

**MAPPING DIGITAL  
RIGHTS AND ONLINE  
FREEDOM OF  
EXPRESSION  
LITIGATION IN EAST,  
WEST AND  
SOUTHERN AFRICA**

**Published by**

**Media Defence**

Published by Media Defence [www.mediadefence.org](http://www.mediadefence.org)  
This report was prepared with the assistance of ALT Advisory  
<https://altadvisory.africa/>

This work is licenced under the Creative Commons Attribution-NonCommercial 4.0 International License. This means that you are free to share and adapt this work so long as you give appropriate credit, provide a link to the license, and indicate if changes were made. Any such sharing or adaptation must be for non-commercial purposes and must be made available under the same “share alike” terms. Full licence terms can be found at <http://creativecommons.org/licenses/by-ncsa/4.0/legalcode>.



# TABLE OF CONTENTS

LIST OF ACRONYMS.....	5
EXECUTIVE SUMMARY .....	7
INTRODUCTION .....	8
Overview.....	8
Defining Digital Rights.....	9
Approach and Methodology .....	10
Acknowledgements .....	10
PART I: THEMES IN DIGITAL RIGHTS.....	12
I.    Defamation.....	12
Criminal defamation .....	12
Online defamation .....	15
Gender-based considerations .....	17
SLAPP suits .....	18
Opportunities for Litigation.....	19
II.   National Security, Counter Terrorism and Public Order Laws.....	20
SIM Card Registration .....	21
Surveillance.....	22
Public Order Laws .....	26
Facial Recognition Technology.....	27
Opportunities for Litigation.....	28
III.  Laws restricting online content and access.....	30
Hate Speech Legislation.....	31
Social Media and Internet Taxes .....	32
Social Media Monitoring .....	33
Mis- and/or disinformation .....	34
Content Regulation in Broadcast and Film .....	37
Net Neutrality .....	39
Opportunities for Litigation.....	39
IV.  Internet shutdowns .....	40
Increasing Incidences of Internet Shutdowns .....	41
Promising Developments.....	42
Catalysts .....	43
Effects of COVID-19.....	44
Opportunities for Litigation.....	45
V.   Cybercrime Legislation.....	47
Rise in Cybercrimes Laws .....	47
Effects of COVID-19.....	50

Opportunities for Litigation.....	51
VI. Media Regulation and Newsgathering Restrictions.....	52
Role of Regional Bodies.....	53
False news and misinformation.....	54
COVID-19 and the misinformation pandemic.....	56
Further Deterioration of Press Freedom.....	56
Promising Developments.....	58
Alternative Mechanisms to Advance Freedom of the Press.....	59
Opportunities for Litigation.....	59
VII. Data Protection.....	60
Proliferation of Data Protection Legislation.....	61
Biometric Data.....	62
Impact of COVID-19.....	63
Opportunities for Litigation.....	64
PART II: JURISPRUDENTIAL TRENDS ANALYSIS.....	68
CONCLUSION.....	75
APPENDIX A.....	76

## LIST OF ACRONYMS

ACHPR	African Commission on Human and Peoples' Rights
ADRF	African Digital Rights Fund
APC	Association for Progressive Communications
AU	African Union
BAKE	Bloggers Association of Kenya
CCTV	Closed Circuit Television
CIPESA	Collaboration on International ICT Policy in East and Southern Africa
CIPIT	Centre for Intellectual Property and Information Technology Law
CPJ	Committee to Protect Journalists
CSO	Civil Society Organisation
DFRL	Digital Forensic Research Lab
DMS	Device Management System
DRLI	Digital Rights Lawyers Initiative
EAC	East African Community
EACJ	East African Court of Justice
ECOWAS	Economic Community of West African States
ECtHR	European Court of Human Rights
EFF	Economic Freedom Fighters (South Africa)
FPB	Film and Publication Board (South Africa)
FRT	Facial Recognition Technology
ICCPR	International Covenant on Civil and Political Rights
ICTs	Information and Communication Technologies
ISP	Internet Service Provider
LCA	Lesotho Communications Authority
LGBTQI+	Lesbian, Gay, Bisexual, Trans, Queer and Intersex Plus
MISA	Media Institute of Southern Africa
MMA	Media Monitoring Africa
MMS	Multimedia Messaging Service
MPDP	Media Policy and Democracy Project
NCDC	National Centre for Diseases Control (Nigeria)
NIMC	National Identity Management Commission (Nigeria)

NGO	Non-Governmental Organisation
NIIMS	National Integrated Identity Management System
NITDA	National Information Technology Development Agency
OHCHR	The Office of the High Commissioner for Human Rights
POPIA	Protection of Personal Information Act 4 of 2013 (South Africa)
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (South Africa)
SADC	Southern African Development Community
SALC	Southern Africa Litigation Centre
SANEF	South African National Editors' Forum
SAPS	South African Police Service
SCA	Supreme Court of Appeal (South Africa)
SLAPP	Strategic Litigation Against Public Participation
SMS	Short Message Service
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization

## EXECUTIVE SUMMARY

In 2018, Media Defence published a research report titled 'Mapping Digital Rights and Online Freedom of Expression in East, West and Southern Africa' that mapped laws relating to digital rights, tracked the status of related litigation, highlighted opportunities for further efforts to advance the field, and identified relevant legal and civil society actors across the region.

The present report serves as an update and thematic review of some of the critical topics in digital rights litigation in East, West and Southern Africa, providing an overview of developments in jurisprudence, legislation and practice in the past three years, and highlighting lessons learned to further advance digital rights in the region going forward.

The report begins with an overview of the digital rights landscape and an introduction to the research methodology, before delving into recent developments in seven themes of particular relevance at present — (i) defamation; (ii) national security, counter-terrorism and public order laws; (iii) laws restricting online content and access; (iv) internet shutdowns; (v) cybercrime legislation; (vi) media regulation and newsgathering activities; and (vii) data protection. Following this review, high-level trends and themes are extracted through a jurisprudential trends analysis, which maps out some of the most significant court cases in digital rights in East, West, and Southern Africa since 1994. This review demonstrates the progress made in multiple areas of digital rights and freedom of expression online across the region, while also highlighting gaps and areas where further litigation might be fruitful.

We find that some landmark judgments have been achieved that significantly advance digital rights and freedom of expression online on the continent, such as those condemning internet shutdowns, invalidating excessive surveillance practices, and overturning criminal defamation laws. Similarly, many countries have implemented data protection and/or cybercrimes laws in a promising sign for the protection of the right to privacy. However, cybercrimes laws have also been widely used to stifle freedom of expression, along with an expansion of usage of the national security defence — particularly in the context of COVID-19 — and the deterioration of press freedom through the use of social media or 'false news' legislation. Despite growing global condemnation, internet shutdowns also continue to be used to stifle criticism, stymie social protest, and even undermine electoral processes.

This review demonstrates that much remains to be done to build a strong and rights-respecting framework for the regulation of the online sphere in East, West, and Southern Africa. Strategic litigation has played, and should continue to play, a crucial role in advancing some of these key developments – but must, importantly, be bolstered through research, advocacy, and educational campaigns so as to meaningfully realise digital rights for all persons in the region.

# INTRODUCTION

## Overview

In 2018, Media Defence published a research report titled ‘Mapping Digital Rights and Online Freedom of Expression in East, West and Southern Africa’ that mapped laws that pose a challenge to digital rights, tracked the outcome or status of related litigation, highlighted opportunities for further litigation, and identified relevant legal and civil society actors in the field. That report emphasised the fact that although freedom of expression online is well entrenched under international law, regional charters and domestic legislation in Africa, it nevertheless remained either under threat or only partially exercisable in practice as a result of low internet penetration, laws seeking to regulate the internet, and closing civic space across the continent.

The present report seeks to update and advance this work by reflecting on developments in the field of digital rights in Africa according to a number of prominent themes, with a particular focus on legislation and litigation introduced since the publication of the original report in 2018. In analysing developments in the field and comparing the state of play between then and now, we refer to the previous report as either ‘the original report’ or ‘the 2018 report.’

The present review highlights that in many respects the field of digital rights has made significant gains in recent years. For example, ground-breaking litigation condemning internet shutdowns at the regional and domestic levels has finally been achieved, setting an important precedent for the circumstances in which internet shutdowns constitute a violation of the right to freedom of expression. Numerous countries have passed data protection legislation in recent years, setting the scene for a society in which data is appropriately treated as a sensitive resource and online privacy is protected. Optimism also stems from the fact that the community of litigators and activists working on digital rights litigation appears to be growing, as evidenced by the acceleration in judgments coming out of both domestic and regional courts that has implications for freedom of expression online. Although the Nigerian Digital Rights and Freedom Bill – which would have been the first specific law on digital rights and internet freedoms in Africa – failed when President Buhari declined to assent to the bill in 2019,<sup>1</sup> it is promising to see that a new draft is in the works. We have also seen the appearance of a number of initiatives specifically targeting digital rights litigation on the continent, such as the Digital Rights Lawyers Initiative (DRLI) in Nigeria, as well as the African Digital Rights Fund (ADRF) established by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA).

A key development since the first edition of this report has been the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa (African Declaration), adopted by the African Commission on Human and Peoples’ Rights (ACHPR) in 2019.<sup>2</sup> This revision seeks to bring article 9 of the African Charter on Human and Peoples’ Rights<sup>3</sup> (African Charter) into the digital era, and includes provisions relating to internet access, privacy, surveillance and data protection. Notably, it requires states to report to the ACHPR on their

<sup>1</sup> Techpoint Africa, ‘Nigeria’s President Refused to Sign its Digital Rights Bill, What Happens Now?’, (2019) (accessible [here](#)).

<sup>2</sup> African Declaration (2019) (accessible [here](#)).

<sup>3</sup> African Charter on Human and Peoples’ Rights (1981) (accessible [here](#)).



compliance with these provisions, which will now mean that states will be directly obliged to answer to the ACHPR for non-compliance with digital rights norms and standards.

However, despite these developments, there have also been some disappointing setbacks which indicate that efforts to advance online freedom of expression through litigation still lag behind mainstream human rights in Africa. While access to the internet has continued to expand in recent years as telecommunications markets liberalised and governments adopted 'digital transformation' strategies to enhance development, this has been accompanied by increased attempts to control the flow of information through online platforms using inventive and often unnecessarily harsh methods.

Cybercrimes and false news legislation have proliferated, in many cases providing legal cover for repressive measures that surveil the media and activists or criminalise dissent. Criminal defamation provisions remain in several African countries, despite numerous judgments against them in both domestic and regional courts, indicating the importance of enforcement measures and other complementary initiatives beside litigation.

Overall, civic space has been closing in many countries in Africa over the past half-decade, a trend accelerated by the COVID-19 pandemic which justified governments' efforts to implement restrictive measures over communication and the media. It remains to be seen whether these measures will prove temporary or whether COVID-19 has precipitated a new era of data-driven surveillance and the criminalisation of speech.

Litigation on freedom of expression online and digital rights remains an impactful path to protecting the media and open democracy, but digital rights legislation and jurisprudence continue to trail behind that of 'traditional' freedom of expression measures. With the changes occasioned in our societies as a result of the COVID-19 pandemic, technologies such as the internet have only become more important, forming the basis of connection between our communities, enabling virtual education and healthcare, and being used as a tool to stem the tide of infections across the continent.

It is, therefore, more crucial than ever that comprehensive legal protections for freedom of expression online and digital rights be put in place and that meaningful access to the internet be further enabled. The ACHPR, the African Court on Human and Peoples' Rights (African Court), the Economic Community of West African States (ECOWAS) Community Court of Justice (ECOWAS Court) and the East African Court of Justice (EACJ) have proven willing to challenge authoritarian governments seeking to bypass human rights in order to exert control and to issue rulings in accordance with regional and international law. It is critical to continue building on this momentum to further advance digital rights in East, West and Southern Africa in order to secure a safe and inclusive internet for all.

## **Defining Digital Rights**

For the purposes of this report, we use the term "digital rights" to refer broadly to human rights in the digital era, and the rights that are implicated in the access and use of the internet and other information and communication technologies (ICTs). This comprises a wide range of distinct but interrelated topics. While the report does not purport to cover the full ambit of

digital rights, it focuses on some of the most pertinent trends and developments seen across the region, and in particular the changes in the eco-system since 2018.

## **Approach and Methodology**

In terms of the temporal scope, the report focuses primarily on developments occurring during the three-year period between mid-2018 to mid-2021, although certain key laws and policies pre-date this period, and have been included to provide a more holistic picture.

In preparing this report, we have relied primarily on secondary sources. The reports of civil society organisations at the domestic, regional and international levels that are active in East, West and Southern Africa have been key in informing its contents. We have also had regard to media reports, press statements, submissions to human rights treaty mechanisms and other similar briefings to develop a fuller understanding. Furthermore, in respect of jurisprudence, laws and policies, regard has also been had to the primary sources that are under discussion.

A further source of information has been through questionnaires sent to legal and civil society organisations working in the region. A copy of the questionnaire has been included as an appendix at the end of this report. We sought input from the respondents on the current context of digital rights, primary developments in the field in the past three years, and their views on the opportunities and challenges for the future. The questionnaire was sent to legal, media and civil society organisations that we are aware of working across all three sub-regions. We are deeply grateful for the input received from the respondents acknowledged below. In terms of the methodology for future iterations of this report, we will continue to strive to include as many respondents' views as possible in order to understand the situational positioning from a diverse range of viewpoints.

We are cognisant that the report presents a high-level overview of complex and nuanced issues. We have, to the extent possible, endeavoured to rely on a range of sources from different actors to ensure that the content of the report is balanced. We have exercised our discretion in selecting the laws, policies and other developments that are highlighted in this report, but recognise that there will certainly be others that have not been included that are also of relevance to digital rights and freedom of expression online.

Lastly, we note that while we have endeavoured to ensure the accuracy of the content contained in the report at the time of publication for the period under consideration, the field of digital rights is dynamic and constantly evolving with new laws, judicial pronouncements and other developments occurring frequently. Changes in leadership, legislative amendments and other developments occur rapidly, and can drastically affect the landscape at any time.

## **Acknowledgements**

We would like to thank the following participants for their input into this research:

- Grace Mutung'u (Centre for Intellectual Property and Information Technology Law (CIPIT))
- Bulanda Nkhowani (Paradigm Initiative)

- Irene Chukwukelu / Olumide Babalola (DRLI)
- Josephine Miliza (Association for Progressive Communications (APC))
- Zaituni Njovu (Zaina Foundation)

We note that while the input of the individuals and organisations above has been considered and incorporated as appropriate, this should not necessarily be construed as them having endorsed the contents of this report.

# PART I: THEMES IN DIGITAL RIGHTS

The digital rights field has undergone a major transformation in recent years, with a flurry of legislation being passed and/or notable legal challenges being brought in some fields. As technology rapidly evolves, so too must the law. The developments highlighted in this section show that there have indeed been significant changes in terms of legislation and litigation in East, West and Southern Africa, although whether it is sufficient to keep pace with technological evolution is a separate question.

This section deals with seven issues within the broader digital rights field that are of relevance in the region for various reasons. First, they are issues on which legislation has recently developed, and/or in which various court challenges of relevance have been brought in the past few years. Second, they speak to some of the most pressing challenges presently facing human rights defenders and journalists operating in the region, and which are common to actors across multiple countries. Finally, they are of utmost importance for freedom of expression and the exercise of fundamental rights and raise questions that are in the process of being defined in international law.

## I. Defamation

Traditional or offline defamation laws form the basis for how online defamation is generally regulated and litigated. In this regard, although courts in the region have only just begun to grapple with the differences between online and offline defamation, and how to apply existing laws to the digital domain, there have nevertheless been some positive developments in how defamation is regulated across the continent. As set out in the African Declaration, the ACHPR has made clear that, in the context of defamation claims, no one shall be found liable for true statements, expressions of opinion or statements which are reasonable to make in the circumstances; public figures shall be required to tolerate a greater degree of criticism; and sanctions should never be so severe as to inhibit the right to freedom of expression.<sup>4</sup>

In what follows, we consider the laws relating to criminal defamation and defamation online, flag some gender-based considerations within the field of defamation, and evaluate the related trends of SLAPP suits and insult laws.

### ***Criminal defamation***

The original report noted that despite recent progress made in much of the world against criminal defamation statutes, a number of African countries retained such laws.<sup>5</sup> It nevertheless highlighted the ground-breaking 2013 judgment of the African Court on Human and Peoples' Rights (African Court) in *Konaté v Burkina Faso*,<sup>6</sup> which held that aspects of criminal defamation laws, particularly those imposing the sanction of imprisonment, violated article 9 of the African Charter and other international human rights provisions recognising the right to freedom of expression. *Konaté* has been particularly influential in other countries in

<sup>4</sup> Principle 21 of the African Declaration, n 2.

<sup>5</sup> Media Defence, 'Mapping Digital Rights Litigation in East, West and Southern Africa', (2018) at p. 88 (accessible [here](#)).

<sup>6</sup> *Konaté v Burkina Faso*, Application No. 004/2013 (accessible [here](#)).

the region, having been cited and followed in domestic court decisions regarding challenges to the offence of criminal defamation.<sup>7</sup>

In the intervening period since the original report, this trend has continued, and several other countries have struck down criminal defamation laws. In Sierra Leone, for example, the criminal libel law was invalidated in 2020,<sup>8</sup> while Lesotho did the same in 2018, stating that it violated the right to freedom of expression as protected under the Lesotho Constitution.<sup>9</sup>

The case of *Media Council of Tanzania v Attorney General* is instructive in this regard. Three non-governmental organisations (NGOs) approached the EACJ to challenge the Tanzanian Media Services Act No. 120 of 2016 for its unjustified limitation on freedom of expression.<sup>10</sup> While this case was not exclusively about online defamation, important arguments were raised about criminal defamation.<sup>11</sup> According to the EACJ, the Media Services Act failed to define defamation in sufficiently precise terms to enable a journalist or other person to plan their actions within the law. Further, the definition made the offence continuously elusive by reason of subjectivity.

The original report noted Rwanda as an example of a country in which penalties for criminal defamation had actually been increased in recent years, counter to the dominant trend.<sup>12</sup> Defamation against private individuals was, however, decriminalised under the revised Penal Code and a provision that criminalised the “humiliation of national authorities” was overturned by the Supreme Court in 2019. Notably, however, it upheld criminal defamation against the president.<sup>13</sup> In a major development for the field of defamation, in 2020 the ACHPR declared that Rwanda’s laws — and criminal defamation and insult laws in general — violated article 9 of the African Charter and requested Rwanda to amend them immediately.<sup>14</sup> The ACHPR stated that:

“[Public officials] must tolerate a higher degree of scrutiny of their actions and must be willing to accept criticism from the press, particularly in the context of political debate, as without such criticism, the public would have no way of holding them accountable and there would be no limits to the exigencies of public officials’ powers.”

Although it is unclear whether this will be implemented by Rwanda, the ACHPR’s decision, building on the prior ruling by the ECOWAS Court in *Federation of African Journalists v The Gambia*,<sup>15</sup> drew a clear line in the sand for all criminal defamation and libel legislation and has created fertile ground for further litigation in this regard on the continent.

---

<sup>7</sup> See, for instance, *Misa-Zimbabwe et al v Minister of Justice et al*, Case No. CCZ/07/15 (accessible [here](#)); *Okuta v Attorney General*, Petition No. 397 of 2016 (accessible [here](#)).

<sup>8</sup> Abdul Brima, ‘After A 55-Year Struggle, A Major Victory For Press Freedom In Sierra Leone’, Mail & Guardian (2020) (accessible [here](#)).

<sup>9</sup> *Peta v Minister of Law*, Constitutional Court of Lesotho, Case no. CC 11/2016 (2018) (accessible [here](#)).

<sup>10</sup> *Media Council of Tanzania and Others v Attorney-General of the United Republic of Tanzania*, East African Court of Justice Ref. No. 2 of 2017 (2019) (accessible [here](#)).

<sup>11</sup> *Media Council of Tanzania v Attorney General* in Global Freedom of Expression at Columbia University, (accessible [here](#)).

<sup>12</sup> Media Defence, n 5, p. 43.

<sup>13</sup> Freedom House, ‘Freedom on the Net: Rwanda 2020’ (2020) (accessible [here](#)).

<sup>14</sup> Media Defence, ‘African Commission Finds Rwandan Authorities Violated Journalists’ Right to Freedom of Expression’, (2020) (accessible [here](#)).

<sup>15</sup> Media Defence, ‘Update: ECOWAS Court Delivers Landmark Decision in One of Our Strategic Cases Challenging The Laws Used To Silence And Intimidate Journalists In The Gambia’, (2018) (accessible [here](#)).

It is increasingly acknowledged in recent years that governments and other public authorities should not be able to bring actions in defamation or insult. The Office of the High Commissioner for Human Rights (OHCHR) has, for example, stated that international jurisprudence supports this view and that the United Nations (UN) Human Rights Committee has called for the abolition of the offence of “defamation of the State.”<sup>16</sup> This may be an arena wherein litigation, both at the domestic, sub-regional and regional level, could be able to progress the conclusion of international law by seeking judgments in this regard. As mentioned above, the African Declaration clearly requires states to repeal all laws that criminalise insult, and further provides that public figures shall be required to tolerate a greater degree of criticism.

As discussed above, the revised Penal Code which Rwanda introduced in 2018 bucks this trend by prescribing prison sentences of five to seven years for defamation against the president and criminalising “humiliating” state officials.<sup>17</sup> Several other countries within the region retain some form of criminal defamation or libel laws, such as Zambia and Namibia, and continue to prosecute in terms of these laws.<sup>18</sup> In Zambia, a 15-year-old boy was arrested on three counts of defamation in 2020 for posting allegedly defamatory or insulting content against the Zambian President on Facebook.<sup>19</sup> In Angola, where a constitutional challenge to the criminal defamation law is in progress,<sup>20</sup> the state continues to charge journalists and activists under the existing law.<sup>21</sup>

## Alternative Mechanisms

Even in Ghana, the first African country to decriminalise defamation, “there has been an increase in civil suits for libel brought by powerful individuals, leading, in some cases, to damages payouts of such large proportions to powerful individuals as to threaten the existence of some media outlets.”<sup>22</sup> Likewise, although Lesotho decriminalised defamation, it retained the crime of *scandalum magnatum* (offences against the royal family), which is increasingly being used against critics by the government of Lesotho.<sup>23</sup>

These examples are evidence that, even in places where criminal defamation is no longer in use, mechanisms closely related to defamation are still being used to close civic space and threaten freedom of expression through overly harsh policing of ‘insulting’ speech.

