Health%20%28COVID-19%20Prevention%2C%20Containment.pdf</a>

Statutory Instrument 136 of 2020. [CAP. 15:17 Public Health (COVID-19 Prevention, Containment and Treatment) (National Lockdown) (Amendment) Order, 2020 (No. 10) accessed on 08 July 2020, available at

http://www.veritaszim.net/sites/veritas\_d/files/SI%202020-136%20%20Public%20Health%20%28CO VID-19%20Prevention%2C%20Containment%20and%20Treatment%29%20%28National%20Lockdown%29%20%28Amendment%29%20Order%2C%202020%20%28No.%2010%29.pdf

Tambudzai Gonese, Amanda Shivamba and Anneke Meerkotter (2020) A legal overview of the impact of COVID-19 on justice and rights in Southern Africa accessed on 08 July 2020, available at

https://www.southernafricalitigationcentre.org/wp-content/uploads/2020/05/Policy-brief-1-of-202 0-COVID-laws.pdf

Thandekile Moyo (2020) Censorship in Zimbabwe: when fake news is true and official news is fake accessed on 08 July 2020, available at

https://www.dailymaverick.co.za/article/2020-04-28-censorship-in-zimbabwe-when-fake-news-is-true-and-official-news-is-fake/#gsc.tab=0

United Cities and Local Governments [UCLG]. (2020). Digital Technologies and the COVID19 pandemic [Ebook] accessed on 08 July 2020, available at:

https://www.uclg.org/sites/default/files/eng\_briefing\_technology\_final\_x.pdf.

United Nations (2020) UN tackles infodemic of misinformation and cybercrime in COVID-19 crisis accessed on 08 July 2020, available at

https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19

United Nations COVID-19 Guidance (2020) accessed on 08 July 2020, available at

https://allafrica.com/stories/202006220883.html

United Nations (2020) COVID-19 and human rights: we are all in this together accessed on 08 July 2020, available at

https://www.un.org/victimsofterrorism/sites/www.un.org.victimsofterrorism/files/un - human rig hts and covid april 2020.pdf

United Nations Report of the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment (2012) accessed on 08 July 2020, available at <a href="https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session19/A.HRC.19.61.A">https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session19/A.HRC.19.61.A</a> dd.3\_EFSonly.pdf

William Gumede (2020) Freedom of expression and COVID-19 in Africa accessed on 08 July 2020, available at <a href="https://democracyworks.org.za/freedom-of-expression-and-covid-19-in-africa/">https://democracyworks.org.za/freedom-of-expression-and-covid-19-in-africa/</a>

World Health Organisation (2020) WHO urges caution as Africa eases lockdowns accessed on 08 July 2020, available at

https://www.afro.who.int/news/who-urges-caution-countries-africa-ease-lockdowns

Worldometer: Mauritius coronavirus (2020) accessed on 08 July 2020, available at

https://www.worldometers.info/coronavirus/country/mauritius/







Silky Oak House | Bally Oaks Office Park | 35 Ballyclare Drive | Bryanston Johannesburg, South Africa

- **\** +27 (0) 11 463 4594
- endcode.org
- base@endcode.org

   base@endcode.org
- @endcode\_org