<sup>16</sup> OHCHR, ‘Report Of The Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression’, E/CN.4/2000/63 (2000) at para. 50 (accessible [here](#)).

<sup>17</sup> Freedom on the Net, ‘Rwanda’, (2019) (accessible [here](#)).

<sup>18</sup> In Zambia, the law on criminal defamation is contained in sections 191-198 of the Penal Code (accessible [here](#)), while civil defamation is covered in Chapter 68 of the Defamation Act of 1953 (accessible [here](#)). On South Africa, see Bregman Moodley Attorneys, ‘Criminal Defamation’, (2019) (accessible [here](#)). On Namibia, see Paradigm Initiative, ‘LONDA: Digital Rights And Inclusion In Africa 2020’, (2021) at p. 68 (accessible [here](#)).

<sup>19</sup> Chris Phiri, ‘ZOOM Arrested For The Offence Of Defamation Of The President’, Zambia Reports (2020) (accessible [here](#)).

<sup>20</sup> Human Rights Watch, ‘Angola, Country Summary’, (2018) at p. 2 (accessible [here](#)).

<sup>21</sup> Committee to Protect Journalists (CPJ), ‘Angolan Editors Questioned In Separate Criminal Defamation Investigations’, (2021) (accessible [here](#)).

<sup>22</sup> PEN South Africa, ‘Stifling Dissent, Impeding Accountability: Criminal Defamation Laws In Africa’, (2017) at p 4 (accessible [here](#)).

<sup>23</sup> Hoolo ‘Nyane, ‘Abolition Of Criminal Defamation And Retention Of Scandalum Magnatum in Lesotho’, African Human Rights Law Journal (2019) (accessible [here](#)).

Religious defamation or blasphemy laws also remain common among countries in the region, many of which inherited the crime of blasphemous libel through the adoption of the common law system. For example, despite ostensibly being a secular country with no state religion, article 816 of Ethiopia's Criminal Code states that anyone who, by:<sup>24</sup>

“...gestures or words scoffs at religion or expresses himself in a manner which is blasphemous, scandalous or grossly offensive to the feelings or convictions of others or towards the Divine Being or the religious symbols, rites or religious personages, is punishable with fine or arrest not exceeding one month.”

Some countries have implemented excessively harsh penalties for the crimes of blasphemy and defamation of religion, including death. Mauritania's blasphemy law, updated in 2017 to include even harsher language, ranks as the worst blasphemy law in the world, containing the penalty of death even if the accused repents for the alleged insult.<sup>25</sup> The Gambia, Zimbabwe, Botswana, Malawi, Kenya, and Ethiopia all also scored highly on the harshness of their religious defamation laws.<sup>26</sup> This is despite clear guidance in General Comment 34 on the International Covenant on Civil and Political Rights<sup>27</sup> (ICCPR) that “prohibitions of displays of lack of respect for a religion or other belief system, including blasphemy laws, are incompatible with the Covenant.”<sup>28</sup>

### **Online defamation**

It appears that the number of defamation cases is increasing in many places, a trend that is at least partly a result of the exponential growth of social media platforms.<sup>29</sup> Publications on social media are not afforded the usual means of redress that mainstream media is, such as complaints to a Press Council or other self-regulatory bodies for the media. For such cases, pursuing action through the courts can be the only option, and we are therefore likely to see the incidence of defamation cases continuing to rise in coming years. The argument has thus been made for faster and cheaper ways to resolve defamation cases that stem from publications on social media.<sup>30</sup>

As legal journalist, Franny Rabkin, points out, the law needs to find ways to adapt to the peculiar characteristics of online defamation cases:

“The nature of publication on social media is different — it is fast, it is often unverified, it goes viral. It is, especially in the case of Twitter, robust, to put it mildly. It is also often anonymous. All this needs to be considered when looking at how to find the balance between free expression and dignity.”

---

<sup>24</sup> End Blasphemy Laws, 'Ethiopia', (2020) (accessible [here](#)).

<sup>25</sup> United States Commission on International Religious Freedom, 'Apostasy, Blasphemy And Hate Speech Laws In Africa: Implications For Freedom Of Religion Or Belief', (2019) at p. 16 (accessible [here](#)).

<sup>26</sup> *Ibid* at p. 15.

<sup>27</sup> International Covenant on Civil and Political Rights (1966) (accessible [here](#)).

<sup>28</sup> UN Human Rights Committee, 'General Comment No. 34', (2011) at p. 12 (accessible [here](#)).

<sup>29</sup> Franny Rabkin, 'Defamation Law's Face Is Changing', Mail & Guardian (2019) (accessible [here](#)).

<sup>30</sup> *Ibid*.

The case of *Manuel v Economic Freedom Fighters and Others*<sup>31</sup> provides insight into how courts may use existing defamation laws to deal with cases involving statements in online publications. The case concerns a defamation claim brought by Trevor Manuel, a prominent South African politician and former Minister of Finance, against the Economic Freedom Fighters (EFF), South Africa's third-largest political party, as a result of a statement published by the EFF on Twitter in March 2019. A ruling by the Johannesburg High Court on 30 May 2019 held that the EFF's statement was defamatory, as the tweet implied that Manuel was dishonest, unscrupulous and lacked integrity.<sup>32</sup> The Court's judgment contained several novel findings related to the medium of publication:<sup>33</sup>

- Because it centred on a statement posted on Twitter, the Court explained that “[t]he hypothetical ordinary reader must be taken to be a reasonable representative of Twitter users who follow the EFF and Mr Malema and share his interest in politics and current affairs”.
- The Court referred to the ‘repetition rule’, whereby persons who repeat a defamatory allegation made by another “are treated as if they made the allegation themselves, even if they attempt to distance themselves from the allegation.” This has implications for others who play a role in disseminating defamatory statements further, such as by ‘retweeting’. The Court did not explicitly address this point further.
- The Court also stated, for the first time, that the reasonable publication defence in a defamation case is applicable beyond just the media to ordinary members of the public, provided they take all reasonable steps to verify the information as normally required under that defence.
- Although the judgment ordered the defendants to remove the impugned statement from their media platforms within 24 hours, the deletion of a tweet on Twitter does not necessarily remove it from all platforms, as there are other ways in which the content may have been distributed not addressed by the deletion (such as retweets in which persons added a comment of their own). This is a particular challenge that social media platforms pose when seeking to find an effective remedy to a claim of defamation.

On appeal in December 2020, the EFF argued that political parties should not have to verify the information they publish on Twitter, arguing that requiring a party to verify content and seek comment before publishing would have a chilling effect on a political party's ability to exercise its constitutional rights. Mr Manuel argued that the EFF knew that the content of the tweet was false and defamatory. The Supreme Court of Appeal (SCA) found that because the publication on Twitter had been circulated as a media release and a whole statement, and was not confined to a limited number of characters or written in a form of shorthand, the fact that the statement was published on Twitter did not require the court to evolve a new approach to the reasonable reader that was applicable in the context of social media platforms.<sup>34</sup> Nevertheless, the SCA did implicitly acknowledge that in cases where publications are of

---

<sup>31</sup> *Manuel v Economic Freedom Fighters and Others*, High Court of South Africa, Gauteng Division, Case no. 13349/2019, (2019) (accessible [here](#)).

<sup>32</sup> *Ibid*.

<sup>33</sup> Avani Singh, ‘Social Media And Defamation Online: Guidance From Manuel v EFF’, ALT Advisory Insights (2019) (accessible [here](#)).

<sup>34</sup> *Economic Freedom Fighters and Others v Manuel*, Supreme Court of Appeal of South Africa, (2020) at para. 26 and 31 (accessible [here](#)).



limited characters or written in shorthand (as on social media), the factors relating to a 'reasonable reader' may need to be reconsidered.

In its ruling, the SCA accepted that “the rise of social media will continue to focus attention on this area of the law”, noting the far reach of content published by ordinary members of society. It upheld the finding that the allegations were defamatory, the removal of the statements from their media platforms, and the interdict against repeating the statement.<sup>35</sup> This case demonstrates a noteworthy step towards the development of legal understandings of defamation in the context of social media. The matter is currently pending on appeal before the Constitutional Court.

For litigators, a particularly interesting aspect of the case involved the fact that the defamation proceedings were instituted by way of application (i.e. on affidavits), rather than running a full trial as would have been the ordinary course. It was therefore a contentious aspect of the case that the High Court awarded damages in the amount of R500 000 (roughly USD35 000), despite no oral evidence having been led. This was overturned by the Supreme Court of Appeal and will be one of the key issues for determination by the Constitutional Court in the appeal. This approach of instituting defamation proceedings by way of application has since successfully been followed in several other cases in South Africa, such as *Gqubule-Mbeki and Another v Economic Freedom Fighters and Another*<sup>36</sup> and *Ramos v Independent Media (Pty) Limited and Others*,<sup>37</sup> although in those cases the applicants did not seek damages for the harm suffered.

While defamation claims can be an important tool to vindicate a person's good name and reputation, it is also noteworthy that defamation cases are on the rise, and we should therefore be vigilant as to how, as the original report noted, defamation is frequently misused as a tool to stifle dissent and participation. In Kenya, for example, “[i]ntermediaries can be held legally responsible for content carried on or through their networks, which amounts to libel under the Defamation Act.”<sup>38</sup> This provides governments with extensive powers to control online communication and leverage intermediaries such as internet service providers (ISPs) to crack down on free speech. The concept of ‘intermediary liability’ is a controversial one, on the one hand serving as a tool to manage illegal content and misinformation online, while on the other posing risks to freedom of expression by enabling “over-broad private censorship.”<sup>39</sup> Some countries in Africa have laws providing for the limitation of intermediary liability, such as Ghana and Uganda.<sup>40</sup>

### **Gender-based considerations**

In recent years, it has become clear that defamation is also frequently used to silence victims and survivors of gender-based violence. In 2014, Shailja Patel, a renowned Kenyan poet,

---

<sup>35</sup> *Ibid.*

<sup>36</sup> *Gqubule-Mbeki v Economic Freedom Fighters*, High Court of South Africa, Case No. 30143/2018 (2020) (accessible [here](#)).

<sup>37</sup> *Ramos v Independent Media (Pty) Ltd and Others*, High Court of South Africa, Case No. 01144/21 (2021) (accessible [here](#)).

<sup>38</sup> Media Defence, n 5, p. 26.

<sup>39</sup> OHCHR, ‘Report Of The Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression’ (2011) (accessible [here](#)).

<sup>40</sup> See article 92 of Ghana's Electronic Transactions Act of 2008 (accessible [here](#)) and section 29 of Uganda's Electronic Transactions Act of 2011 (accessible [here](#)). For more on litigating intermediary liability, see *Delfi AS v Estonia* and *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*, both in the European Court of Human Rights.

playwright and activist, publicly accused a fellow writer, Tony Mochama, of sexual harassment at a writers' workshop that the two attended. Mochama sued for defamation, claiming the allegations were false and Patel had a pre-existing grudge against him. In 2019, a judge found against Patel, ordered her to pay damages of more than \$87 000, to apologise, and to never publish defamatory statements against Mochama again. The magistrate also castigated Patel for initially turning to social media for justice as she did not believe the justice system would treat her case fairly.<sup>41</sup>

On the flipside, online 'naming and shaming' has become a popular recourse for victims of gender-based violence, particularly in countries where there is little trust in the criminal justice system to fairly investigate such crimes, and in which women are frequently blamed, including by police and the courts, for purportedly 'enabling' the crime. In some cases, public 'registers' have even been compiled of accused perpetrators with the aim of warning future potential victims and raising awareness about the pervasiveness of these crimes. In South Africa, for example, the hashtag #RURferenceList was published on social media naming alleged rapists at Rhodes University, catalysing widespread student protests against what activists said was an institutionalised rape culture at the university.<sup>42</sup> However, such efforts often come up against harsh defamation laws. There is therefore a need to find a balance between these competing needs that promotes truth-seeking and a victim-centric approach while maintaining appropriate protections for violations against reputation and dignity. This is arguably an area where the law must be further developed, and in which litigation may have a role to play.

It is important to note that defamation proceedings have also been used to vindicate the rights of victims of the non-consensual sharing of intimate images, such as in the case of *KS v AM and Another*<sup>43</sup> that is currently pending before the High Court of South Africa. In this case, the respondent was interdicted from publishing explicit sexual video footage and photos of the applicant on Facebook and was ordered to submit the footage to the sheriff for forensic audit and removal from the digital equipment.

### **SLAPP suits**

In recent years, defamation suits are also becoming a central component of a new intimidation tactic against activists frequently used by private actors to suppress criticism of their activities. Strategic Lawsuits Against Public Participation (SLAPP suits) are on the rise around the world,<sup>44</sup> and are used intentionally to bury critics under expensive and often baseless legal claims in order to silence them. Often, the objective in these cases is not a positive judgment, but rather to leverage the threat of financial damage. Defamation, libel, and slander claims can therefore be apt tools for such an objective.

In 2021, the Western Cape High Court in South Africa issued a ground-breaking ruling recognising a SLAPP defence in a defamation case for the first time in the country.<sup>45</sup> The

---

<sup>41</sup> Tamerra Griffin, 'She Was Ordered To Pay Damages And Apologize To The Man Who Allegedly Assaulted Her – So She Left The Country', BuzzFeed News (2019) (accessible [here](#)).

<sup>42</sup> Sonke Gender Justice, 'Call for Policy Reform At Rhodes University Following Release Of List Of Alleged Rapists', (2016) (accessible [here](#)).

<sup>43</sup> *KS v AM*, High Court of South Africa, Case No. A3032/2016 (2017) (accessible [here](#)).

<sup>44</sup> Foreign Policy Centre, 'The Increasing Rise, And Impact, Of SLAPPs: Strategic Lawsuits Against Public Participation', (2020) (accessible [here](#)).

<sup>45</sup> *Mineral Sands Resources (Pty) Ltd and Another v Reddell and Others; Mineral Commodities Limited and Another v Dlamini and Another; Mineral Commodities Limited and Another v Clarke*, Western Cape High Court of South Africa (2021) (accessible [here](#)).

case involved a mining company that had been seeking to develop a project in an environmentally protected region of South Africa, and which had sued environmental activists who criticised the project publicly for defamation for an amount of approximately R14 million (equivalent to roughly \$1 million). The court ruled that the mining company was seeking “exorbitant amounts for damages” which the defendants could not afford; that it was “evident that the strategy adopted” by the company was that “the more vocal and critical the activist is ... the higher the damages amount claimed.” The court also stated that because the company “would be satisfied to dispose of the matter on the basis of a public apology”, it was clear that the action was not aimed at obtaining monetary or financial damages but rather at “vindicating a right” or for some other purpose.<sup>46</sup>

### **Other SLAPP Suits Against Environmental Defenders**

In another example in Cameroon, an international timber company filed multiple lawsuits against an investigative journalist after he published what he alleged was evidence of its various unlawful practices.<sup>47</sup> The lawsuits claim that Mr Nestor Nga Etoga had published defamatory information and false news. Media Defence, which is supporting Mr Nga Etoga, argues that the case is a typical example of the heightened legal risks that journalists reporting on environmental issues often face, particularly those reporting critically on multi-national corporations.

A similar case was brought against an environmental group in South Africa that is accused of bringing “obstructive, delaying and frustrating” objections to attempts by two property developers to develop an environmentally sensitive area.<sup>48</sup> The matter is currently pending before the High Court, and the SLAPP suit defence has been raised on behalf of the activists.

### ***Opportunities for Litigation***

Litigation in regional and sub-regional fora should be used to further the reach of the decisions of the African Court, the ACHPR and the ECOWAS Court on criminal defamation and libel, and to ensure implementation of those rulings. In the African Declaration, the ACHPR has made clear that “[s]tates shall repeal laws that criminalise sedition, insult and publication of false news”, and further that “[s]tates shall amend criminal laws on defamation and libel in favour of civil sanctions which must themselves be necessary and proportionate”.<sup>49</sup> It goes on to state that the imposition of custodial sentences for the offences of defamation and libel is a violation of the right to freedom of expression.<sup>50</sup> It is therefore an apt time to advance existing case law to seek the removal of remaining criminal defamation law across the continent.

---

<sup>46</sup> *Ibid* at para. 62.

<sup>47</sup> Media Defence, ‘Media Defence Supports Legal Defence Of Cameroonian Journalist In Multiple Lawsuits Filed By International Timber Company’, (2021) (accessible [here](#)).

<sup>48</sup> *Century Property Developments (Pty) Ltd and Another v Kallesen and Another*, Case No. 5098 (2021) (accessible [here](#)).

<sup>49</sup> Principle 22(2) and (3) of the African Declaration, n 2.

<sup>50</sup> Principle 22(4) of the African Declaration, n 2.

Digital rights can also be further advanced by challenging defamation laws that provide for the offence of ‘defamation of the state’ or that enable government and other public officials to bring defamation actions. Likewise, litigators should be encouraged to target related laws that remain on the books such as scandalum magnatum in Lesotho and religious defamation or blasphemy laws. It is also important to challenge the increasing trend of exorbitant civil damages being awarded, which can prove as stifling for freedom of expression and the press as criminal defamation laws.

There appears to be room for the expansion of litigation seeking to use the SLAPP defence or other abuse of processes statutes in meritless defamation cases, including those online, relying on the example of South Africa. The past success of replicating the ‘reasonable publication’ defence from South Africa in Namibia may prove instructive in this regard.<sup>51</sup> In some jurisdictions, it may also be worthwhile to explore the possibility of enacting anti-SLAPP legislation, as has been done in Canada,<sup>52</sup> an area wherein the ACHPR and sub-regional bodies have the potential to play a leading role in developing model laws. Notably, some jurisdictions deal with defamation under the common law instead of in legislation, in which case this recommendation may need to be nuanced.

While there are certainly concerns with the way in which defamation claims have been raised to stifle criticism or dissent, the law of defamation remains a powerful and important tool to vindicate the good name and reputation of affected persons in appropriate circumstances. It can effectively be used to counter disinformation spread, including on social media. It is therefore necessary to consider ways in which swift and effective remedies can be found in response to such claims, including where defamation takes place via social media, which may require litigators and courts to be more creative.

Finally, further exploration is recommended with regards to the role of defamation law in gender-based violence, as there is a need to find an appropriate balance between protecting reputation while enabling transparency and freedom of expression about wrongdoing. Litigation may be a useful tool to consider in this regard.

## II. National Security, Counter Terrorism and Public Order Laws

As emphasised in the 2018 report, “human rights violations are frequently committed under the guise of national security or antiterrorism measures.”<sup>53</sup> In numerous African countries, national security has long been used as a justification for laws criminalising dissent, misinformation or fake news, and various measures aimed at controlling free speech, such as SIM card registration initiatives (such as in Kenya and Nigeria), surveillance and interception programmes (such as those in Kenya and Rwanda), and partial or total internet or social media shutdowns (such as in Uganda). In particular, some countries’ laws criminalise speech that ‘disturbs the peace’ or ‘threatens national integrity’, as well as placing harsh sentences on those who criticise the president or head of state. National security legislation can have wide-reaching implications for media freedom and can be used to avoid constitutional checks and balances. The major challenge with these amorphous concepts is that they are seldom

---

<sup>51</sup> *Trustco Group International Ltd and Others v Shikongo*, Supreme Court of Namibia, Case No. SA 8/2009 (2010) (accessible [here](#)).

<sup>52</sup> Osler, O’Brien and Tsilivis, ‘Ontario Court Of Appeal Clarifies Test Under “Anti-SLAPP” Legislation’ (2018) (accessible [here](#)).

<sup>53</sup> Media Defence, n 5, p. 92.

defined, but are applied broadly to encapsulate a wide range of speech activities, therefore unduly limiting the right to freedom of expression.

The 2018 report also noted the harsh sentences imposed in a number of countries on statements that were seen to encourage terrorism, such as in Ethiopia.<sup>54</sup> Some laws go so far as to require individuals to register telecommunications equipment (including smartphones) with the government (for example, in Ethiopia) or to hold ISPs or intermediaries liable for any information passing through their services that promotes terrorism (for example, in Uganda).

This section reflects on the ways in which national security justifications have continued to be used broadly across the region in the past three years. It sets out various methods through which governments use the defence of national security to infringe on freedom of expression online, including SIM card registration programmes, public order laws, surveillance tools and facial recognition technology.

### ***SIM Card Registration***

Mandatory SIM card registration has continued to serve as a popular means for controlling access to the internet and online speech across Africa, ostensibly for national security, counterterrorism or crime-fighting purposes. As of February 2019, more than 50 countries in Africa had implemented such laws, with another one (Namibia) considering doing so.<sup>55</sup> Nigeria recently attempted to rapidly implement a SIM card registration process in 3 months,<sup>56</sup> per the Revised National Identity Policy for SIM Card Registration,<sup>57</sup> a process that experienced numerous delays after additional complications became evident.

SIM card registration raises concerns for access to the internet by raising the barriers to entry and effectively discouraging or disabling the most marginalised from accessing the internet and communications infrastructure.<sup>58</sup> In South Africa, a major operator lost 1 million subscribers after the introduction of SIM card registration laws, while in Zimbabwe about 2 million and in Kenya more than 1.2 million were lost.<sup>59</sup> Evidence also shows that SIM card registration programmes depressed growth in mobile penetration.<sup>60</sup> They further have implications in terms of chilling free speech, by making it easier for government or security agencies to track and monitor communications through targeted surveillance, a process that is frequently abused by governments to target journalists and critics.<sup>61</sup>

Lastly, SIM card registration raises concerns for data protection, by relying on the collection of biometric and personal information, often in the absence of comprehensive data protection

---

<sup>54</sup> *Ibid* at p. 22.

<sup>55</sup> Privacy International, 'Africa: SIM Card Registration Only Increases Monitoring And Exclusion', (2019) (accessible [here](#)).

<sup>56</sup> Dennis Ezezi, 'Buhari Directs NCC To Collect Nigerians' Phone IDs In Three Months', The Guardian Nigeria (2021) (accessible [here](#)).

<sup>57</sup> Federal Ministry of Communications and Digital Economy, 'Revised National Identity Policy For SIM Card Registration', (2021) (accessible [here](#)).

<sup>58</sup> Women are more likely to lack formal proof of identification and therefore to face challenges in getting and registering a prepaid SIM card. Desai, Diofasa and Lu, 'The Global Identification Challenge: Who Are The 1 Billion People Without Proof Of Identity?', World Bank Blogs (2018) (accessible [here](#)).

<sup>59</sup> Privacy International, n 55.

<sup>60</sup> Nicola Jensch, 'Implications Of Mandatory Registration Of Mobile Phone Users In Africa', (2012) Telecommunications Policy (accessible [here](#)).

<sup>61</sup> Stephanie Kirchgaessner et al, 'Revealed: Leak Uncovers Global Abuse Of Cyber-Surveillance Weapon', The Guardian (2021) (accessible [here](#)).

legislation. As of 2019, only 43% of African countries had any form of data privacy laws, and only 5 countries had ratified the African Union Convention on Cyber Security and Personal Data Protection (known as the Malabo Convention).<sup>62</sup>

For example, in its Communications (Subscriber Identity Module and Mobile Device Registration) Regulations of 2021, Lesotho proposes a system wherein it is required for “everyone in that country using mobile phones to have their personal information stored with the Lesotho Communications Authority (LCA) [in a centralised database] and accessed by security agencies with ease without their consent.”<sup>63</sup>

This is despite evidence that SIM card registration programmes have little meaningful effect on organised crime or crime in general. In South Africa, agents registering the information collected to satisfy the SIM card registration law have no way to authenticate the information provided, and agents are not required to be vetted.<sup>64</sup> As a result, the information is notoriously inaccurate, and crime is not reduced. In fact, identity crimes and black markets have often increased.<sup>65</sup> These laws are also easily circumventable by producing false documents, trading phones, etc.

## **Surveillance**

Surveillance likewise remains a concern of growing importance in the discussion on freedom of expression online, as countries have increasingly sought out new technologies and equipment to enhance their surveillance capabilities.<sup>66</sup> In a number of African countries, additional surveillance capacities have been sought by the state within the past three years, including both legal and technological means for advanced interception of communications.

In Nigeria, executive budget documents indicate an amount of ₦5 billion (approximately \$12 million) allocated towards the purchase of surveillance-related equipment in 2020.<sup>67</sup> This is in a context in which CPJ has previously reported that the Nigerian military has used surveillance technologies to extract information from phones and computers to spy on ordinary Nigerians and the press, despite government assurances of its necessity solely for fighting terrorist groups.<sup>68</sup> Nigeria also instituted draft Lawful Interception of Communications Regulations in 2019, which enable interception both with and without a warrant under different circumstances, and require mobile phone companies to store voice and data communications for three years.<sup>69</sup>

Kenya has witnessed several concerning surveillance and interception regulations come into force recently, an example of the legislative means being used to advance surveillance on the continent. The Statute Law Miscellaneous Amendment Act, an amendment to the Official

---

<sup>62</sup> Privacy International, n 55.

<sup>63</sup> MISA Zimbabwe, ‘New Lesotho Regulations Violate Right to Privacy’, Kubatana.net (2021) (accessible [here](#)).

<sup>64</sup> Heidi Swart, ‘Missed Call: RICA Registration “Useless” for Crime Prevention Purposes’, Daily Maverick (2016) (accessible [here](#)).

<sup>65</sup> Privacy International, ‘101: SIM Card Registration’, (2019) (accessible [here](#)).

<sup>66</sup> Media Defence, n 5, p. 89.

<sup>67</sup> Abdul Abdulrahim, ‘Government Surveillance And Free Speech In Nigeria’, Stears (2021) (accessible [here](#)).

<sup>68</sup> Jonathan Rozen, ‘Nigerian Military Targeted Journalists’ Phones, Computers With “Forensic Search” For Sources’, CPJ (2019) (accessible [here](#)).

<sup>69</sup> Government Notice No. 23, ‘Lawful Interception of Communications Regulations, 2019’, Federal Republic of Nigeria (2019) (accessible [here](#)).

Secrets Act (Cap 187), was signed into law in December 2020. According to Access Now, it gives sweeping powers to the Cabinet Secretary of Interior and Coordination of National Security to “access data from any phone or computer and introduces hefty penalties for anyone who refuses to comply.”<sup>70</sup> The Act does not make it mandatory for the Cabinet Secretary to obtain a court order when seeking data, and the wording of the law does not require these surveillance powers to be used only to protect national security. There is evidence of surveillance technologies being abused in the past to spy on journalists, civil society and critics of the government,<sup>71</sup> raising concerns for these additional powers.

In Angola, a law that permits law enforcement to conduct electronic surveillance and location tracking with minimal oversight and in a wide range of circumstances came into force in May 2020.<sup>72</sup> Although it prohibits surveillance on political grounds or on the basis of discriminatory motivation, the law has raised concerns that it merely provides legal coverage for existing surveillance practices with little or no oversight.<sup>73</sup>

### Foreign surveillance technology

Many instances of domestic surveillance abuse rely on the importation of foreign surveillance technologies from countries in Europe, the United States and Asia. Reports indicate foreign surveillance software has been used in Togo to target priests and members of the opposition.<sup>74</sup> The software, allegedly created by Israeli firm NSO Group and which exploited a WhatsApp vulnerability to hack mobile phones, targeted individuals who had been known to be critical of President Faure Gnassingbé, and coincided with widespread protests against Gnassingbé for an attempt to extend term limits for the president.<sup>75</sup> The same software has reportedly been used in Kenya, Nigeria, Zambia and Zimbabwe as well.<sup>76</sup>

In Uganda, the Wall Street Journal reported in 2019 that Ugandan security officials had worked with Huawei technicians – embedded with cybersecurity forces in the country – to hack into opposition politician Robert Kyagulanyi’s (known popularly as Bobi Wine) phone,<sup>77</sup> under the guise of accusations of treason and attempted terrorism.<sup>78</sup>

Some of these practices appear to arguably conflict with the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa, which provides under principle 41 as follows:

<sup>70</sup> Bridget Andere, ‘Kenya’s Sneak Attack On Privacy: Changes To The Law Allow Government Access To Phone And Computer Data’, AccessNow (2021) (accessible [here](#)).

<sup>71</sup> Privacy International, ‘In Kenya, Communications Surveillance Is A Matter Of Life And Death’, (2017) (accessible [here](#)).

<sup>72</sup> Freedom House, ‘Freedom on the Net: Angola 2020’, (2020) (accessible [here](#)).

<sup>73</sup> *Ibid.*

<sup>74</sup> Radio France Internationale, ‘Togo Church Leaders In Crosshairs Of Israeli Spyware And WhatsApp Exploit’, AllAfrica (2020) (accessible [here](#)).

<sup>75</sup> *Ibid.*

<sup>76</sup> Marzak et al, ‘Running In Circles Uncovering The Clients Of Cyberespionage Firm Circles’, Citizen Lab (2020) (accessible [here](#)).

<sup>77</sup> Parkinson et al, ‘Huawei Technicians Helped African Governments Spy On Political Opponents’, Wall Street Journal (2019) (accessible [here](#)).

<sup>78</sup> Robert Ariaka, ‘Bobi Wine Faces Treason Charges’, New Vision (2018) (accessible [here](#)).

- “1. States shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person’s communications.
2. States shall only engage in targeted communication surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.
3. States shall ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy, including:
  - a. the prior authorisation of an independent and impartial judicial authority;
  - b. due process safeguards;
  - c. specific limitation on the time, manner, place and scope of the surveillance;
  - d. notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;
  - e. proactive transparency on the nature and scope of its use; and
  - f. effective monitoring and regular review by an independent oversight mechanism.”

One of the most significant developments in digital rights, and surveillance specifically, in Africa in recent years was the ruling by the Constitutional Court of South Africa in 2021 confirming a judgment by the High Court that declared various elements of the country’s surveillance law – the Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002 (RICA) – to be unconstitutional. In *amaBhungane Centre for Investigative Journalism and Another v Minister of Justice and Others*,<sup>79</sup> the Constitutional Court ruled that RICA failed to provide adequate safeguards to protect the right to privacy, as buttressed by the rights of access to courts, freedom of expression and the media, and legal privilege. The applicants, an investigative journalism centre and one of its founders, Sam Sole, approached the court when evidence emerged that Mr Sole had been subject to surveillance in the course of his work. While the court acknowledged the important purpose served by surveillance in combatting crime, protecting national security and maintaining public order, it found that there were insufficient safeguards in place to protect against abuse, and ruled that RICA be amended to allow for notification of a subject after they have been surveilled, to prescribe procedures to ensure that data obtained is managed lawfully and that measures be put in place to ensure the independence of the judge appointed to oversee communications interception. Notably, the judgment also held that RICA failed to provide special protections against abuse in the case of surveillance of lawyers and journalists, agreeing that by their nature both professions warrant additional protections to maintain legal privilege and the confidentiality of journalistic sources. Parliament now has three years from the date of judgment to amend RICA, which is a key opportunity to see positive legislative reform in the context of surveillance.

In another notable judgment, the High Court in Zimbabwe granted an order in 2020 interdicting the government, Econet Wireless Zimbabwe, and other respondents from implementing a police warrant seeking information on the mobile phone operator’s transactions.<sup>80</sup> MISA-Zimbabwe, along with Zimbabwe Human Rights Association (ZimRights), brought the application to prevent the police from seizing information on Econet’s platforms relating to the communications and activity of the two human rights organisations. The High Court granted the interdict, in addition to ordering Econet Wireless to strictly maintain the privacy and

---

<sup>79</sup> *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*, Constitutional Court of South Africa Case CCT278/19 & CCT279/19 (2021) (accessible [here](#)).

<sup>80</sup> MISA-Zimbabwe, ‘Court Grants Order In Favour Of MISA Against Econet Search Warrant’, (2020) (accessible [here](#)).



confidentiality of information in its possession relating to the applicants, their members and their employees. The High Court further ordered them not to divulge any of the relevant information to the respondents, namely the Minister of Home Affairs, Police Commissioner-General, Detective Inspector Mkhululi Nyoni and the Postal and Telecommunications Regulatory Authority of Zimbabwe.<sup>81</sup>

Progress has also been made in pressuring governments in the foreign states where these surveillance technologies are often produced to implement stricter export controls on such technologies. The European Union adopted a new regulation in March 2021 on exports of dual-use technologies by EU-based companies, requiring EU authorities to publicly provide detailed information about export licenses that have been approved or denied and the human rights risks associated with the applications for export technologies, as well as mandating countries to consider the risk of use “in connection with internal repression or the commission of serious violations of international human rights and international humanitarian law.”<sup>82</sup> However, the regulation has been criticised for not going far enough.<sup>83</sup>

### Digital identity programs

In the context of surveillance, the impetus towards implementing digital identity programs is potentially of concern. Kenya is one of many countries implementing digital identity programs with the justification of, among other things, tackling crime and terrorism and protecting national security. Critics argue, however, that:<sup>84</sup>

“Digital identity systems will only make governments more efficient at what they are already doing. If a government is currently using its identity systems to discriminate against minorities<sup>85</sup> and exclude them from power, then they will only become more efficient at that.”

Digital identity systems risk not only excluding already marginalised groups from public services but also being used as mechanisms of control against the media, civil society and political opponents, threatening freedom of expression.

It should also be noted that although the situation is rapidly evolving, many countries in the region still lack adequate data protection laws or have not fully implemented existing legislation, raising concerns for how data collected through digital identity programs is managed.

Research by the Media Policy and Democracy Project (MPDP) in Southern Africa has found that despite the existence of some constitutional and legislative privacy protections in most countries in the region, surveillance has continued and advanced unabated through the use

---

<sup>81</sup> *Ibid.*

<sup>82</sup> Access Now et al, ‘Human Rights Organizations’ Response To The Adoption Of The New EU Dual Use Export Control Rules’, (2021) (accessible [here](#)).

<sup>83</sup> *Ibid.*

<sup>84</sup> Nanjala Nyabola, ‘National Digital ID Initiatives Have A Trust Problem’, Rest of World (2021) (accessible [here](#)).

<sup>85</sup> See Abdi Latif Dahir, ‘Kenya’s New Digital IDs May Exclude Millions Of Minorities’, New York Times (2020) (accessible [here](#)).

of new technologies and the use of national security justifications to implement invasive digital surveillance programs:

“Across the region, governments appear to be exercising intrusive spying powers with insufficient limitations or safeguards. In particular, communications metadata (information about a person’s communications, rather than the content of their communications) is left with little legal protection. In several countries, the state’s surveillance powers are not subject to approval by a judge, eschewing the most basic standard for independent oversight. In some parts of the region, governments have exercised these intrusive powers with no legal framework in place; others have legal frameworks full of overlaps, conflicts and blind spots. Above all, irrespective of strengths or weaknesses in legal framework, a pattern emerges across the region: states have used their surveillance powers for antidemocratic purposes.”<sup>86</sup>

By way of example, Mozambique has installed public security cameras and implemented the compulsory registration of SIM cards, efforts which are seen to “substantiate citizens’ perceptions that the state is using them to spy on citizens” rather than for the purpose of guaranteeing security or fighting crime and insurgency.<sup>87</sup>

In Angola, the research found that “there is near paranoia about the issue of digital surveillance” as evidenced by the accusation by Isobel dos Santos that the famous ‘Luanda Leaks’ – a series of revelations about corruption in the highest levels of government in the former administration – were obtained not by the hacker, Rui Pinto, as claimed, but rather by Angola’s security services through a digital surveillance operation.<sup>88</sup>

In Zimbabwe, surveillance has been driven by the military, a practice that is not provided for in the Constitution and which raises concerns about the process being politicised and threatening human rights.<sup>89</sup> Further, the country has developed close links with China and there are indications that data and technology are being shared between the two countries.<sup>90</sup>

### **Public Order Laws**

Nevertheless, some muted progress has been made in challenging national security justifications for limitations on rights by litigating historical ‘public order’ statutes, many of which are based on colonial or pre-independence laws. In South Africa, for example, the Constitutional Court of South Africa in 2020 found part of the Riotous Assemblies Act inconsistent with the constitutional protections for freedom of expression and invalid insofar as it provided for criminal sentences for the incitement of a person to commit an offence, and punished incitement with the same severity as a person who committed a crime.<sup>91</sup> This ruling may have implications for national security justifications of restrictions on freedom of expression and online content restriction laws more broadly, particularly as it pertains to sentences. To the extent that public order laws are increasingly being used to suppress freedom of speech online, digital rights litigators should consider strategies for challenging

---

<sup>86</sup> Hunter and Mare, ‘A Patchwork For Privacy: Mapping Communications Surveillance Laws In Southern Africa’, MPDP (2020) (accessible [here](#)).

<sup>87</sup> Nhanale, ‘Electronic Surveillance In Mozambique: The Risks And Suspicions In A Context of Authoritarianism And Military Conflict’, MPDP (2021) (accessible [here](#)).

<sup>88</sup> Verde, ‘Words and Actions: A Realistic Enquiry Into Digital Surveillance In Contemporary Angola’, MPDP (2021) (accessible [here](#)).

<sup>89</sup> Munoriyarwa, ‘The Growth Of Military-Driven Surveillance In Post-2000 Zimbabwe’, MPDP (2021) (accessible [here](#)).

<sup>90</sup> *Ibid.*

<sup>91</sup> Nomahlubi Sonjica, ‘Riotous Assemblies Act Inconsistent With Freedom Of Expression: Constitutional Court’, Sowetan Live (2020) (accessible [here](#)). The Constitutional Court only dealt with incitement insofar as it pertains to sentencing in section 18(2) of the Riotous Assemblies Act; the actual offence of incitement – contained in section 17 – was not challenged.

these laws as outdated and incompatible with modern democracies and understandings of the right to freedom of expression.

### ***Facial Recognition Technology***

Finally, an additional new threat to freedom of expression under the auspices of protecting national security and maintaining public order, and which is increasingly prevalent across Africa, is that of facial recognition technology (FRT) and surveillance cameras. Governments frequently justify their use by hailing cameras' crime-fighting abilities. Furthermore, in some places, facial recognition is implemented by the private sector instead of government itself. In South Africa, FRT cameras have been likened to the apartheid-era pass laws.<sup>92</sup> By seeking to 'filter' who may access certain neighbourhoods, being used as a justification to harass people, and targeting protestors, such cameras have the potential to do significant damage to human rights. In addition, there is little evidence, other than anecdotally, that such cameras are effective in fighting crime.<sup>93</sup> Evidence does show, however, that such technologies displace crime to other, usually poorer neighbourhoods, whose residents cannot afford similar private services, and place certain groups under greater official scrutiny.<sup>94</sup>

There are indications that other African countries are similarly implementing widespread FRT or surveillance cameras. Kenya, for example, has launched an FRT program involving the installation of thousands of cameras, also using license plate recognition technology, along major roads and highways and at the country's borders.<sup>95</sup> The cameras have been criticised not only for being ineffective in deterring crime, but also for the fact that police do not have to seek judicial authorisation or consent to conduct surveillance using the cameras. There have also been examples of protestors being arrested after or during protests in Nairobi, raising the prospect of their being used for mass surveillance of protests.<sup>96</sup>

Botswana deployed smart closed-circuit television (CCTV) cameras in 2019 and the Botswana Police Service signed a Memorandum of Understanding with Huawei in 2018 to deploy CCTV surveillance cameras through the Safe City projects.<sup>97</sup> Zambia has been reported to have done the same in 2019.<sup>98</sup> Surveillance cameras installed in Angola's capital Luanda are equipped with facial recognition technology, and concerns have been raised that a law that came into effect in January 2020 allowing the installation exempts security agencies from many of the provided safeguards.<sup>99</sup>

Research by MPDP found that the use of security camera systems in each of South Africa, Zimbabwe, Botswana and Angola was "headed in the same direction: AI-powered

---

<sup>92</sup> Carien du Plessis, 'Why Johannesburg's Anti-Crime Cameras Are Similar To Apartheid-Era Pass Laws - Expert', News24 (2021) (accessible [here](#)).

<sup>93</sup> Ratcliffe and Groff (2018) in a robust empirical study find no impact of CCTV surveillance on violent street felonies and disorder incidents (accessible [here](#)). For more, see Jane Duncan, 'How CCTV Surveillance Poses A Threat To Privacy In South Africa,' The Conversation (2018) (accessible [here](#)).

<sup>94</sup> Jane Duncan, n 93 and Doyle et al, 'Eyes Everywhere: The Global Growth Of Camera Surveillance', (2012) (accessible [here](#)).

<sup>95</sup> International Network of Civil Liberties Organisations, 'In Focus: Facial Recognition Tech Stories And Rights Harms From Around The World', (2021) (accessible [here](#)).

<sup>96</sup> *Ibid.*

<sup>97</sup> Paradigm Initiative, 'LONDA: Digital Rights and Inclusion in Africa 2020', (2021) at p. 10 (accessible [here](#)).

<sup>98</sup> Lusaka Times, 'Huawei to Plant 24 Hour Cameras Across Lusaka', (2019) (accessible [here](#)).

<sup>99</sup> Freedom House, n 72.

surveillance, with features like facial recognition and a variety of other video analytics, often with the assistance of international industrial partners, in particular from China.”<sup>100</sup>

## ***Opportunities for Litigation***

Litigation is critical to ensure that surveillance and content restriction activities undertaken under the guise of law enforcement activities meet the three-part test for a justifiable limitation. There may therefore be scope for legal challenges to such initiatives under the three-part test on the grounds that such efforts are neither necessary, because they are ineffective, nor proportional, since they are a mass surveillance technique.

### **The three-part test for the justifiability of a limitation on rights**

The revised Declaration of Principles on Freedom of Expression and Access to Information in Africa reaffirms the position that states may only limit the exercise of the rights to freedom of expression and access to information if the limitation:<sup>101</sup>

- a. is prescribed by law;
- b. serves a legitimate aim; and
- c. is a necessary and proportionate means to achieve the stated aim in a democratic society.

The Declaration also goes further in stating that any law that limits the rights to freedom of expression and access to information must be clear, precise, accessible and foreseeable, amongst other requirements. This provides a solid foundation for challenging various laws with vague and broad provisions that are abused by governments to limit freedom of expression online. As will become clear in this report, this is a common occurrence with national security, hate speech, and cybercrimes legislation as well as regulations relevant to media freedom.

The Declaration further provides specific guidelines on what constitutes a legitimate aim and necessary and proportionate action.

Concerning the use of imported surveillance technology, it is worth noting that another Israeli company known for producing and exporting surveillance equipment, Cellebrite, is facing a court battle in Israel over the firm’s exports to Hong Kong, where security forces have used the software in violent crackdowns against pro-democracy protestors.<sup>102</sup> Cellebrite technology has also reportedly been used by authorities in Botswana to search reporters’ phones and expose their sources.<sup>103</sup> Digital rights litigators may therefore consider efforts that target

<sup>100</sup> Swart and Munoriyarwa, ‘Video Surveillance In Southern Africa: Case Studies Of Security Camera Systems In The Region’, MPDP (2020) (accessible [here](#)).

<sup>101</sup> Principle 9 of the African Declaration, n 2.

<sup>102</sup> Patrick Howell O’Neill, ‘Israeli Phone Hacking Company Faces Court Fight Over Sales To Hong Kong’, MIT Technology Review (2020) (accessible [here](#)).

<sup>103</sup> Jonathan Rozen, ‘Botswana Police Use Israeli Cellebrite Tech To Search Another Journalist’s Phone’, CPJ (2021) (accessible [here](#)).

companies in their home jurisdictions to hold them accountable for human rights violations resulting from the sale of their equipment elsewhere.

There may also be opportunities to litigate SIM card registration programs on the grounds that they are both unnecessary and disproportionate. In addition, such laws may be challenged under data protection regulations on the grounds that the collection of the information is excessive and not adequately protected, although many data protection frameworks exclude national security from their ambit of application, thereby creating a tension regarding the protection of personal information.

The *amaBhungane* judgment regarding the constitutionality of RICA provides a solid foundation for other African countries to pursue litigation challenging the adequacy of security safeguards put in place to protect against the abuse of surveillance and interception laws. Research has shown that not only do many countries lack any such protections, even those which do, in theory, often fail to abide by them in the practice of national surveillance programs. The Constitutional Court's willingness to include user-notification as part of its remedy, as well as the specific safeguards in respect of the surveillance of lawyers and journalists, are key protections that may be developed in other jurisdictions as well.

Other litigation strategies may be available in questions of national security laws as well. In the case of Kenya's Statute Law Miscellaneous Amendment Act, there has been criticism that the state used an omnibus bill to sneak in substantive changes to the law without adequate public participation, not the first time such a critique has been levelled against the government in recent years.<sup>104</sup> This raises the prospect of using public participation laws and constitutional provisions (in the case of Kenya, and likely other countries) to challenge problematic laws where appropriate. This argument was applied in the case of *Nubian Rights Forum and Others v Attorney-General of Kenya and Others* challenging the legality of the implementation of the National Integrated Identity Management System (NIIMS), although the Court found that appropriate public participation procedures had been followed in this case.<sup>105</sup>

Finally, international law and regional human rights instruments can provide further grounding on which to challenge infringements on the basis of national security. National security is indeed a legitimate restriction on fundamental rights and freedoms in the ICCPR<sup>106</sup> and the African Charter,<sup>107</sup> but these instruments provide careful protections against misuse. While the African Charter does not contain an explicit national security justification for limitations on freedom of expression, article 9 does state that it is to be exercised "within the law" and article 29(3) states that an individual has a general duty "not to compromise the security of the State whose national or resident he is."<sup>108</sup> The African Declaration goes further in stating that "freedom of expression shall not be restricted on public order or national security grounds unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression."<sup>109</sup> Fora such as state-reporting to the UN Human Rights Committee and the ACHPR should be encouraged, as recommendations from

---

<sup>104</sup> Bridget Andere, n 70.

<sup>105</sup> *Nubian Rights Forum and Others v Attorney-General and Others*, High Court of Kenya at Nairobi, Consolidated Petitions No. 56, 58 & 59 of 2019 (2019) at para. 1023-1026 (accessible [here](#)).

<sup>106</sup> Articles 19, 21 and 22 of the ICCPR.

<sup>107</sup> Articles 3, 11, 12 and 27 of the African Charter.

<sup>108</sup> *Ibid.*

<sup>109</sup> Principle 22(5) of the African Declaration, n 2.

such bodies may indeed trigger law reform processes domestically or be catalysed for litigation.

Litigators should keep track of the growing trend in the context of COVID-19 of digital identity systems expanding even further into the domain of ‘digital vaccine passports’. Although there is little evidence as yet of countries in the region implementing such systems, rollout in other parts of the world is proceeding swiftly, with major consequences for online privacy and freedom of expression. In Singapore, the government reneged on a promise not to share information collected during the pandemic for public health reasons with police for surveillance purposes.<sup>110</sup> Defenders of freedom of expression in Africa should consider the consequences of COVID-19 management legislation, including digital tracking and vaccine passports, and evaluate the opportunities and necessity for litigation to defend digital rights in this regard.

### III. Laws restricting online content and access

The 2018 report found that all the countries under review had made use of content restrictions in some way in recent years. While the nature and justifiability of the restrictions varied – in South Africa, for example, there appear to have been some legitimate efforts to prevent hate speech against minorities<sup>111</sup> – in others, laws have been viewed as thinly veiled attempts to stifle free speech, such as the Hate Speech Bill in Nigeria,<sup>112</sup> which prescribes a life sentence or the death sentence for propagating hate speech.<sup>113</sup>

As mentioned above in the discussion on surveillance, countries are increasingly installing technologies that enable the interception of online communication as a way of controlling access and content. The original report noted that among the various ways in which online speech is controlled, content restrictions were a particular trend in East Africa. In Tanzania, for example, online content is strictly regulated through the Electronic and Postal Communications (Online Content) Regulations of 2018.<sup>114</sup> In Kenya, misinformation and bots targeted those believed to align with the opposition during the 2017 election; the Communications Authority of Kenya sought the powers to monitor calls and text messages and to monitor and restrict political messages being sent; and licences were required to post videos online, even on social media.<sup>115</sup>

Some of the Kenyan content restrictions were challenged in July 2019 when a constitutional challenge was brought against 24 separate laws that had been passed by the Kenyan National Assembly without the involvement of the Senate, contrary to the Constitution which creates a bicameral legislature. The High Court voided a number of the laws that had been passed, including the Computer Misuse and Cybercrimes Act, Kenya’s principal ICT legislation.<sup>116</sup> However, the ruling was suspended for nine months to give parliament time to rectify the situation. In the meantime, a separate constitutional challenge was launched in 2017 against

<sup>110</sup> Andrew Illmer, ‘Singapore Reveals Covid Privacy Data Available To Police’, BBC News (2021) (accessible [here](#)).

<sup>111</sup> The Prevention and Combatting of Hate Crimes and Hate Speech Bill in South Africa (accessible [here](#)), flagged as a potentially chilling piece of legislation, remains under consideration in the National Assembly.

<sup>112</sup> Media Defence, n 5, p. 65 and 88.

<sup>113</sup> Oyewole Oladapo and Ayo Ojebode, ‘Nigeria Digital Rights Landscape Report’, Institute of Development Studies (2021) at p. 159 (accessible [here](#)).

<sup>114</sup> *Ibid* at page 16.

<sup>115</sup> Media Defence, n 5, p. 24-6.

<sup>116</sup> Paradigm Initiative, n 97, p. 52.

the section of the Act which penalised the publication of false information with up to ten years in prison.<sup>117</sup> That case was decided in February 2020, when the High Court ruled that the Act was indeed constitutional and upheld the contested provisions.

This section reviews developments in the area of laws regulating the posting of online content, such as hate speech legislation, and other more indirect methods of controlling online content, such as the use of taxes on social media or internet access and social media monitoring tools, in addition to legislation specifically regulating the use of social media or the posting of misinformation online. Finally, it addresses developments in the related areas of broadcast and film as well as the concept of net neutrality to evaluate new ways in which access to online content is increasingly restricted.

### ***Hate Speech Legislation***

As the case of Nigeria demonstrates, and as was reflected in the 2018 report,<sup>118</sup> rather than protecting human rights, hate speech legislation can instead be used as a tool to stifle dissent. Nigeria's Hate Speech Bill (formally, the National Commission for the Prohibition of Hate Speech Bill) has been criticised for giving authorities arbitrary powers to punish critical speech on the internet.<sup>119</sup> Section 4, in particular, threatens freedom of expression through the vague and broad wording of behaviour it prohibits, defined as abusive, threatening and insulting behaviour, and the bill further prescribes the death penalty for anyone found guilty of spreading a falsehood that leads to the death of another person.<sup>120</sup>

By way of additional examples, both Ethiopia and Tanzania introduced hate speech regulations recently. In the case of Ethiopia, the Hate Speech and Disinformation Prevention and Suppression Proclamation<sup>121</sup> passed in 2020, and while having seemingly well-intentioned objectives, has been decried by civil society as a threat to freedom of expression and access to information online.<sup>122</sup> In addition to "having overbroad and ambitious definitions that are subject to misinterpretation and abuse," the law introduced harsh penalties that are generally seen to be contrary to international human rights law and article 9 of the African Charter.<sup>123</sup> The law also holds intermediaries liable for policing content, requiring them to remove offending content within 24 hours of receiving a notification.<sup>124</sup>

In the case of Tanzania, the Online Content Regulation of 2020, in addition to regulating the publication of online content services outside of private communications through applications for licenses, also prohibits content harming the "reputation prestige or status" of Tanzania.<sup>125</sup>

---

<sup>117</sup> Freedom House, 'Freedom On The Net: Kenya 2020', (2020) (accessible [here](#)).

<sup>118</sup> Media Defence, n 5, p. 26.

<sup>119</sup> Amnesty International, 'Nigeria: Bills On Hate Speech And Social Media Are Dangerous Attacks On Freedom Of Expression', (2019) (accessible [here](#)).

<sup>120</sup> QueenEsther Iroanusi, 'Explainer: Important Things To Know About Nigeria's "Hate Speech" Bill', Premium Times (2019) (accessible [here](#)).

<sup>121</sup> Hate Speech and Disinformation Prevention and Suppression Proclamation, Federal Negarit Gazette of the Federal Democratic Republic of Ethiopia (2020) (accessible [here](#)).

<sup>122</sup> Edrine Wanyama, 'Ethiopia's New Hate Speech And Disinformation Law Weighs Heavily On Social Media Users And Internet Intermediaries', CIPESA (2020) (accessible [here](#)).

<sup>123</sup> *Ibid.*

<sup>124</sup> *Ibid.*

<sup>125</sup> Paradigm Initiative, n 97, p 106.

As these examples demonstrate, concerns with hate speech regulation are often raised when legislation is vague, leaving it open to abuse for political or other reasons. South African courts reflected on this question recently in the case of *Qwelane v South African Human Rights Commission and Another* in 2019.<sup>126</sup> Mr Qwelane, who at the time was serving as South Africa’s ambassador to Uganda, had published a column in a local newspaper disparaging the “lifestyle and sexual preferences” of homosexuals. The High Court found that the statement constituted hate speech as defined in the Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000 (Equality Act), section 10 of which prohibits the publishing of hurtful statements that cause harm or spread hate.

Mr Qwelane then sought to have section 10 of the Equality Act declared unconstitutional on the basis that it infringed on the right to freedom of expression. In 2019, the SCA agreed the section was unconstitutional because it “extends far beyond the limitations on freedom of expression provided for in the Constitution and is in many respects is unclear.”<sup>127</sup> The SCA deemed the section’s use of the word “hurtful” particularly vague, adding that all definitions of the word “are concerned with a person’s subjective emotions... in response to the actions of a third party. This does not equate with causing harm or incitement to harm.”

In July 2021, the Constitutional Court held that section 10 of the Equality Act was unconstitutional to the extent that it included the word “hurtful” as part of the threshold requirement for hate speech.<sup>128</sup> Furthermore, it concluded that Mr Qwelane’s statements did amount to hate speech, describing hate speech as “one of the most devastating modes of subverting the dignity and self-worth of human beings”.<sup>129</sup>

### **Social Media and Internet Taxes**

The 2018 report also noted the growing trend of tax and licensing rules for social media, such as the ‘social media tax’ in Uganda and new rules on bloggers in Tanzania and Kenya.<sup>130</sup> In Uganda, evidence has since emerged that the social media tax implemented in 2018 forced more than 5 million users off the internet (pushing internet penetration from 47% to 35%) in just three months, with severe consequences not only for freedom of expression but likewise for education, financial inclusion and economic growth.<sup>131</sup> After the initiative’s clear failure, the Ugandan government announced it was considering repealing the ‘over-the-top tax’ in 2021 and replacing it with an additional 12% levy on internet data, with exemptions only for the purchase of medical and educational services, an effort that is likely to have equally devastating effects on digital inclusion and freedom of expression.<sup>132</sup> Kenya also initiated a new effort in June 2021 to increase the rate of excise duty on telephone and data services

---

<sup>126</sup> *Qwelane v South African Human Rights Commission and Another*, Supreme Court of Appeal of South Africa, Case No. 686/2018 (2018) (accessible [here](#)).

<sup>127</sup> *Ibid*.

<sup>128</sup> *Qwelane v South African Human Rights Commission and Another*, Constitutional Court of South Africa, Case No. CCT 13/20 (2021) (accessible [here](#)).

<sup>129</sup> *Ibid* at para. 1.

<sup>130</sup> Media Defence, n 5, p. 29, 32 and 38.

<sup>131</sup> Juliet Nanfuka, ‘Social Media Tax Cuts Ugandan Internet Users By Five Million, Penetration Down From 47% to 35%’, CIPESA (2019) (accessible [here](#)).

<sup>132</sup> Fred Ojambo, ‘Uganda Considers New Internet Tax As Social Media Levy Fails’, (2021) (accessible [here](#)).



from 15% to 20%<sup>133</sup> and implemented a Digital Services Tax, effective as of 1 January 2021, of 1.5% of the total value of business services rendered through online platforms.<sup>134</sup>

Since 2018, several other countries have likewise initiated efforts to tax internet or social media usage. Nigeria reintroduced the Communication Service Tax Bill in 2019, which had previously failed to pass the National Assembly due to opposition from stakeholders, but which has now successfully passed the first reading.<sup>135</sup> The Bill would require consumers to pay a 9% tax on voice calls, data consumption, SMS, MMS and Pay-TV, with serious consequences for internet access throughout the country. Ghana was one of the first countries to implement such a tax in 2008, and further revised it upwards from 6% to 9% in 2019,<sup>136</sup> causing telecommunication companies to shift the additional cost on to consumers.

Cameroon also introduced a tax of 19,25% on any advertising on Facebook under the 2020 Finance Law, which is expected to be expanded soon to other platforms like Google and Amazon.<sup>137</sup> In addition, the Ministers of Finance and of Post and Telecommunication signed a joint decision in March 2020 setting out the modalities for the electronic collection of customs duties and taxes on phones, tablets, terminals and software, but after attracting widespread criticism the decision was overturned by a letter from the President.<sup>138</sup> Benin also introduced a levy on some internet service in 2018 but backtracked after a backlash from citizens.<sup>139</sup>

A 2019 review by APC of recent initiatives in Uganda, Kenya and Tanzania to tax the internet through excise duties on access or use concluded that Tanzania's licence-related fees for online content services constituted a violation of international human rights norms and standards because the fees imposed were so high that they would render the cost of posting content online unaffordable for the vast majority of Tanzania's people.<sup>140</sup> Likewise, the Ugandan excise duty on 'over-the-top services' was also found to be a violation, though Kenya's excise duty on internet data services was not due to the fact that the increase in price was unlikely to hinder access to and/or use of the internet for Kenya's people.<sup>141</sup> This approach is in line with the African Declaration, which provides that economic measures on internet services should not undermine universal, equitable, affordable, and meaningful access to the internet.<sup>142</sup>

The conclusion of the original report on social media taxes – that they are unlikely to pass muster on the three-part test if appropriately challenged before the courts – still stands. Unfortunately, there have been few conclusive instances of litigation tackling such taxes in Africa, although, fortunately, public pushback has been successful in some cases.

## **Social Media Monitoring**

---

<sup>133</sup> Susan Nyawira, 'Cost Of Data, Calls Could Go Up If New Tax Amendment Is Passed', *The Star* (2021) (accessible [here](#)).

<sup>134</sup> KPMG, 'Kenya: Digital Services Tax Regulations Provide Details; Scheduled Effective Date Of 2021', (2020) (accessible [here](#)).

<sup>135</sup> Wole Olayinka, 'How A Proposed Bill Could Increase Internet Costs In Nigeria', *TechCabal* (2019) (accessible [here](#)).

<sup>136</sup> *Ibid.*

<sup>137</sup> Paradigm Initiative, n 97, p. 16.

<sup>138</sup> *Ibid.*

<sup>139</sup> Internet Sans Frontières, 'Bénin: Government Repeals Social Media Tax – Internet Sans Frontières', (2018) (accessible [here](#)).

<sup>140</sup> Justine Limpitlaw, 'Human Rights Impacts of Taxing Popular Internet Services', APC (2019) (accessible [here](#)).

<sup>141</sup> *Ibid.*

<sup>142</sup> Principle 37(2) of the African Declaration, n 2.

The 2018 report noted that “surveillance and the monitoring of social media has also been prevalent in the countries under review, without adequate safeguards to ensure the protection of freedom of expression and privacy.”<sup>143</sup> The enforcement mechanisms occasioned by the COVID-19 pandemic have only accelerated this practice, with potentially significant consequences for the regulation of online content in the future.

Early in the pandemic, South Africa, for example, published regulations making it an offence to publish any disinformation, through any medium, about COVID-19,<sup>144</sup> and Namibia did the same in April 2020.<sup>145</sup> In both cases, the regulations required that, in order to fall foul of the provision, the person publishing false information must have the intention to deceive in connection with the COVID-19 pandemic.<sup>146</sup>

Multiple countries issued regulations or declarations that social media would be monitored to deter the sharing of mis- and/or disinformation about COVID-19, such as Cameroon.<sup>147</sup> In Ethiopia, several journalists were arrested in the immediate aftermath of the declaration of a state of emergency, ostensibly for publishing false information about the pandemic.<sup>148</sup> In Ghana, the Establishment of Emergency Communications System Instrument was adopted in 2020 under section 100 of the Electronic Communications Act in response to the pandemic, which requires network operators and other communications services providers to provide subscriber information to the National Communications Authority and other state agencies when requested, including caller and called numbers, merchant codes, mobile station international subscriber directory number codes, international mobile equipment identity codes and site locations, roaming files and location log files.<sup>149</sup>

However, it must be noted that social media monitoring is not solely conducted under the auspices of pandemic-management. In Nigeria, the National Communications Commission recommended in 2019 that all organisations operating in the country “install social media monitoring devices or set up a monitoring team to avoid being implicated by the social media activities of their employees.”<sup>150</sup>

### ***Mis- and/or disinformation***

In addition to monitoring, the past few years have seen the rise of so-called ‘social media bills’, legislation specifically designed to control speech on social media platforms under the guise of limiting ‘gossip’, hate speech or misinformation.

In Nigeria, the notorious Protection from Internet Falsehood and Manipulation Bill, 2019, known as the ‘social media bill’, resurfaced in the wake of the #EndSARS protests of 2020 against police brutality. The bill criminalises the sharing of information that can diminish public

---

<sup>143</sup> Media Defence, n 5, p. 66.

<sup>144</sup> Republic of South Africa Government Gazette, ‘Regulations Issued In Terms Of The Disaster Management Act 57 of 2002 (2020)’ at regulation 11 (accessible [here](#)).

<sup>145</sup> Paradigm Initiative, n 97, p. 65.

<sup>146</sup> Government of South Africa, ‘Disaster Management Act: Regulations Relating To COVID-19’, Government Notice 318 of 2020 at section 11(5) (2020) (accessible [here](#)); Amanda Manyame, ‘Fake News About COVID-19 Now A Crime In Namibia’, EndCode (2020) (accessible [here](#)).

<sup>147</sup> Paradigm Initiative, n 97, p. 16.

<sup>148</sup> Human Rights Watch, ‘Ethiopia: Free Speech At Risk Amid Covid-19’, (2020) (accessible [here](#)).

<sup>149</sup> Paradigm Initiative, n 97, p. 48.

<sup>150</sup> Oyewole Oladapo and Ayo Ojebode, n 113, p. 159.

confidence in the performance of any duty or function of, or in the exercise of any power of, the Nigerian government, and criminalises the operation of parody accounts on social media.<sup>151</sup> Despite not yet being passed, the bill has already been used to arrest a Nigerian university student for operating on Twitter a parody account in the name of former President Goodluck Jonathan.<sup>152</sup>

Notably, research has shown that the Nigerian government itself is highly active in online manipulation and spreading misinformation on social media.<sup>153</sup> In November 2020, the Digital Forensic Research Lab (DFRL) released a report finding that influencer and sockpuppet Twitter networks were amplifying pro-government content in a concerted campaign targeting activists in the days and weeks after the protests.<sup>154</sup> #EndSARS was an extensive grassroots movement protesting the violent tactics used predominantly by the notorious Special Anti-Robbery Squad, but also the police more broadly. Protests sprung up nationwide but mainly in the largest city, Lagos, and attracted a brutal crackdown from the military and police. DFRL's research showed that a coordinated network was producing content centrally for distribution on Twitter through two networks of pro-government accounts, one mainly comprised of recently created grassroots sockpuppet accounts, and another of high follower paid influencers.<sup>155</sup>

To add insult to injury, when Nigerian activists attempted to upload content to Facebook and Instagram in support of the protests, posts were blocked by the social media companies as 'fake news.'<sup>156</sup> This highlights the additional challenge of content restrictions faced by users in countries in which global social media companies do not have a meaningful presence and from which they employ few content moderators who can understand the local context. Facebook later confirmed that the #EndSARS hashtag had been incorrectly flagged.<sup>157</sup>

Zimbabwe has also grappled with the regulation of online content in recent months, and especially in the context of the pandemic, with multiple incidents indicating a turn towards harsher punishment for those found to be propagating misinformation on social media. The case of Hopewell Chin'ono is instructive in this regard. Chin'ono, a renowned Zimbabwean journalist, was arrested multiple times in late 2020 and early 2021,<sup>158</sup> reportedly being charged with "communicating falsehoods" in relation to his reporting of COVID-19 lockdown measures and other corruption stories. Chin'ono was acquitted by the High Court, which found that the law under which he had been charged, section 31 of the Criminal Law (Codification and Reform Act) which deals with "publishing or communicating false statements prejudicial to the State", had been expunged by the Constitutional Court and no longer existed in Zimbabwean law.<sup>159</sup> Chin'ono's trial on separate charges of incitement to public violence nevertheless went ahead in May 2021,<sup>160</sup> and other people continue to be charged under the impugned law.<sup>161</sup>

---

<sup>151</sup> *Ibid* at p. 153.

<sup>152</sup> *Ibid* at p. 153.

<sup>153</sup> Oyewole Oladapo and Ayo Ojebode, n 113, p. 159-160.

<sup>154</sup> DFRL, 'Nigerian Government-Aligned Twitter Network Targets #EndSARS Protests', (2020) (accessible [here](#)).

<sup>155</sup> *Ibid*.

<sup>156</sup> David Gilbert, 'Facebook And Instagram Are Censoring Protests Against Police Violence In Nigeria,' Vice World News (2020) (accessible [here](#)).

<sup>157</sup> *Ibid*.

<sup>158</sup> The Guardian, 'Zimbabwe Journalist Hopewell Chin'ono Arrested For Third Time In Six Months', (2021) (accessible [here](#)).

<sup>159</sup> Fazila Mahomed, 'Zimbabwean Journalist Hopewell Chin'ono Faces Another Court Battle', Daily Maverick (2021) (accessible [here](#)). This section of the law was declared unconstitutional in *Chimakure v Attorney General* in 2014 (accessible [here](#)).

<sup>160</sup> Frank Chikowore, 'Hopewell Chin'ono: Zimbabwean Journalist on Trial For ... What Precisely?', Daily Maverick (2021) (accessible [here](#)).

<sup>161</sup> The Citizen, 'Couple Detained For Claiming Mnangagwa Died Of Covid-19', (2021) (accessible [here](#)).

Seeking to tackle misinformation and/or disinformation on social media is an important and laudable goal in today's society, and where such information is so egregious that it meets the definitional elements of hate speech or other crimes, legislation can be necessary. However, such legislation frequently oversteps the bounds of protecting freedom of expression, and it is concerning that there appears to be a clear trend in East, West and Southern Africa regarding shifting narratives to criminalise this content without appropriate safeguards being put in place.

In Zambia, for example, the Minister of Transport and Communication stated in March 2020 that the Zambian government intends to legislate against the creation and propagation of fake news, noting that fake news is dangerous and threatens the country's development.<sup>162</sup> There have also been shifting attitudes within the South African Police Services (SAPS) regarding disinformation, with some SAPS members having noted that the publication, distribution, disclosure, transmission, circulation or spreading of false information or fake news is an offence, whereas others cautioned the public against the incessant promotion and distribution of malicious untruths that seek to sow panic and pandemonium amongst communities.<sup>163</sup>

Perhaps the best illustration of this shifting narrative is the resolution of the 40<sup>th</sup> Ordinary Summit of the Southern African Development Community (SADC), which urged member states to "take pro-active measures to mitigate external interference, the impact of fake news and the abuse of social media, especially in electoral processes."<sup>164</sup> These examples point to the likelihood of other countries attempting to pass and implement false news or social media bills in the immediate future.

---

<sup>162</sup> Lusaka Times, 'Communication Minister Plans To Introduce A Statutory Instrument To Deal With Fake News And Online Insults', (2020) (accessible [here](#)).

<sup>163</sup> South African Police Service, 'Media Statement: Office Of The Provincial Commissioner Gauteng', (2020) (accessible [here](#)).

<sup>164</sup> SADC, 'Communiqué Of The 40<sup>th</sup> Ordinary Summit Of SADC Heads Of State And Government', (2020) (accessible [here](#)).

## Legislative responses to misinformation

Media Monitoring Africa (MMA) has highlighted three main concerns with using legislation to police misinformation online:<sup>165</sup>

- First, efforts to legislate mis- and disinformation tend to be used to limit more than disinformation but cater, intentionally or unintentionally, to greater incursions on freedom of expression, arguably making the problem worse.
- Second, legislation is often slow, and in most instances seeks to punish or deal with offenders who transgress the law. It is not always catered at addressing systemic issues such as access to information and media and information literacy.
- Thirdly, and most importantly, the problem is bigger than any single government, and while states have a critical role to play, they alone are unlikely to meaningfully address the core issues. A multi-stakeholder and multi-disciplinary approach, which includes the state, regional and international bodies, social media platforms, the media, and civil society, is likely to be more effective.

An attempt at such a multi-disciplinary approach was made in South Africa when Facebook was summoned to appear before South Africa's Parliament in May 2021 to speak to its plans for mitigating the spread of mis- and dis-information in the run-up to local government elections to be held in October 2021.<sup>166</sup> This meeting would have been the first of its kind on the continent. However, after initially agreeing to meet, Facebook subsequently withdrew citing the fact that other tech companies invited had not agreed to attend.<sup>167</sup>

### **Content Regulation in Broadcast and Film**

Other types of content regulation have also appeared across Africa in recent years, including in the more traditional arena of broadcast and film in which public bodies with the power to regulate content have flexed their muscles. The Kenyan film, *Rafiki*, despite being the first Kenyan film to premiere at Cannes, was banned in Kenya in 2018 due to the depiction of homosexual content.<sup>168</sup> The director, Wanuri Kahui, sued the Kenyan Film and Classifications Board, which had issued the ruling, on the grounds that the banning was a violation of her constitutional rights, as well as arguing that the ban would prevent the film from being considered for the Oscars. The High Court issued a temporary injunction, allowing *Rafiki* to be screened for the minimum seven days required to be eligible for the Oscars, but in April 2020 the High Court of Kenya in Nairobi confirmed the ban on content relating to same-sex relations imposed by the Kenya Film Classification Board.<sup>169</sup> This decision has received criticism for limiting freedom of expression and restricting content.<sup>170</sup>

<sup>165</sup> Media Monitoring Africa, 'Submission By Media Monitoring Africa To The UN Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression: Disinformation Report', (2021) (accessible [here](#)).

<sup>166</sup> Phumzile Van Damme, 'DA Looks Forward To Historic Meeting In Parliament With Facebook,' Democratic Alliance (2021) (accessible [here](#)).

<sup>167</sup> News24, 'Facebook Refuses to Appear Before SA Parliament On Its Own', (2021) (accessible [here](#)).

<sup>168</sup> Eyder Peralta, "'Rafiki': The Lesbian Love Story That Kenya Banned And Then Unbanned', NPR (2018) (accessible [here](#)).

<sup>169</sup> *Kahui v Mutua*, High Court of Kenya in Nairobi Petition No. 313 of 2018 (2020) (accessible [here](#)).

<sup>170</sup> Mbithi and Yiega, 'Removing Kenya's Futile Blanket Ban on Homosexual Content In Films To Stimulate

Interestingly, and prior to the *Kahiu* ruling, the Nairobi High Court in Kenya ruled in *Andama v Director of Public Prosecutions* that provisions in the Kenyan Information and Communication Act that criminalise the publication of “obscene information in electronic form” amount to an unjustifiable limitation of the rights to freedom of expression and to a fair trial.<sup>171</sup> Here the Court found that the provisions in question had a chilling effect on online expression and media. In 2021, the Nairobi High Court in Kenya was approached again by the same blogger and social media activist, Cyprian Andama, who this time challenged the constitutionality of certain provisions of the Penal Code dealing with “alarming publications” on the grounds that it limits his rights to freedom of expression and a fair trial. The Court declared the provisions unconstitutional and made important pronouncements on the right to freedom of expression online.<sup>172</sup> Unfortunately, it seems these positive rulings are not consistently won, and the right to freedom of expression online is not yet solidified in jurisprudence in Kenya.

With regard to traditional broadcast, there have been various examples of online content regulations being couched in regulations targeted at offline broadcasters, despite the obvious differences between the two mediums, and with problematic consequences. In South Africa, the Film and Publications Amendment Bill was signed into law in 2019<sup>173</sup> and was, along with its associated regulations, vehemently opposed by civil society in South Africa, many of whom pointed to the fact that the framework would require commercial online content distributors to submit content on their platforms for prior classification by the Film and Publication Board (FPB) or enter into individual exemption agreements with the FPB, as well as the broad and vague terminology used as evidence of the fact that it would infringe on freedom of expression.<sup>174</sup>

The Media Institute of Southern Africa reported that the Lesotho government, through the Lesotho Communications Authority (LCA), proposed to promulgate the Lesotho Communications Authority (Internet Broadcasting) Rules in 2020, which stipulate that individuals with more than 100 followers on social media platforms will be considered as internet broadcasters and may need to register with authorities in order to obtain an internet broadcasting allowance.<sup>175</sup>

---

Human Rights, Social, Individual And Economic Development’, (accessible [here](#)).

<sup>171</sup> *Andama v Director of Public Prosecutions*, High Court of Kenya at Nairobi, Petition No. 214 of 2018 (2019) (accessible [here](#)).

<sup>172</sup> *Andama v Director of Public Prosecutions*, High Court of Kenya at Nairobi, Petition No. 3 of 2019 (2021) (accessible [here](#)).

<sup>173</sup> ALT Advisory, ‘Films and Publications Amendment Bill Signed Into Law’, (2019) (accessible [here](#)).

<sup>174</sup> Sibahle Malinga, ‘Citizens Reject “Internet Censorship Act”, Threaten Court Action’, IT Web (2020) (accessible [here](#)).

<sup>175</sup> MISA-Zimbabwe, ‘Lesotho Proposed Internet Broadcasting Rules Will Stifle Free Speech’, (2020) (accessible [here](#)).

## ***Net Neutrality***

It is also worth noting the potential effect that so-called 'net neutrality' laws may have on limiting access to content online. Net neutrality refers to the principle that ISPs should treat all data that travels over their networks fairly, without improper discrimination in favour of a particular website or service.<sup>176</sup> Without net neutrality, information flows may be affected in a way that affects the right to freedom of expression and access to information. Net neutrality is arguably at risk in Africa because of the wide prevalence of 'zero-rating' and 'paid prioritisation schemes' as practices to advance access to the internet, wherein the use of particular applications or services do not garner charges from telecommunications providers.<sup>177</sup>

The 2017 Report of the UN Special Rapporteur on Freedom of Expression notes that, in the digital age, the freedom to choose among information sources is meaningful only when internet content and applications of all kinds are transmitted without undue discrimination or interference by non-state actors, including providers.<sup>178</sup> However, given the slow rate of growth of internet penetration in Africa and the increasing recognition of access to the internet as a fundamental right, a careful balance must be struck between the two concerns. It is also noteworthy that the African Declaration provides a resounding endorsement of net neutrality in Principle 39(1).<sup>179</sup>

## ***Opportunities for Litigation***

The landscape for litigation against content restrictions such as false news and social media laws is still open. In a small number of cases, progressive judgments have been won, while in others repressive measures have been upheld by the courts. It is therefore necessary to continue building out this body of jurisprudence, accompanied by advocacy efforts to build a narrative for the problematic nature of these laws. It may be that judiciaries need further education on the role of social media in enabling freedom of speech online and for digital rights activists to further build understanding of the international law stance on these issues and how they apply in Africa.

First, there is a need to use legal action to push back against the proliferation of hate speech legislation that is overly vague or broad (building off the reasoning in the *Qwelane* case), or that prescribes excessively harsh punishments, such as that in Nigeria (on the argument that the limitation is disproportionate).

We have yet to see many efforts at litigating against social media taxes on the basis that they inhibit access to the internet and therefore the exercise of other human rights, building off the increasingly widely held view that the internet is an enabling right (which is addressed further below). The case of the constitutional challenge against the social media taxes in Uganda relied on the argument of net neutrality.<sup>180</sup> It is therefore worth exploring the further use of a

---

<sup>176</sup> Electronic Frontier Foundation, 'Net Neutrality' (accessible [here](#)).

<sup>177</sup> Research ICT Africa, 'Much Ado About Nothing? Zero Rating In The African Context', (2016) (accessible [here](#)).

<sup>178</sup> UN Special Rapporteur on Freedom of Expression, Report A/HRC/38/35 on the Role of Digital Access Providers at para. 23 (2017) (accessible [here](#)).

<sup>179</sup> Principle 39(1) of the African Declaration, n 2.

<sup>180</sup> CNN, 'Uganda Government Sued Over Social Media Tax', (2018) (accessible [here](#)).

breach of net neutrality as grounds for challenging various content restriction measures currently in place.

Finally, an area of particular focus for litigators could arguably be the so-called social media and false news bills. It is unlikely that many of those bills would pass muster under the three-part test under international law due to the excessively broad provisions on prohibiting false content online. These laws have attracted significant public outcry in many countries, so legal action could serve to complement existing advocacy campaigns. False news laws will be addressed in further detail below.

#### **IV. Internet shutdowns**

Although an express right to the internet has not, as yet, been recognised in any international treaty or similar instrument, there has been much debate about whether the internet should be considered a human right.<sup>181</sup> There is increasing recognition though that access to the internet is indispensable to the enjoyment of an array of fundamental rights, a fact which has only been enhanced since the COVID-19 pandemic forced many daily activities online. For example, the African Declaration provides that universal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression, access to information and the exercise of other human rights.<sup>182</sup> It further prohibits states, in principle 38(2), from engaging in or condoning any disruption of access to the internet for segments of the public or an entire population.

Of greatest significance to the debate on internet access and shutdowns in the African context was the ruling in *Amnesty International Togo & Others v The Togolese Republic* (2020) in which the ECOWAS Court confirmed that internet shutdowns constitute a form of prior restraint and ruled that the internet shutdowns implemented by the Togolese government in 2017 were illegal.<sup>183</sup> The ECOWAS Court held that although access to the internet is not in itself a fundamental human right, it provides a platform to enhance the exercise of freedom of expression and therefore becomes a derivative right. The judgment reasoned that although international law recognised the national security justification for a derogation from human rights, the action taken by the state was not taken in accordance with the law as no national legislation existed at the time and was, therefore, a violation of Article 9 of the African Charter.

This section evaluates the state of internet shutdowns in East, West and Southern Africa by highlighting the growing use of shutdowns as a tool to stifle criticism, contrasted with evidence that case law condemning shutdowns as an unjustifiable violation of human rights is growing. This is followed by an analysis of the most common catalysts for shutdowns in the region, including partial restrictions that target specific platforms or applications, and concludes with a review of the implications of COVID-19 and further opportunities for litigating internet shutdowns.

---

<sup>181</sup> For more see Juan Carlos Lara, 'Internet Access And Economic, Social And Cultural Rights', Association for Progressive Communications (2015) at pp 10-11 (accessible [here](#)).

<sup>182</sup> Principle 37(2) of the African Declaration, n 2.

<sup>183</sup> *Amnesty International Togo v The Togolese Republic* (2020) (accessible [here](#)).



## ***Increasing Incidences of Internet Shutdowns***

Despite the significant milestone achieved with *Amnesty International Togo*, the trend noted in the 2018 report of the extensive and growing use of either total or partial shutdowns to quell protests in Africa, especially in election times and to stifle critical media, has continued.<sup>184</sup> In 2019, there were 25 documented instances of partial or total internet shutdowns, compared with 20 in 2018 and 12 in 2017.<sup>185</sup> Access Now further notes that several shutdowns in Africa, particularly those in 2021 thus far, have occurred around elections with the seeming intent to mar elections and control information.<sup>186</sup>

As an example of the abovementioned trend, Benin shut down the internet for the first time in the country's history on the day of legislative elections in April 2019.<sup>187</sup> In March 2020, social media sites were blocked in Guinea during a referendum,<sup>188</sup> and in October that same year, a general shutdown of the internet ensued during the general election.<sup>189</sup> Even after the general connection was re-established in Guinea, users reported that certain sites, specifically Facebook, remained blocked for several weeks. Niger likewise disrupted mobile internet three days after the presidential election in February 2021 when protests erupted following the official announcement of results,<sup>190</sup> and Tanzania implemented a partial shutdown in October 2020, 24 hours ahead of its general elections, blocking social media platforms such as WhatsApp, Facebook and Twitter in a practice known as 'throttling'.<sup>191</sup> Most recently, eSwatini shut down the internet in July 2021 in response to widespread protests against King Mswati III.<sup>192</sup>

One of the longest shutdowns recorded on the continent was that which occurred in Cameroon from 2017 onwards. Although access was eventually restored in March 2018, it remained slow and inaccessible in some parts of the country for some time after, and in January 2020, the internet was shut down once again following protests against the arrest of civil society leaders resisting government efforts to impose the Francophone legal and education systems in predominantly Anglophone regions of the country.<sup>193</sup>

Media Defence, in collaboration with Cameroon's Veritas Law Offices had, in April 2017, instituted two cases challenging the internet shutdowns on two fronts: a judicial review before the High Court; and a constitutional challenge before the Constitutional Court.<sup>194</sup> Various civil society organisations (CSOs) intervened, and the defendants included the government of Cameroon, Cameroon Telecommunications and other ISPs. The petitioners sought to challenge the shutdowns on the basis of their being a violation of the rights to freedom of

---

<sup>184</sup> Media Defence n 5, p. 19.

<sup>185</sup> Christopher Giles and Peter Mwai, 'Africa Internet: Where and How Are Governments Blocking It?', BBC News (2020) (accessible [here](#)).

<sup>186</sup> Marianne Diaz Hernandez et al, '#KeepItOn Update: Who is Shutting Down The Internet In 2021?', Access Now (2021) (accessible [here](#)).

<sup>187</sup> Paradigm Initiative, n 97.

<sup>188</sup> Access Now, 'A broken Promise To #KeepItOn: Guinea Cuts Internet Access And Blocks Social Media On Referendum Day', (2020) (accessible [here](#)).

<sup>189</sup> Access Now, 'How Internet Shutdowns Are Threatening 2020 Elections, And What You Can Do About It', (2020) (accessible [here](#)).

<sup>190</sup> Access Now, 'Niger Blacks Out Internet After Presidential Runoff Election', (2021) (accessible [here](#)).

<sup>191</sup> Global Voices, 'Internet Throttling, SMS Blocking In Days Leading Up To Election In Tanzania', (2020) (accessible [here](#)).

<sup>192</sup> Tawanda Karombo, 'Africa's Last Kingdom Is Using Modern Methods To Silence Dissent', Quartz Africa (2021) (accessible [here](#)).

<sup>193</sup> Media Defence, 'Media Defence And Veritas Law Bring Case Before The Constitutional Council Of Cameroon Challenging Internet Shutdown', (2017) (accessible [here](#)).

<sup>194</sup> Media Defence, 'An Appalling Violation Of The Right To Freedom Of Speech', (2017) (accessible [here](#)).

expression, access to information, non-discrimination based on language, and hindering economic, social and cultural rights.<sup>195</sup> It was argued that the interference with the internet violates the right to seek, receive and impart information and ideas through digital means and that a blanket ban is disproportionate and lacks a legitimate aim.<sup>196</sup> The internet was switched back on shortly after the filing of the case, but violence and repression against protesters, including through online suppression, continued.<sup>197</sup> According to Access Now, this does illustrate, however, that on occasion “simply filing the lawsuit can get results, like increased transparency and responsiveness from telcos or the state.”<sup>198</sup>

In another case to be watched, Cameroonian barrister Emmanuel Nkea, Media Defence and Mayer Brown filed two complaints in 2019 before the ACHPR alleging the shutdown of the internet in 2017 and the shutdown of access to social media and messaging platforms in 2017 to 2018 violated article 2 and article 9 of the African Charter.<sup>199</sup>

### ***Promising Developments***

International law has become increasingly clear in recent years on the fact that internet shutdowns constitute a form of prior restraint on freedom of expression, something which the ICCPR clearly provides a prohibition on.<sup>200</sup>

This has translated into some initial wins in the courts on litigating such shutdowns, including *Amnesty International Togo*. In relation to that case, Media Defence’s Legal Director Pádraig Hughes commented:

“This judgment should act as a warning to other governments considering using Internet shutdowns as a tool to silence dissent. Importantly, the Court has ruled not only that the shutdown was illegal, but that it should not be repeated.”<sup>201</sup>

The ruling came shortly after the Togolese government had once again shut off the internet on election day in February 2020,<sup>202</sup> and there is hope that it will set a precedent for West African countries (and beyond) similarly seeking to restrict the flow of information on online channels through total shutdowns.

Nevertheless, it is likely to take some time for this precedent to trickle down in practice, and there is still a great need for further litigation challenging internet shutdowns across the continent in other regions and in varying circumstances. Numerous countries have continued to implement shutdowns in the intervening period.

---

<sup>195</sup> Quartz Africa, ‘Cameroon Is Being Sued For Blocking The Internet In Its Anglophone Regions’, (2018) (accessible [here](#)).

<sup>196</sup> CIPESA, ‘Litigating Against Internet Shutdowns In Cameroon’, (2018) (accessible [here](#)).

<sup>197</sup> Media Defence, ‘Anglophone Journalists In Cameroon Continue to Face State Repression’, (2021) (accessible [here](#)).

<sup>198</sup> Peter Micek and Madeline Libbey, ‘Judges Raise The Gavel To #KeepItOn Around The World’, Access Now (2019) (accessible [here](#)).

<sup>199</sup> Media Defence, n 197.

<sup>200</sup> This has been inferred from the *travaux préparatoires* of the ICCPR that prior restraints are absolutely prohibited under article 19 of the ICCPR. See Marc J Bossuyt, ‘Guide to the “Travaux Préparatoires” of the International Covenant on Civil and Political Rights’, Martinus Nijhoff at p. 398 (1987) (accessible [here](#)).

<sup>201</sup> Media Defence, ‘Landmark Judgment: ECOWAS Court Finds Togo Violated FoE With Internet Shutdown’, (2020) (accessible [here](#)).

<sup>202</sup> Paradigm Initiative, n 97, p. 100.

We note, for example, the case of Ethiopia. Despite what appeared to be promising reforms and optimism about the opening of democratic space in the country as a result of the change in administration as detailed in the 2018 report, the period since has instead continued to be dire in terms of online freedom of expression, with the internet being shut down eight times in 2020, making the country one of the worst internet shutdown offenders in the world.<sup>203</sup> According to Paradigm Initiative:<sup>204</sup>

“In 2020, the first outage in western Oromia lasted three months – from January till late March 2020. The second and most impactful shutdown was nationwide, a measure imposed on June 30 following the killing of a famed Oromo artiste Hachalu Hundessa, in the capital Addis Ababa. That blackout lasted over three weeks. In November, a total internet outage was imposed in the northern Tigray region when the government started the “State of Emergency and Rule of Law Operation” against the then regional government led by the Tigray People’s Liberation Front (TPLF) ... EthioTelecom confirmed in late November that it had begun restoring service to parts of Tigray, days after Prime Minister Abiy announced the end of the operation. Allied to the Tigray operation, government issued arrest warrants for some activists, writers and academics who it averred were using “a variety of media outlets to destroy the country.””

Internet services remained inaccessible in part of Tigray in January 2021 as fighting continued in the region, and the government continued to blame social media as an instigating force.

The original report highlighted the fact that in many countries, such as The Gambia, the apparatus for blocking content included state control over the country’s dominant telecommunications provider(s), giving authorities the ability to restrict access to internet content without oversight, a fact which highlights the need for private sector accountability in addition to constraints on the exercise of public power.<sup>205</sup> Partial state ownership in some countries, including Zambia and Kenya, was also cited as a primary cause of concern over the government’s ability and ease to restrict internet connectivity.<sup>206</sup>

There is therefore optimism concerning Ethiopia that the prospective opening up of the telecommunications market may make it more difficult for the government to continue taking advantage of centralised connections through EthioTelecom to “cut off the internet at will”.<sup>207</sup> The government has initiated a process of awarding new telecommunications licences for the first time in a country historically dominated by the state-run company as part of its bid to liberalise the country’s economy.<sup>208</sup> This is also likely to have significant positive consequences for internet penetration in the country. Elections to be held in the country in June 2021 will, however, be decisive with regard to the general political path forward.<sup>209</sup>

## **Catalysts**

In addition to elections, common catalysts for shutdowns have been protests or civil unrest and, in a relatively new phenomenon, reactions to content moderation by the major technology

---

<sup>203</sup> *Ibid* at p. 40.

<sup>204</sup> *Ibid* at p. 41.

<sup>205</sup> Media Defence, n 5, p. 65.

<sup>206</sup> *Ibid* at p. 81.

<sup>207</sup> *Ibid* at p. 21.

<sup>208</sup> Reuters, ‘Ethiopia Receives Two Bids For Two Telecoms Operating Licences’, (2021) (accessible [here](#)).

<sup>209</sup> Declan Walsh, ‘From Nobel Hero To Driver Of War, Ethiopia’s Leader Faces Voters’, New York Times (2021) (accessible [here](#)).

companies. In relation to the former, the internet was shut down in Senegal after civil unrest connected to the arrest of a popular opposition leader on charges of rape, in addition to the suspension of two private television channels that covered the protests.<sup>210</sup>

In relation to the latter, Uganda shut down the internet on the eve of the Presidential elections in early 2021, an action reportedly ordered by the government in retaliation for Facebook's blocking of several pro-government accounts.<sup>211</sup> Another prominent example is that of the Nigerian Twitter shutdown, which is ongoing at the time of writing. Following the deletion of a tweet by President Muhammadu Buhari which contravened the company's policy on incitement to violence for threatening to punish regional secessionists, the government issued an order to service providers to restrict access to the social media platform.<sup>212</sup> The ban has since been challenged by a local human rights group at the ECOWAS Court<sup>213</sup> and by two other CSOs at the ACHPR.<sup>214</sup> In June 2021, the ECOWAS Court restrained the government from imposing sanctions or harassing, intimidating, arresting or prosecuting Twitter users until the lawsuit is heard.<sup>215</sup> It is notable that the Nigerian social media bill, mentioned above in the context of restrictions on content, would also empower government to cut off internet access or block specific social media platforms such as WhatsApp, Facebook and Twitter at its discretion if passed.<sup>216</sup>

## Partial Internet Shutdowns

It is important to note that a shutdown need not entail a wholesale interruption of the internet to cause significant consequences, both in terms of human rights and economic costs. Targeted filtering is a phenomenon that has continued as a trend in East, West and Southern Africa. In Ethiopia, hundreds of websites were blocked between 2012 and 2018, including the websites of LGBTQI+ organisations, media outlets and CSOs like the Electronic Frontier Foundation.<sup>217</sup> In 2017, during a spate of anti-government protests, Facebook, Twitter, WhatsApp and Dropbox were frequently blocked as well. Despite the change of regime, which brought with it hopes of political opening and under which hundreds of websites were unblocked,<sup>218</sup> politically motivated blocking and filtering remain concerning, especially given that there remain no procedures for determining which websites are blocked or for appealing blocking decisions.<sup>219</sup>

## Effects of COVID-19

<sup>210</sup> Aaron Ross, 'Senegal Opposition Leader Faces Rape Charge In Court As Followers Intensify Protests', Reuters (2021) (accessible [here](#)).

<sup>211</sup> BBC News, 'Uganda Election: Internet Restored But Social Media Blocked', (2021) (accessible [here](#)); Reuters, 'Facebook Takes Down Ugandan Pro-Museveni Accounts Ahead Of Election', (2021) (accessible [here](#)).

<sup>212</sup> Al Jazeera, 'Twitter Restricted In Nigeria After Government Decree', (2021) (accessible [here](#)).

<sup>213</sup> Al Jazeera, 'Nigerians Launch Legal Action Against Government's Twitter Ban', (2021) (accessible [here](#)).

<sup>214</sup> Tobi Soniyi, 'Nigerian CSOs Ask African Commission to Invalidate Twitter Ban', This Day (2021) (accessible [here](#)).

<sup>215</sup> Chike Olisah, 'Breaking: ECOWAS Court Restrains FG From Sanctioning Twitter, Nigerians, Others', Nairametrics (2021) (accessible [here](#)).

<sup>216</sup> Timileyin Omilana, 'Nigerians Raise Alarm Over Controversial Social Media Bill', Al Jazeera (2019) (accessible [here](#)).

<sup>217</sup> Media Defence, 'Advanced Modules On Digital Rights And Freedom Of Expression Online: Module 2: Restricting Access And Content', (2020) at p. 13 (accessible [here](#)).

<sup>218</sup> Freedom House, 'Freedom On The Net: Ethiopia 2018', (2018) (accessible [here](#)).

<sup>219</sup> Freedom House, 'Freedom On The Net: Ethiopia 2020', (2020) (accessible [here](#)).

As the COVID-19 pandemic erupted in early 2020, further concerns arose in many African countries around the use of COVID-19 as a justification for disruptions of internet access. In Angola, for example, the government issued a decree in March 2020 ordering state-run and private media outlets to collaborate with public agencies as part of the country's response to the pandemic, raising concerns of media manipulation.<sup>220</sup> Other governments have not needed to rely on COVID-19 containment measures to implement shutdowns where it suited them, though it has provided a convenient excuse for more recent measures.

### ***Opportunities for Litigation***

Research has shown that internet shutdowns are largely the tool of choice for authoritarian regimes.<sup>221</sup> According to CIPESA, 77% of the countries where internet shutdowns have been ordered in the last five years are categorised as authoritarian under the Democracy Index produced by the Economist Intelligence Unit, while all other African countries in which shutdowns have been implemented are hybrid regimes.<sup>222</sup> Further, countries whose leaders have been in power for several years are also more likely to order internet shutdowns.<sup>223</sup>

There is nevertheless hope for defenders of freedom of expression in the fact that there has been a notable accumulation of judgments against internet shutdowns around the world in the period since the original report that now constitutes a considerable body of works available for reference in litigating such events, in addition to the African example of *Amnesty International Togo*. For example, in *Bhasin v Union of India; Azad v Union of India* (2020) the Supreme Court of India found that freedom of speech and expression and the freedom to practice any profession or occupation over the medium of the internet enjoys constitutional protection, and that suspending internet services indefinitely is impermissible.<sup>224</sup> Likewise in *Ahmet Yildirim v Turkey* (2012), the European Court of Human Rights (ECtHR) held that a blocking order on a website hosting platform produced arbitrary effects, and that blocking segments of the internet for whole populations or segments of the public can never be justified.<sup>225</sup>

When provided for in law, internet shutdowns are typically enabled either by communications or cybersecurity legislation. Ironically, in countries in which disrupting access is not explicitly provided for in law, the existing communications or cybersecurity legislation may provide the grounds on which to challenge shutdowns. For example, laws regulating the interception of communications often prohibit the unlawful interference or obstruction of electronic communications.<sup>226</sup>

Various other strategies could be pursued in litigation as well. The Southern African Litigation Centre (SALC) points out that:<sup>227</sup>

---

<sup>220</sup> Freedom House, n 72.

<sup>221</sup> CIPESA, 'Despots And Disruptions: Five Dimensions Of Internet Shutdowns In Africa', (2019) (accessible [here](#)).

<sup>222</sup> *Ibid.*

<sup>223</sup> *Ibid.*

<sup>224</sup> *Bhasin v Union of India; Azad v Union of India* (2020) (accessible [here](#)).

<sup>225</sup> *Ahmet Yildirim v Turkey* (2012) (accessible [here](#)).

<sup>226</sup> Southern African Litigation Centre, 'Navigating Litigation During Internet Shutdowns In Southern Africa', (2019) at p. 26 (accessible [here](#)).

<sup>227</sup> *Ibid* at p. 34-35.

“Many times, the orders which are given to ISPs to shut down the internet are Presidential Directives or Executive Directives. While these directives carry some legally binding authority, they cannot always be considered to carry the force of law.”

This may also, therefore, provide grounds for challenging a shutdown. SALC further highlights other potential avenues based on contract law, declarations of emergency and other areas of law.

The Zimbabwean High Court ruled in 2019 that the government had no authority to order the internet shutdown that coincided with widespread protests in January 2019,<sup>228</sup> but the ruling was on the basis that the minister who issued the order did not have the authority to do so, rather than on the constitutional arguments of the plaintiffs.<sup>229</sup> This indicates the importance of continued creative litigation against internet shutdowns to build precedent across the continent.

As previously stated, international and regional law in Africa is clear that internet shutdowns constitute an extreme and often unjustifiable restriction on freedom of expression. The African Declaration, for example, provides that:<sup>230</sup>

“States shall not interfere with the right of individuals to seek, receive and impart information through any means of communication and digital technologies, through measures such as removing, blocking and filtering of content, unless such interference is justifiable and compatible with international human rights law.

States shall not engage in or condone any disruption of access to the internet and other digital technologies for segments of the public or an entire population.”

The above standard makes it clear that internet shutdowns result in rights violations. The practicality of litigating against states, therefore, requires a nuanced understanding of the international human rights standards of legality, necessity and proportionality, and when there can be reasonable and justifiable limitations on fundamental human rights, particularly the right to freedom of expression.<sup>231</sup>

When it comes to access to the internet, the flipside of the argument should also be considered in respect of the positive obligation on states to redress the digital divide. As noted by the Alliance for Affordable Internet, the COVID-19 pandemic has highlighted that access to the internet is a lifeline – not a luxury.<sup>232</sup> While access to the internet is certainly premised on the right to freedom of expression and access to information, it also enables a wide range of other rights, such as education, healthcare, occupation and trade. In considering opportunities for litigation, litigators may want to seek to have the state develop a plan to connect the unconnected, to realise the commitments made in the national broadband policy, or

---

<sup>228</sup> *Zimbabwe Lawyers for Human Rights and Another v The Minister of State in the President's Office Responsible for National Security and Others*, High Court of Zimbabwe Case No. HC 265/19 (2019) (accessible [here](#)).

<sup>229</sup> Freedom House, 'Freedom On The Net: Zimbabwe 2020' (2020) (accessible [here](#)).

<sup>230</sup> Principle 38 of the African Declaration, n 2.

<sup>231</sup> For more, see Media Defence, n 217. For practical tips, see SALC, 'Navigating Litigation During Internet Shutdowns In Southern Africa', (2019) (accessible [here](#)).

<sup>232</sup> Alliance for Affordable Internet, 'COVID-19 shows why internet access is a basic right. We must get everyone connected', (2020) (accessible [here](#)).

alternatively to have regard to particular segments of the population that are affected by a lack of internet access, such as schools.<sup>233</sup>

## V. Cybercrime Legislation

While cybercrimes legislation is necessary to address serious and legitimate concerns, such as hacking, disinformation and gender-based violence online, such laws also present a risk of curtailing participation, stifling criticism, or criminalising anonymous speech. Cybercrime laws are frequently vague and lack necessary safeguards.

This section reviews the large number of new cybercrimes laws that have been passed in the region since 2018. It reflects on the often very gendered nature of cybercrimes, highlights notable legal challenges against such legislation and calls out the changes wrought on the field by COVID-19, before concluding with a reflection on the opportunities for litigation to challenge overly repressive cybercrimes laws in the region.

### *Rise in Cybercrimes Laws*

At the time of the original report, a number of African countries were actively considering new cybercrime legislation or had recently passed such legislation, including Namibia, South Africa and Zambia. Perhaps most concerningly, many included provisions that were overly broad and vague, and therefore raised questions about whether they constituted a justifiable limitation of free speech.<sup>234</sup>

The original report indicated that cybercrime laws in multiple countries have been used to harass private citizens who criticise the government on online platforms, such as the Tanzanian Cybercrimes Act of 2015.<sup>235</sup> The case of Maxence Melo, co-founder of JamiiForums, a prominent media platform in Tanzania, was widely viewed as a bellwether of the state of freedom of expression in Tanzania. In 2016, he and a co-founder were charged under the Cybercrimes Act and while, encouragingly, Mr Melo was acquitted on a charge of operating a website that was not registered in Tanzania, he was convicted of obstructing police investigations by failing to disclose the identities of users on the platform.<sup>236</sup> Various provisions of the Cybercrimes Act have been criticised for, amongst other things, empowering the government to arbitrarily ban and sanction the dissemination of newspaper articles or social media posts which it deems critical, giving too much power to the police to arrest any person publishing 'false information' without meaningful oversight, and giving law enforcement extensive powers to search and seize electronic devices and computer systems without a court order, even without proof of direct involvement in a crime.<sup>237</sup>

---

<sup>233</sup> ALT Advisory et al, 'Access denied: Internet access and the right to education in South Africa', (2020) (accessible [here](#)).

<sup>234</sup> Media Defence, n 5, p. 89.

<sup>235</sup> *Ibid* at p. 35.

<sup>236</sup> CPJ, 'Jamii Forums Founder Maxence Melo Convicted On Obstruction Charge, Released In Tanzania', (2020) (accessible [here](#)).

<sup>237</sup> APC, 'The Struggle For The Realisation Of The Right To Freedom Of Expression In Southern Africa', (2021) at p. 62-63 (accessible [here](#)).

Since 2018, there have been several significant legal developments in the cybercrimes landscape in the region, though most have perpetuated the previously identified trend of overly broad and harsh provisions that risk criminalising dissent and free expression.

The *Bloggers Association of Kenya (BAKE)* case,<sup>238</sup> challenging the constitutionality of Kenya's Computer Misuse and Cybercrimes Act, was much anticipated for the role it could play in setting a precedent against the increasing usage of stifling cybercrimes legislation across the continent. As noted previously, the Kenyan High Court voided the Act in 2019 on procedural grounds but implementation of the judgment was suspended to allow Parliament to regularise the procedure in which the laws were passed. BAKE subsequently challenged the constitutionality of 26 sections of the Act on the grounds that they limited fundamental freedoms in the Constitution, but in February 2020 the Court upheld the Act in its entirety<sup>239</sup>. Notably, BAKE had contended that sections criminalising false publications as well as cyber harassment infringed on the rights to freedom of conscience, religion, belief and opinion, expression and the media. Specifically, BAKE averred that truth was not a condition of free speech and that the protection of speech extends even to that which is false. As analysed by CIPT:<sup>240</sup>

“In considering the proportionality of the limitation in section 22, the court considered the impact (on the freedom of expression) not only from the point of view of a private citizen but also from the view of the larger public i.e., the sharing of information via the internet generally. In weighing the limitation vis a vis the right protected, Makau J found that the petitioner had failed to demonstrate the excessive nature of the limitation. This was in light of the court's perception that the objective of the section was to prevent sharing of (potentially harmful) false information. The court was unable to find any other (less restrictive) means of achieving this objective, and the Petitioner also failed to adduce examples... The court relied on the social contract theory and the government's role of maintaining social order, to uphold the limitation prescribed by section 22, noting that recent trends in fake news may induce panic or unrest.”

The petitioner also contested provisions empowering the police with broad search and seizure powers in the investigation of cybercrimes. However, the Court found that the powers are limited by judicial determination and include adequate safeguards that appropriately balance privacy rights with the public interest.<sup>241</sup> The judgment effectively ended the suspension of the Act that had been put in place when BAKE's challenge was filed, and the Act, therefore, came fully into force on 20 February 2020.<sup>242</sup>

In South Africa, the Cybercrimes Act 19 of 2020 was signed into law in June 2021.<sup>243</sup> While it has been lauded for criminalising the sharing of non-consensual intimate images,<sup>244</sup> some provisions in earlier drafts of the Bill attracted fierce criticism from defenders of freedom of expression. For example, a previous version included a provision making it a criminal offence to distribute a harmful data message that is inherently false – which would have created a

---

<sup>238</sup> *BAKE v Attorney General*, High Court of Kenya in Nairobi, Petition No. 206 of 2019 (2020) (accessible [here](#)).

<sup>239</sup> CIPT, 'The Computer Misuse And Cybercrimes Act Judgment: A Digest', (2020) (accessible [here](#)).

<sup>240</sup> *Ibid.*

<sup>241</sup> *Ibid.*

<sup>242</sup> Mahesh Acharya and Neema Oriko, 'Kenya: Kenya's Computer Misuse And Cybercrimes Act, 2018: Suspended Provisions Now Effective', Mondaq (2020) (accessible [here](#)).

<sup>243</sup> Admire Moyo, 'President Ramaphosa Signs Cyber Crimes Bill Into Law', IT Web (2021) (accessible [here](#)).

<sup>244</sup> BusinessTech, 'Sending These WhatsApp Messages In South Africa Can Now Land You With a Fine And Jailtime', (2021) (accessible [here](#)).



dichotomy between information shared online versus that shared offline – but this was removed from the final version after criticism.<sup>245</sup> The initial version also contained various provisions relating to cybersecurity, having initially been called the Cybercrimes and Cybersecurity Bill, but the cybersecurity provisions were separated out after widespread criticism of the chilling effect that such provisions would have on the right to freedom of expression and other fundamental rights.

### **The gender considerations of cybercrimes**

Concerningly, many cybercrimes exhibit a particularly gendered nature, such as cyberstalking and the non-consensual sharing of intimate images, but few countries have legislation specifically addressing this. In addition to the Cybercrimes Act, South Africa also passed the Films and Publications Amendment Act<sup>246</sup> in 2019 which explicitly criminalises the practice of non-consensual dissemination of intimate images, stating that:

<sup>247</sup>

“[A]ny person who knowingly distributes private sexual photographs and films in any medium including through the internet, without prior consent of the individual or individuals and where the individual or individuals in the photographs or films is identified or identifiable in the said photographs and films, shall be guilty of an offence and liable upon conviction.”

At the time of writing, both the Cybercrimes Act and the Films and Publications Amendment Act had been signed into law, but neither had been brought into force as yet.

Several other recently passed cybercrimes laws in Africa have received harsh criticism and been challenged in court. Nigeria’s controversial Cybercrime Act, which was passed in 2015, includes a provision (section 24) stating that any person who knowingly or intentionally spreads messages online that “he knows to be false, to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent” faces a fine and imprisonment if convicted.<sup>248</sup> The Court of Appeal in Lagos dismissed a challenge to the constitutionality of the Act in 2019, disagreeing that the challenged provision was vague, overly broad or ambiguous.<sup>249</sup> However, in 2020, the ECOWAS Court ruled<sup>250</sup> that section 24 of the Act did not align with Nigeria’s obligations under the African Charter and the ICCPR, and therefore ordered Nigeria to repeal or amend the law.<sup>251</sup> Despite this notable success, activists have highlighted that implementation of the order is now a primary challenge.

<sup>245</sup> Paradigm Initiative, n 97, p. 98.

<sup>246</sup> South Africa Films and Publications Amendment Act No. 11 of 2019 (accessible [here](#)).

<sup>247</sup> *Ibid* at section 24(e).

<sup>248</sup> Abdul Abdulrahim, n 67.

<sup>249</sup> *Okedara v Attorney-General*, Court of Appeal in the Lagos Judicial Division (2019) (accessible [here](#)).

<sup>250</sup> *The Incorporated Trustees of Laws and Rights Awareness Initiatives v Nigeria*, ECOWAS Court Suit No. ECW/CCJ/APP/53/2018 (2020) (accessible [here](#)).

<sup>251</sup> APA News, ‘ECOWAS Court Orders Nigerian Government To Repeal Law on Cybercrime’, Agence de Presse Africaine (2020) (accessible [here](#)).

Zambia's Cybersecurity and Cybercrime Act has also been challenged in the High Court of Zambia by a coalition of CSOs who argue that the law's provisions threaten the right to protection of the law and the right to freedom of expression.<sup>252</sup> The law enables the government to intercept communications without a court order and requires service providers to provide services that are "capable of rendering real-time and full-time monitoring facilities for the interception of communications."<sup>253</sup> The case is ongoing.

Uganda's Computer Misuse Act has been used to arrest and intimidate numerous opposition voices, including prominent activist Stella Nyazi, social media user Robert Shaka, and popular blogger Toma Voltaire Okwalinga (a pseudonym), while the Democratic Republic of Congo also introduced a Cybercrimes Bill into the National Assembly in 2020 with the goal of "[filling] a legal vacuum" in the sector.<sup>254</sup>

Rwanda enacted Law N° 60/2018 on the prevention and punishment of cybercrimes in 2018,<sup>255</sup> which has likewise been criticised for using terrorism and national security as justification for what are considered some repressive measures. For example, the law was used to arrest a photographer under a provision on "publishing rumours",<sup>256</sup> and in a country that reportedly considers many exiled opposition organisations "terror groups", the provisions on the publication and use of "terrorist groups" is also likely to be problematic for freedom of expression.<sup>257</sup>

In Zimbabwe, the Cyber Security and Data Protection Bill was published in the Zimbabwean Government Gazette – shortly after extensive public protests had taken place over rising fuel and commodity prices in the country – with the stated intention of consolidating cyber-related offences, providing for data protection and seeking to "create a technology-driven business environment and encourage technological development and the lawful use of technology."<sup>258</sup> However, the Bill has been roundly condemned as a tool for the Zimbabwean government to stifle freedom of expression and access to information, promote interference of private communications and data, and to use search and seizure powers to access the information of activists in order to quell protests.<sup>259</sup> MISA-Zimbabwe criticised the Bill for:<sup>260</sup>

"Criminal[is]ing the sending of messages that incite violence or damage to property. In the past, this charge has been used to prosecute organizers of peaceful protests and other forms of public disobedience. The same goes for sections 164A and 164B that criminalize the sending of threatening messages and cyber-bullying and harassment respectively."

## **Effects of COVID-19**

The COVID-19 pandemic appears to have accelerated the trend of countries passing increasingly restrictive cybercrime legislation in an attempt to control the spread of mis- and/or

---

<sup>252</sup> MISA-Zimbabwe, 'Zambia's Newly Enacted Cybercrime Law Challenged In Court', (2021) (accessible [here](#)).

<sup>253</sup> *Ibid.*

<sup>254</sup> Providence Baraka, 'In DR Congo, Will New Legislation Protect Citizens' Digital Rights?', Global Voices (2020) (accessible [here](#)).

<sup>255</sup> Paradigm Initiative, n 97, p. 88.

<sup>256</sup> *Ibid.*

<sup>257</sup> Freedom House, n 13.

<sup>258</sup> ALT Advisory, 'Zimbabwe Gazettes Cyber Security And Data Protection Bill', (2020) (accessible [here](#)).

<sup>259</sup> Paradigm Initiative, 'On Zimbabwe's Approval Of A Cybercrime And Cybersecurity Bill', (2019) (accessible [here](#)).

<sup>260</sup> MISA-Zimbabwe, 'Commentary On Cybersecurity And Data Protection Bill HB-18 of 2019' (2019) (accessible [here](#)).

disinformation about the pandemic online, and to provide additional protections as activities such as education, health and daily work have increasingly been moved online. While cybercrimes laws may play an important role in ensuring a safe and secure internet, regard must also be had to the overreach of such legislation, particularly where the scope expands into issues of content regulation or seeks to stifle criticism and dissent. It has been noted that:<sup>261</sup>

“When state’s laws criminalize content that other countries don’t recognize as criminal, and then devote cybercrime enforcement resources to chasing this kind of “crime” rather than what people generally think of as cybercrime, it complicates or prevents international cooperation, discredits cybercrime legislation and enforcement efforts, and diverts resources from solving the serious problem of cybercrime. While there is certainly content that is universally reviled, i.e. child pornography, there are many disagreements about the creation and dissemination of other content, e.g. political materials or art work. For some states, free speech is an exceptionally important principle. For others, the control of offensive or dangerous content is essential. Achieving agreement on how to approach these differences is, frankly, going to be a challenge.”

### ***Opportunities for Litigation***

Given the recent wave of legal reforms in the space of cybersecurity and cybercrimes, there is presently an opportunity to influence the scope and substance of these laws to better align with human rights standards through litigation. When considering litigation on cybercrimes, the most important instrument to consider in the African landscape is the African Union Convention on Cyber Security and Personal Data Protection 2014 (known as the ‘Malabo Convention’). However, it has still not achieved widespread adoption to date, limiting its efficacy. As of June 2020, only eight states had ratified it,<sup>262</sup> out of the fifteen needed for it to enter into force. Further, the Convention has been criticised for using vague language which may be open to abuse by states,<sup>263</sup> for example, by criminalising the use of insulting language.<sup>264</sup>

Given the international and cross-border nature of cybercrimes, there may be scope for exploring accountability through litigation in foreign jurisdictions. For example, in South Africa, the family of a teenager who was sent graphic threats through Instagram from an anonymous account has sought to force Facebook, the owner of Instagram, to release the identity of the person behind the anonymous account sending the threats.<sup>265</sup>

Unfortunately, the “positive foundation for similar challenges relating to ... cybercrimes laws in Africa”<sup>266</sup> that was anticipated out of the *BAKE* judgment against Kenya’s cybercrimes act has not been borne out, and litigators will need to look elsewhere for precedent to defend

---

<sup>261</sup> Gene Burrus, ‘Cybercrime and freedom of speech – A counterproductive entanglement’, Microsoft Blogs (2017) (accessible [here](#)).

<sup>262</sup> African Union, ‘List of Countries Which Have Signed, Ratified/Acceded To The African Union Convention On Cyber Security And Personal Data Protection’, (2020) (accessible [here](#)).

<sup>263</sup> Council on Foreign Relations, ‘The African Union Cybersecurity Convention: A Missed Human Rights Opportunity’, (2015) (accessible [here](#)).

<sup>264</sup> Article 3(g) of the Convention on Cyber Security and Personal Data Protection (2014) (accessible [here](#)).

<sup>265</sup> Daily Maverick, ‘Anonymously Threatened With Gang Rape And Murder, SA Teenager Takes Facebook Inc To Court To Disclose Perpetrator’, (2020) (accessible [here](#)).

<sup>266</sup> Media Defence, n 5, p. 30.

against rights-encroaching cybercrimes laws. *Okoiti*<sup>267</sup> remains of use in providing guidance as to the checks and balances required by states when undertaking surveillance measures, as does *amaBhungane* and *Incorporated Trustees of Laws and Rights Awareness Initiative*. *Andare* remains authoritative on establishing the three-part test on the justifiability of a restriction as applicable to cybercrimes legislation and laws regulating online communications,<sup>268</sup> and *SANEF v Black Land First*<sup>269</sup> is relevant to online harassment. On other provisions of cybercrimes legislation, it may be useful to refer to litigation in other jurisdictions, such as *Shreya Singhal v Union of India*<sup>270</sup> on intermediary liability and *Disini v Secretary of Justice*, which found that the Philippines Cybercrime Prevention Act violated freedom of expression and privacy.<sup>271</sup>

Despite some of the setbacks of recent litigation in Africa against repressive cybercrimes legislation, it remains important to continue to challenge these provisions in court to firmly establish the boundaries of appropriate regulation in a rapidly changing and ever-evolving space. As countries continue to acquire new and more sophisticated technology to facilitate surveillance and law enforcement, it will be important to remain vigilant as to the consequences for freedom of expression and to ensure legislation remains up to speed with regulating these technologies. For example, much of the existing case law on surveillance cameras was litigated prior to the existence of high-accuracy facial recognition software, which dramatically alters the dynamics of the use of such technology with regard to freedom of expression, as well as other fundamental rights such as privacy and freedom of movement. Furthermore, it is expected that evidence as to the accuracy and potential biases of such technology will continue to accumulate in the coming years, providing further evidence for challenges against their use.

It is necessary to continue litigating overly broad cybercrimes legislation that claws back at protections gained over the years in other areas such as access to information, data protection, and press freedom. In particular, regional bodies such as the ECOWAS Court and the ACHPR have proven more progressive and nuanced in their judgments on related issues and should be considered as potential fora for legal challenges. Follow-up litigation to ensure implementation may also need to be considered, as in the case of Nigeria. It is particularly important that such litigation is undertaken now in order to prevent the solidification of COVID-19 era restrictions on expression implemented ostensibly for temporary pandemic management.

## VI. Media Regulation and Newsgathering Restrictions

The 2018 report highlighted several significant recent developments that have further solidified freedom of the press in case law on the continent and advanced the right to freedom of expression. For example, a landmark case at the regional level that played a role in advancing freedom of the press in Africa is that of *Zongo v Burkina Faso*,<sup>272</sup> which defended the right to

---

<sup>267</sup> *Okoiti v Communication Authority of Kenya and Others*, Constitutional Petition No. 53 of 2017 (2017) (accessible [here](#)).

<sup>268</sup> *Andare v Attorney General*, Petition No. 149 of 2015, (2015) (accessible [here](#)).

<sup>269</sup> *SANEF v Black Land First*, High Court of South Africa, Case No. 23897/17 (2017) (accessible [here](#)).

<sup>270</sup> *Shreya Singhal v Union of India*, Supreme Court of India, Petition No. 167 of 2021 (2015) (accessible [here](#)).

<sup>271</sup> *Disini v Secretary of Justice*, Supreme Court of the Philippines, G.R. No. 203335 (2014) (accessible [here](#)).

<sup>272</sup> *Zongo v Burkina Faso*, Application No. 013/2011 (accessible [here](#)).

freedom of expression and found that Burkina Faso had violated article 9 of the African Charter by failing to investigate and prosecute the murder of a prominent journalist.

The 2021 Reporters Without Borders Press Freedom Index indicates that press freedom has deteriorated around the world in the past year: “The coronavirus pandemic has been used as grounds to block journalists’ access to information sources and reporting in the field.”<sup>273</sup> Although some of the biggest gainers on the Index between 2020 and 2021 were African countries (Burundi, Sierra Leone and Mali all saw significant improvements), on the whole, Africa’s average score declined from 35,99 to 36,68 (higher scores indicate a poorer press freedom environment).<sup>274</sup>

This section evaluates the state of press freedom in the region and elaborates on the remaining challenges faced by the media in East, West, and Southern Africa. The leadership of regional bodies has proven a bright spot, and the COVID-19 pandemic has demonstrated the importance of reliable and credible media in informing the public. However, it has also provided a convenient excuse for some governments to implement harsh measures constraining freedom of the press in the name of limiting false news and misinformation. The section concludes by weighing various examples of the further deterioration of press freedom in the region against areas of hope and highlights alternative mechanisms for the advancement of press freedom.

### ***Role of Regional Bodies***

Freedom of the press has been an area in which we have seen the continued growing influence of regional bodies. The original report noted the active role played by the ACHPR Special Rapporteur on Freedom of Expression and Access to Information in furthering the right to freedom of expression, both online and offline, and particularly in defending freedom of the press. In addition to leading the development of several soft law instruments, the Special Rapporteur was active in publishing statements on current affairs of topical importance, such as attacks on journalists, which served to put pressure on states and guide state-action on matters that impact the enjoyment of freedom of expression.

The EACJ and the ECOWAS Court have also demonstrated an increased willingness to play a role in expanding the protection of fundamental rights through progressive judgments. The 2018 report states that since establishing its jurisdiction to hear cases relating to freedom of expression and the press, the EACJ is now developing an important body of jurisprudence upholding the right to freedom of expression, and it has continued to do so since. For example, in 2018, the EACJ advanced freedom of the press in *Mseto v Attorney General of Tanzania* by declaring that a ministerial order banning a Tanzanian newspaper for three years violated the right to freedom of expression and press freedom and was a breach of the EAC Treaty.<sup>275</sup> The original report also noted, however, that the EACJ had not, as of 2018, dealt directly with freedom of expression online.

---

<sup>273</sup> Reporters Without Borders, ‘2021 World Press Freedom Index: Journalism, The Vaccine Against Disinformation, Blocked In More Than 130 Countries’, (2021) (accessible [here](#)).

<sup>274</sup> *Ibid.*

<sup>275</sup> *Mseto v Attorney General of Tanzania*, East African Court of Justice, Case Number 7 of 2016 (2018) (accessible [here](#)).

The case of *Media Council of Tanzania and Others v Attorney General of Tanzania*<sup>276</sup> may be an example of how the court has begun to do so more recently. In reflecting on the false news provisions in the Tanzanian Media Services Act 120 of 2016, something closely associated with social and new online media, the EACJ found that the wording in section 50(1)(c) of the Act – “threatening the interests of defence, public safety, public order, the economic interests of the United Republic, public morality or public health” – was too broad and imprecise to enable a journalist or other person to regulate their actions. Similarly, the EACJ held that the wording in section 54 – “likely to cause fear and alarm to the public or to disturb the public peace” – was too vague and did not enable individuals to regulate their conduct.<sup>277</sup> As such, the EACJ held that sections 50(1)(c)(i) and 54 of the Act were in violation of articles 6(d) and 7(2) of the East African Community Treaty (EAC Treaty). The Act would also have vested absolute power in the Minister to prohibit the importation of publications or sanction media content. Most importantly perhaps for online freedom of expression, the Court agreed – in the context of reflecting on accreditation requirements for journalists – that the definition of a “journalist,” in line with international law, should be broad enough to include a wide range of activities including those who engage in self-publication on the internet.<sup>278</sup> In 2020, the EACJ upheld the judgment on appeal that multiple provisions of the Act were incompatible with the EAC Treaty, and instructed the Government of Tanzania to bring the Act into compliance by amending the impugned provisions which restricted certain types of news or content without reasonable justification.<sup>279</sup>

There are hopes that the state of press freedom in Tanzania is changing since President Samia Saluhu has taken office. Early indications show that President Saluhu may be willing to open up civic space and dissent to a greater extent than her predecessor.<sup>280</sup>

### ***False news and misinformation***

The passing of ‘false news’ laws in various countries has been a primary driver of the deterioration of press freedom on the continent in recent years. According to analysis by Africa Check, in the past five years governments in 11 countries across Africa doubled the number of laws and regulations in place related to ‘false information’ from 17 to 31, although that is also likely an undercount.<sup>281</sup> This has resulted in a “chilling effect” on media and political freedom, at the same time as the efficacy of such laws on mitigating the harm caused by misinformation is questionable since most are reactive rather than being used to prevent the future spread of misinformation.<sup>282</sup>

---

<sup>276</sup> *Media Council of Tanzania*, n 10.

<sup>277</sup> ALT Advisory, ‘Landmark Ruling From The East African Court Of Justice Upholding Media Freedom’, (2019) (accessible [here](#)).

<sup>278</sup> *Media Council of Tanzania*, n 10.

<sup>279</sup> *Ibid.*

<sup>280</sup> Mercy Juma, ‘Samia Suluhu Hassan – Tanzania’s New President Challenges Covid Denial,’ BBC News (2021) (accessible [here](#)).

<sup>281</sup> Africa Check, ‘Governments In Africa Have Doubled “False News” Laws, To Little Effect. Another Way Is Possible,’ (2021) (accessible [here](#)).

<sup>282</sup> *Ibid.*

## Defining The Terms: Fake News, Misinformation and Disinformation

It is important to note the distinction between ‘false news’ and ‘misinformation’, concepts that are commonly conflated. ‘False news’ refers to items that are intentionally and verifiably false and seek to mislead readers by posing as legitimate news. Many so-called ‘false news laws’ take a broad view of the definition of ‘news’, including all online publications such as blogs and social media communications, resulting in the effective criminalisation even of the unintentional or well-meaning dissemination of misinformation.

‘Misinformation’ is defined to refer to misleading information created or disseminated without manipulative or malicious intent, while a third category, disinformation, relates to deliberate (often orchestrated) attempts to confuse or manipulate people through the provision of dishonest information.<sup>283</sup>

The European Commission has stated that the term ‘fake news’ is inadequate and misleading because it includes a range of content that ranges from completely fabricated to information blended with facts and activity that includes automated networks of fake followers, organised trolling, and much more:<sup>284</sup>

“The term is also misleading because it has been appropriated by some politicians and their supporters to dismiss coverage that they find disagreeable. It has therefore become a weapon with which powerful actors can interfere in circulation of information and attack and undermine independent news media. Research has shown that citizens often associate the term ‘fake news’ with partisan political debate and poor journalism broadly, rather than more pernicious and precisely defined forms of disinformation.”

UNESCO poignantly highlights the risks of sweeping action against ‘fake news’ by stating that the term is an oxymoron – if content is news, it cannot be fake, and if it is fake, it cannot be called news – and that therefore the term “lends itself to undermining the credibility of information which does indeed meet the threshold of verifiability and public interest.”<sup>285</sup>

There are various other ways in which the impulse to control the flow of mis- and disinformation has manifested in law and regulation in the region, to problematic effect. Nigeria issued fines against a number of leading broadcast media houses for airing footage obtained from “unverified and unauthenticated social media sources” in the wake of the #EndSARS protests, justifying the act under the Nigeria Broadcasting Code (though it is contested whether the Code prohibits the use of user-generated footage as claimed).<sup>286</sup>

---

<sup>283</sup> UNESCO, ‘Journalism, “Fake News” And Disinformation’: Handbook For Journalism Education And Training’, (2018) at p 20 (accessible [here](#)).

<sup>284</sup> European Commission, ‘A Multi-Dimensional Approach To Disinformation: Report Of The Independent High Level Group On Fake News And Online Disinformation’, (2018) at p. 10 (accessible [here](#)).

<sup>285</sup> UNESCO, n 283, p. 20.

<sup>286</sup> Premium Times, ‘#EndSARS: NBC Imposes N3m Sanction Each On AIT, Channels, Arise TV’, (2020) (accessible [here](#)). See sections 3.15 and 5.6.1 to 5.6.3 of the Broadcasting Code [here](#).

The African Declaration draws a clear line in the sand with regard to false news laws in Principle 22(2) which states that “states shall repeal laws that criminalise sedition, insult and publication of false news,” providing a foundation on which to challenge such laws, and change the narrative on mis- and disinformation, going forward.<sup>287</sup> Furthermore, the 2021 report of the UN Special Rapporteur on Freedom of Expression on disinformation also notes that social media laws as responses to managing mis- and disinformation are inappropriate to the extent that they fail to meet the three-part test of legality, necessity and proportionality.<sup>288</sup>

### ***COVID-19 and the misinformation pandemic***

Accurate and reliable information has never been more important than in the context of the COVID-19 pandemic when the spread of mis- and disinformation threatens the containment efforts of governments and the health of the public. Despite this, the UN Special Rapporteur on Freedom of Expression noted that there has been a “flurry” of false news laws with at least 17 states around the world adopting legislation to address pandemic-related problematic information in the year up to mid-2021.<sup>289</sup>

Governments across the continent have similarly reacted to the challenging environment occasioned by the pandemic, along with the misinformation pandemic, by passing restrictive false news provisions that infringe on press freedom or seek to leverage the excuse of the misinformation pandemic to stifle dissent at a time when governments are facing criticism for their handling of COVID-19. States have also found various other ways to constrain the activities of the media in the context of COVID-19.

In Benin, for example, several media outlets had been awaiting authorisations from the High Authority of Audiovisual and Communication (HAAC) for months with no response from the regulatory body when the HAAC issued a statement threatening to “put an end to all publications.”<sup>290</sup> In Botswana, renowned as a leader on press freedom on the continent, two journalists were detained for “common nuisance” in June 2020 for photographing a building connected to the Directorate of Intelligence and Security Services.<sup>291</sup> Zimbabwe’s Cabinet approved proposed amendments to the Criminal Law Codification and Reform Act in October 2020, which would make it a crime for activists to make “unsubstantiated claims” of human rights abuses and criminalise “the unauthorised communication or negotiation by private citizens with foreign governments.”<sup>292</sup>

### ***Further Deterioration of Press Freedom***

Pandemic-related initiatives have combined with broader trends to contribute to a deterioration of press freedom in East, West and Southern Africa since 2018.

---

<sup>287</sup> Principle 22(2) of the African Declaration, n 2.

<sup>288</sup> United Nations Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression, ‘Disinformation And Freedom Of Opinion And Expression’, Report to the Human Rights Council (2021) (accessible [here](#)).

<sup>289</sup> *Ibid.*

<sup>290</sup> Paradigm Initiative, n 97, p. 3.

<sup>291</sup> *Ibid* at p. 7.

<sup>292</sup> Lenin Ndebele, ‘Zanu-PF Pushes For Law Banning Criticism Of Regime And Talking To Foreign Governments’, Times Live (2020) (accessible [here](#)).



The government of Mozambique has sought to replace the current Press Law with a new Social Communication Act and a new Broadcasting Act, which are presently before parliament. On 22 March 2021, Mozambican civil society organisations rejected the proposal, arguing that the proposed laws would criminalise journalists and restrict media freedom.<sup>293</sup> Others argued that the two laws would make Mozambique “one of the most closed media markets in Africa.”<sup>294</sup> Opposition political parties also rejected the law.<sup>295</sup>

Amnesty International has documented the deterioration of civic space and press freedom in Nigeria along with an increase in human rights violations in 2019,<sup>296</sup> even prior to the large-scale #EndSARS protests in October 2020 previously discussed. For example, the offices of media outlet Premium Times were raided by police in 2017, and the publisher Dapo Olorunyomi and a reporter Evelyn Okakwu were arrested.<sup>297</sup> The same occurred in January 2019 to Daily Trust, when their regional editor Uthman Abubakar and reporter Ibrahim Sawab were arrested during a raid of the newspaper’s offices.<sup>298</sup> Both cases appeared to be the result of reporting on the Nigerian military. Perhaps the best demonstration of the deterioration was a bill tabled in the Nigerian National Assembly — the Nigerian Press Council Amendment Bill, 2019 — which would have made it compulsory for all practising journalists to have a ‘media degree’ and increased the punishments and fines for ‘untrained’ journalists.<sup>299</sup> The bill was ostensibly aimed at targeting false news but was widely viewed as censoring predominantly online media.<sup>300</sup>

Arguably, this latter provision would constitute a violation of principle 13(2) of the African Declaration, which states that any registration system for media should be for solely administrative purposes and should not impose excessive restrictions on the media.<sup>301</sup>

Other countries on the continent have also continued to crack down on media. In Cameroon, for example, journalists in the Anglophone region of the country still bear the brunt of the government’s attempt to suppress civil unrest in the region. Journalist Samuel Wazizi was finally confirmed to have died in prison shortly after his arrest in 2019, after an extended period in which the government resisted efforts to establish what had happened to him.<sup>302</sup>

In September 2020, the Uganda Communications Commission (UCC) ordered all news websites and online broadcasters to register their services by 5 October 2020, including all blogs, online television and radio, online newspapers, and streaming services.<sup>303</sup> The UCC threatened to block non-compliers, and there are therefore concerns that such regulations serve to give the regulator more control over online content producers.<sup>304</sup>

---

<sup>293</sup> DW, ‘Moçambique: Sociedade Civil Quer Regulador Da Comunicação Social Independente’, (2021) (accessible [here](#)).

<sup>294</sup> DW, ‘Press Freedom In Mozambique Under Pressure’, (2021) (accessible [here](#)).

<sup>295</sup> DW, ‘MDM Alerta Para “Grande Retrocesso” Nas Propostas De Lei Da Comunicação Social,’ (2021) (accessible [here](#)).

<sup>296</sup> Amnesty International, ‘Nigeria: Endangered Voices: Attack On Freedom Of Expression In Nigeria’, (2019) (accessible [here](#)).

<sup>297</sup> Samuel Ogundipe, ‘Police Raid Premium Times Head Office; Arrest Publisher, Journalist’, Premium Times (2017) (accessible [here](#)).

<sup>298</sup> Sani Tukur, ‘Armed Soldiers Raid Nigerian Newspaper Offices, Arrest Journalists’, Premium Times (2019) (accessible [here](#)).

<sup>299</sup> Emmanuel Paul, ‘What You Need To Know As Nigeria’s Lawmakers Plan To Disqualify Journalists Without Media Degrees’, TechPoint Africa (2021) (accessible [here](#)).

<sup>300</sup> *Ibid.*

<sup>301</sup> Principle 13 of the African Declaration, n 2.

<sup>302</sup> Media Defence, ‘Government Confirms Cameroon Journalist Samuel Wazizi Died In Detention In August 2019’, (2020) (accessible [here](#)).

<sup>303</sup> Paradigm Initiative, n 97, p. 121.

<sup>304</sup> *Ibid.*

In Ethiopia, the arrest of prominent media businessmen Jawar Mohammed in 2020 in the midst of unrest following the murder of popular musician Hachalu Hundessa set off a further wave of violence in the country.<sup>305</sup> Mohammed was charged with terrorism alongside 22 other individuals and the media house he used to run. This was despite hopes that the new administration of Nobel Peace Prize winner Abiy Ahmed would strike a new tone with the media and was in contrast to other seeming efforts to liberalise the country.

In January 2019, Angola approved a new Penal Code that contains provisions specifically pertaining to the media, including fines and up to six months' imprisonment for "abuse of press freedom", which can encompass incitement, the dissemination of hate speech, and the defence of fascist or racist ideologies. The measure also covers those who disseminate texts, images, or sounds obtained by fraudulent means, as well as those who intentionally publish "fake news."<sup>306</sup>

### ***Promising Developments***

In light of these relatively bleak events for press freedom, it is worth reflecting on some of the more positive developments in the region to glean areas of hope and lessons for other countries. In general, South Africa has experienced a marked improvement in media freedom since the change of administration in 2018. As foreseen in the earlier report, the RICA ruling, confirmed by the Constitutional Court in 2021, has indeed significantly reformed the current surveillance landscape in the country and put in place better oversight mechanisms, as well as acknowledging special protections for practising journalists.

Secondly, in *Brown v Economic Freedom Fighters*, the South Gauteng High Court in Johannesburg ruled that an opposition politician, Julius Malema, had breached the relevant electoral laws by posting a journalist's phone number online in retaliation for what he believed was an attempt by the journalist to surveil his political party.<sup>307</sup> In particular, the judge ruled that the Economic Freedom Fighters (EFF) had failed to "instruct and take reasonable steps to ensure that their supporters do not harass, intimidate, threaten or abuse journalists and especially women." This raises interesting questions regarding the steps that can or should be taken to prevent or stop online harassment of journalists and the liability of influential members of society on social media for the actions of their followers. It also suggests that litigators may explore electoral laws as a potential avenue for protecting journalists under threat, especially during election periods of heightened political contestation.

Finally, Zambia approved the Zambia Council for Journalists Bill in 2020, which has been lauded by civil society, including by MISA Zambia, for enabling self-regulation of the media.<sup>308</sup>

According to Africa Check, while false news laws are rarely effective in that they target 'falsity' rather than reducing harm, some countries have followed more effective solutions that rely on access to information and propagating correcting narratives.<sup>309</sup> In this regard, there were

---

<sup>305</sup> BBC News, 'Jawar Mohammed: Top Ethiopia Opposition Figure "Proud" Of Terror Charge', (2020) (accessible [here](#)).

<sup>306</sup> Freedom House, n 72.

<sup>307</sup> *Brown v Economic Freedom Fighters*, South Gauteng High Court, Johannesburg, Case No. 14686/2019 (2019) (accessible [here](#)).

<sup>308</sup> MISA-Zambia, 'Zambian Cabinet Approves Media Bill', (2020) (accessible [here](#)).

<sup>309</sup> Africa Check, n 281.

positive developments with Ghana, Malawi and Zimbabwe having passed access to information laws in 2020.<sup>310</sup> Malawi also introduced a new law in 2016 obliging broadcasters to air “counter-versions” from those “affected by an assertion of (a false) fact.”<sup>311</sup> Likewise, Senegal introduced a self-regulatory code aimed at raising standards against misinformation.<sup>312</sup>

### ***Alternative Mechanisms to Advance Freedom of the Press***

In addition to state repression, some of the gravest challenges to press freedom around the world stem from broader social and economic developments, such as the advent of the internet which has disrupted the financial model for print media and democratised news publication, leading to an explosion of online publications and muddying the water with regards to self-regulation.

In acknowledging this fact, principle 11 of the African Declaration provides that states should take positive measures to promote a diverse and pluralistic media to facilitate the free flow of information and ideas.<sup>313</sup> Various efforts are underway to address some of these challenges. For example, the South African National Editors’ Forum has proposed the creation of a Media Sustainability Fund to provide financial support to credible news media, as well as advocated for consideration of tax relief and other state support schemes.<sup>314</sup> Similarly, the newly established International Fund for Public Interest Media seeks to divert development funds to support public interest media organisations worldwide.<sup>315</sup> Alternative revenue streams, such as membership and subscription models, are being tested all around the world, including in Africa,<sup>316</sup> and various countries have considered ways to ensure technology platform companies compensate media for content published on their platforms.<sup>317</sup>

It is important to note that members of the media from vulnerable or marginalised groups, such as women, the LGBTQI+ community and minority religions, face disproportionate harassment and abuse online in the course of carrying out their jobs. Advancing press freedom therefore necessarily requires a targeted approach to remove obstacles for these groups and ensure that minorities are not systematically excluded from the journalism profession in the online age. Equality laws may also, therefore, be of relevance for litigation efforts. In recognition of this, the African Declaration notes that states should take specific measures to ensure the safety of female journalists and media practitioners.<sup>318</sup>

### ***Opportunities for Litigation***

It is clear that regional courts such as the EACJ and ECOWAS Court provide some of the best options for litigating freedom of the press in Africa, and efforts to continue to do so should be

---

<sup>310</sup> Paradigm Initiative, n 97, p. 47 and 135.

<sup>311</sup> Africa Check, n 281.

<sup>312</sup> *Ibid.*

<sup>313</sup> Principle 11 of the African Declaration, n 2.

<sup>314</sup> SANEF, ‘Media Sustainability And Universal Access To Public Interest Journalism’, (2021) (accessible [here](#)).

<sup>315</sup> International Fund for Public Interest Media, ‘The Fund’, (undated) (accessible [here](#)).

<sup>316</sup> Membership Puzzle Project, ‘Tactics’, (undated) (accessible [here](#)).

<sup>317</sup> For example, in 2020, the Australian Competition and Consumer Commission enacted the Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act, 2020, which requires technology companies to negotiate compensation with local media companies (accessible [here](#)).

<sup>318</sup> Principle 20(6) of the African Declaration, n 2.

encouraged. It is also clear that legislative means are inappropriate for regulating the flow of mis- and disinformation online, and efforts to push back against such laws are therefore crucial. The prospects for challenging false news laws have also been discussed above.

Other repressive legislative measures, such as the Nigerian Press Council Amendment Bill, could also seemingly be challenged in court. The African Declaration may provide new opportunities to litigate violations of press freedom as it provides one of the first clear standards against false news laws in African regional law. It may be helpful to consider the legal arguments in jurisdictions where litigation has recently been successful in securing the protection of journalists. It is, however, also necessary for legal actions to be complemented by advocacy and broad-scale activism that works to address some of the root causes of the current weaknesses in the media sector, including economic challenges, in order to provide protections for media independence.

In what will likely be important test case litigation, Media Rights Agenda has filed a suit to compel the Federal Government of Nigeria to investigate attacks against journalists and punish perpetrators.<sup>319</sup> The basis of the claim is article 9 of the African Charter, which is domesticated under Nigerian law. Notably, Media Rights Agenda is also asking the Court to hold that the African Declaration constitutes subsidiary legislation in Nigeria with binding legal effect by virtue of the fact that the African Charter is domestic law in Nigeria.<sup>320</sup> At the time of writing, no date had been set for the hearing of the matter.

This raises important considerations of the positive obligations on states when it comes to press freedom, as well as the weight to be attached to the African Declaration. With regard to the first, it appears that there is ample scope for more litigation regarding the positive steps that states need to take to safeguard media freedom in their respective jurisdictions. Drawing guidance from the 2019 decision of the ECtHR in *Ismayilova v Azerbaijan*, the ECtHR affirmed the positive obligation on states, holding that the guarantee of the right to freedom of expression requires states “to create, while establishing an effective system of protection of journalists, a favourable environment for participation in public debate by all persons concerned, enabling them to express their opinions and ideas without fear, even if they run counter to those defended by official authorities or by a significant part of public opinions, or even irritating or shocking to the latter.”<sup>321</sup>

## VII. Data Protection

The original report summarised the state of data protection in Africa in 2018 as follows:

“The right to privacy is recognised in the national laws of many African states. However, states have still been slow to enact comprehensive data protection laws that appropriately safeguard the rights of data subjects. While there has been some recent impetus towards the enactment of more data protection laws – driven in significant part in order to facilitate trade with other states, particularly member states of the European Union following the coming into force of the

---

<sup>319</sup> Media Rights Agenda, ‘MRA Files Suit To Compel Federal Government To Investigate Attacks Against Journalists, Punish Perpetrators’, (2021) (accessible [here](#)).

<sup>320</sup> *Ibid.*

<sup>321</sup> ALT Advisory, ‘European Court Finds Harassment And Surveillance Of Journalist Violates Privacy And Free Speech Rights’, (2019) (accessible [here](#)).

General Data Protection Regulation of the European Union – only 18 out of the 55 African states have comprehensive data protection laws, not all of which have been fully operationalised. This leaves persons in those countries exposed to exploitative data practices that can severely infringe their rights to privacy among others.”<sup>322</sup>

At the time, data protection in Africa was in a significant state of flux, with a number of laws pending and data protection authorities in the process of being set up.<sup>323</sup> This section reflects on the continued changes occasioned in the field since then, with numerous countries passing legislation, and reflects on new challenges stemming from biometric data and COVID-19 and notes the many opportunities and needs for further litigation.

### ***Proliferation of Data Protection Legislation***

Several countries have made progress in either passing or implementing data protection laws in the past three years. South Africa finally announced that the Protection of Personal Information Act 4 of 2013 (POPIA) will come into force on 1 July 2021. South Africa also took some other steps in 2020 that have potential implications for the right to privacy. First, the Official Identity Management Policy was published for comment in December 2020, which reflects South Africa’s efforts to develop a digital identity system.<sup>324</sup> Second, the Minister of Communications and Digital Technologies published a Draft National Data and Cloud Policy for public comment in early 2021, which, if implemented, may have significant consequences for data localisation and cross-border data transfers.<sup>325</sup> Third, the Children’s Amendment Bill seeks to amend the Children’s Act to, among other things, provide for children’s privacy rights and the protection of their personal information.<sup>326</sup>

Togo’s Personal Data Act came into effect in October 2019 (Togo also passed a law effecting a biometric identity system – e-ID Togo – in September 2020, which also regulates the management of citizens’ biometric data).<sup>327</sup> Uganda passed the Data Protection and Privacy Act in 2019, but the Data Protection Office, as mandated by the Act, has not yet been established, and the associated regulations to implement the Act have likewise not yet been formulated.<sup>328</sup>

The Nigerian Data Protection Regulation was issued by the National Information Technology Development Agency (NITDA) in 2019 but has been criticised for lacking comprehensiveness and independence for enforcement.<sup>329</sup> Since then, a draft Data Protection Bill 2020 was tabled in the National Assembly which is intended to serve as a more comprehensive effective legal regime for data protection and privacy in Nigeria, but is still under consideration.<sup>330</sup> Botswana passed its Data Protection Act in 2018<sup>331</sup>, Zambia finally passed its own Data Protection Act

---

<sup>322</sup> Media Defence, n 5, p. 91.

<sup>323</sup> *Ibid* at p. 86.

<sup>324</sup> Paradigm Initiative, n 97, p. 99.

<sup>325</sup> Anri van der Spuy, ‘Unpacking South Africa’s Draft National Data And Cloud Policy: Towards Data Justice Or Greater Digital Inequality?’, Research ICT Africa (2021) (accessible [here](#)).

<sup>326</sup> Children’s Amendment Bill (2021) (accessible [here](#)).

<sup>327</sup> Paradigm Initiative, n 97, p. 110.

<sup>328</sup> Privacy International, ‘One Year On, What Has Uganda’s Data Protection Law Changed?’, (2020) (accessible [here](#)).

<sup>329</sup> Paradigm Initiative, n 97, p. 76; Stears, ‘Data & Digital Rights In Nigeria: Assessing The Activities, Issues And Opportunities’, (2021) at p. 4 (accessible [here](#)).

<sup>330</sup> Bisola Scott and Sandra Eke, ‘Nigeria: A Review Of The Nigerian Data Protection Bill 2020’, (Mondaq) (2020) (accessible [here](#)).

<sup>331</sup> Paradigm Initiative, n 97, p. 9.

in 2021,<sup>332</sup> and Malawi issued a call for public comments on the new Data Protection and Privacy Bill in June 2021.<sup>333</sup> The Telecommunications and Information and Communication Technologies Act n° 20/17 of 2020 in the Democratic Republic of the Congo also contains provisions relating to the protection of personal information and privacy.<sup>334</sup>

## Case Study: Kenya's Data Protection Act

It is worth digging further into the case of the enactment by Kenya of the Data Protection Act in November 2019, which resulted in the creation of the office of the Information Commissioner to enforce it.<sup>335</sup> Notably, this development seems to have been sparked by litigation efforts brought about by the attempted implementation of the Huduma Numba (the country's digital and biometric identity system), demonstrating the potential impact of successful digital rights litigation. In a ground-breaking judgment for data protection on the continent, the High Court in Nairobi ruled in *Nubian Rights Forum and Others v Attorney General and Others* that the government could not implement a new comprehensive digital identity system without an adequate data protection law being in place.<sup>336</sup>

### Biometric Data

Another noteworthy aspect of the Kenyan example is the collection of biometric data, which presents a unique set of concerns. As biometric data can remain relevant for the course of a person's life, the security of this data is paramount, and biometric data breaches can seriously infringe on individuals rights through identity theft or fraud, financial loss or other damage. Although the *Nubian Rights Forum* ruling has gone some way to address concerns surrounding the "biometric craze" in Kenya that was noted in the 2018 report, challenges remain regarding the independence and powers of the Information Commissioner's office.<sup>337</sup> Implementation of the Act remains a challenge and it is clear that progress in data protection requires systemic, cultural, and technical change, in addition to legal change. According to Freedom House, in April 2020, the Court of Appeal permitted the government to implement a Device Management System (DMS), a mechanism intended to identify counterfeit and illegal phones that gives the Communications Authority access to mobile subscriber data, including call records,<sup>338</sup> with potentially serious consequences for data privacy. While the Kenyan courts proved progressive in their ruling requiring the government to implement a data protection act before enabling the digital identity program to move forward, the DMS decision raises questions for the level of communications monitoring and interception that will be allowed now that a data protection act is in place. It is evident that the existence of such legislation on its own is no silver bullet for the protection of privacy.

<sup>332</sup> Data Protection Act No. 3 of 2021 (accessible [here](#)).

<sup>333</sup> Jimmy Kainja, 'Data Protection Law On The Horizon In Malawi', CIPESA (2021) (accessible [here](#)).

<sup>334</sup> Innocent Olenga, 'Nouvelle Loi Sur Les Télécoms Et TIC : Voici Quelques Innovations', Scoop RDC (2020) (accessible [here](#)).

<sup>335</sup> One Trust Data Guidance, 'Kenya - Data Protection Overview', (2021) (accessible [here](#)).

<sup>336</sup> *Nubian Rights Forum*, n 105, para. 1023-1026.

<sup>337</sup> Privacy International, 'Analysis Of Kenya's Data Protection Act, 2019', (2020) (accessible [here](#)).

<sup>338</sup> *Ibid*.

Nevertheless, they are a necessary if not sufficient component of a rights-respecting digital regulation framework, particularly as across the continent, privacy-implicating measures such as SIM card registration, digital or biometric identity programs, and surveillance programs using advanced technology such as facial recognition cameras continue apace.

### **The impetus behind data protection**

The driving force behind the increased pace of enactment of data protection legislation in recent years is likely linked to global trends – more specifically, western trends concerning the protection of personal information, as noted in the 2018 report. Additional forces are also now at play though. Economic relations in the private sector, coupled with advocacy by civil society, have also contributed to the advancement of data protection laws, along with the drive towards a single African market occasioned by the new African Continental Free Trade Area agreement. Cybercrimes legislation is closely related as these laws often also contain some data protection provisions and have also proven popular in recent years in the region. However, their enactment may, unfortunately, be linked to more nefarious intentions. States may be using cybercrimes legislation to legitimise limitations on free speech and privacy, as well as broader surveillance powers and capabilities. This appears to be happening in states where authorities are adopting a variety of measures to consolidate control, limit dissent, and regulate content.

The African Declaration may further contribute to the momentum behind data protection by requiring states to report progress against principle 42, which provides detailed requirements for the provisions states should take to adopt laws for the protection of personal information.<sup>339</sup> It is important that data protection and cybercrimes legislation serve to advance digital rights rather than roll back some of the progress that has been made in access to information, freedom of the press, and other areas of freedom of expression online.

### ***Impact of COVID-19***

Despite the progress in data protection, several problematic privacy developments occurred on the continent in the context of COVID-19 management from early 2020 onwards. In Rwanda, for example, digital tools were deployed to monitor positive cases that were able to geo-fence people in localised isolation centres to ensure they did not leave their areas of confinement. Digital tools were also used to record the identities of people who violated the COVID-19 management rules with a view to tracking 'recidivism' to inform 'serious actions' against the violators.<sup>340</sup> Private messages from WhatsApp, Skype and emails have been presented as evidence in court cases, raising serious concerns about the protection of privacy in the country.

In Nigeria, COVID-19 containment measures were equally concerning with regard to privacy and data protection. As Paradigm Initiative points out:

---

<sup>339</sup> Principle 42 of the African Declaration, n 2.

<sup>340</sup> Paradigm Initiative, n 97, p. 89.

“[T]he Nigerian Minister of Communications and Digital Economy is reported to have cited data mining, based on SIM registration data, as a way to identify the financial status of Nigerians in order to provide adequate aid. In another instance of the undisguised violation of privacy, the Minister of Humanitarian Affairs and Disaster Management, Sadiya Farouq, at a press briefing at the State House, disclosed plans to provide financial aid to Nigerians using information directly sourced from Biometric Verification Number (BVN) linked to bank accounts and confidential data provided to mobile networks.”<sup>341</sup>

The Control of Infectious Diseases Bill 2020 introduced in the Federal House of Representatives also empowered the Director General of the National Centre for Diseases Control (NCDC) to forcefully access and seize information based on ‘personal judgement’.<sup>342</sup>

In Togo, the use of electoral data to implement a digital financial assistance program for people hard hit by the pandemic resulted in the exclusion of people who had not voted.<sup>343</sup>

In a more positive development, after harsh criticism the South African government incorporated several important privacy safeguards, including user notification and an express provision that the interception of the content of communications is not permitted, in its contact tracing methods.<sup>344</sup> A judge was also appointed to oversee the contact tracing program.

### COVID-19 Contact Tracing

Since the COVID-19 pandemic began in early 2020, it appears that public health management has become another frequently used justification for stifling dissent, cracking down on ‘misinformation’ or ‘fake news’, and controlling free speech in Africa along the lines of pre-existing ‘public order’ legislation. An extensive research project evaluating contact tracing apps implemented in South Africa found various potential freedom of expression concerns with the use of the apps, despite the existence of privacy safeguards in some, and highlighted the risk of function creep towards increased usage for social control.<sup>345</sup>

### ***Opportunities for Litigation***

Despite the legislative progress made in recent years, many of the opportunities for litigation highlighted in 2018 remain relevant today. While data protection has advanced, implementation remains a primary challenge: “Enforcement of the data protection legislation will be a matter on which civil society and other stakeholders need to be vigilant.”<sup>346</sup> Many questions related to data protection still need to be settled in the courts, such as the extent of the national security justification for exclusions, and where the line between the potentially conflicting principles of access to information and data protection should sit. Many data

<sup>341</sup> *Ibid* at p. 75.

<sup>342</sup> Oyewole Oladapo and Ayo Ojebode, n 113, p. 163.

<sup>343</sup> *Ibid* at p. 111.

<sup>344</sup> Paradigm Initiative, n 97, p. 95.

<sup>345</sup> ALT Advisory, ‘COVID-19 Apps: South Africa Project Report’, (2021) (accessible [here](#)).

<sup>346</sup> Media Defence, n 5, p. 91.



protection laws in the region do not provide for pre-emptive notification of a data subject when their personal information is being processed by a responsible party or data controller, or when a data breach occurs, raising questions for how violations will be uncovered and policed. It also remains to be seen whether fines levied through the administrative or civil liability procedures will prove effective deterrents to private and public sector controllers, or how remedies for breaches should be defined. This is despite the number of significant data breaches that have occurred on the continent in recent years. For example, in 2020 it was revealed the African Union itself had experienced a serious breach of data from its security cameras.<sup>347</sup>

Many data protection laws, such as that in South Africa, also contain provisions that protect citizens from decisions based solely on automated means, but how such provisions will be interpreted and enforced remains an open question. As data protection laws continue to emerge it is expected that litigation will be used as a means to gain legal certainty on areas of the legislation that are not yet clear.

Little progress has also been made on defining the so-called 'right to be forgotten' in the region, despite some relevant case law in other regions.<sup>348</sup> Another avenue for possible litigation will be the role played by global actors, such as social media platforms, in respecting and protecting the right to privacy of members of the public in Africa. In South Africa, for example, the Information Regulator issued a stern warning to WhatsApp regarding the proposed changes to the privacy policy, and indicated that it was considering legal action if the platform continued with the approach that it had proposed.<sup>349</sup> Other jurisdictions, particularly the European Union, have seen extensive fines being levied against social media platforms for non-compliance with privacy obligations, and it will be interesting to see whether a similar approach will be followed by the regional data protection authorities in Africa.

As wide-scale collection of data for the purpose of mandatory SIM card registration or for the population of biometric databases, and more, continue apace, it is of utmost importance that litigation on data protection be undertaken across the continent to further define the right to privacy in the digital age.

Some initiatives have begun to do so. Paradigm Initiative challenged the rollout of Nigeria's National Identification Number in the Federal High Court and successfully won a ruling – although the specific data breach concerns of the applicants had been resolved before judgment – directing the National Identity Management Commission (NIMC) to improve on its data privacy and security systems in order to avoid a breach of citizens' rights to privacy.<sup>350</sup> It is hoped that similar challenges will be brought across the region to properly define the boundaries of the right to privacy in the digital age.

In a significant ruling, the UN Human Rights Committee recently ruled that the biometric identity scheme introduced in Mauritius violated the right to privacy under article 17 of the

---

<sup>347</sup> Raphael Satter, 'Exclusive-Suspected Chinese hackers Stole Camera Footage From African Union – Memo', Reuters (2020) (accessible [here](#)).

<sup>348</sup> For example, see case law in Media Defence's Resource Hub on the 'right to be forgotten' (accessible [here](#)).

<sup>349</sup> Information Regulator, 'Media Statement: Information Regulator SA Provides Legal Analysis On WhatsApp Privacy Policy', (2021) (accessible [here](#)).

<sup>350</sup> Andersen Global, 'Federal High Court Affirms The Data Privacy Rights Of Nigerian Citizens', (2019) (accessible [here](#)).

ICCPR.<sup>351</sup> According to the Human Rights Committee, given the nature and scale of the interference arising out of the mandatory processing and recording of fingerprints, it would be essential “to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness”.<sup>352</sup> This is a key ruling in respect of the impact that biometric collection has on the right to privacy, and an important reminder that alternative fora, such as the Human Rights Committee, provide crucial opportunities for litigation and law reform.

The Malabo Convention includes provisions relating to data protection, e-transactions, cybercrimes, and cybersecurity and is therefore of relevance for litigation efforts. The provisions relating to data protection are contained in Chapter II and include the conditions for the lawful processing of personal information, as well as the rights afforded to data subjects. As mentioned above, the Convention has suffered from poor support, with only five countries ratifying it so far, short of the fifteen required for it to come into force. Nevertheless, it is worth considering that there may in the future potentially be a binding legal instrument on data protection in Africa.

In West Africa, there are opportunities to rely on the Supplementary Act on Personal Data Protection within ECOWAS (ECOWAS Supplementary Act), designed to be directly transposed into a domestic context, and which, in a similar vein to the Malabo Convention, provides in detail for the conditions for lawful processing of personal information and the rights of data subjects. ECOWAS has continued to be particularly active and influential in advancing freedom of expression and other civil and political rights, especially with regards to strengthening coordination around and implementation of data protection laws.

It should be noted that as with the right to freedom of expression, any limitation of the right to privacy must comply with the three-part test for a justifiable limitation. According to the South African Constitutional Court:<sup>353</sup>

“A very high level of protection is given to the individual’s intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual’s activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation.”

One of the most significant developments occasioned by the African Declaration is the recognition of the right to privacy, which is not in itself a right that is expressly included under the African Charter.<sup>354</sup> In terms of principle 42, states are required to adopt laws for the

---

<sup>351</sup> ALT Advisory, ‘Human Rights Committee Finds Mauritian Biometric Identity Scheme Violates Right To Privacy’, (2021) (accessible [here](#)).

<sup>352</sup> *Ibid.*

<sup>353</sup> *NM and Others v Smith and Others*, [2007] ZACC 6, 4 April 2007 at para 33 (accessible [here](#)), citing with approval *Bernstein and Others v Bester NNO and Others*, [1996] ZACC 2, (1996) at para 77.

<sup>354</sup> Principles 40 and 41 of the African Declaration, n 2.

protection of personal information of individuals in accordance with international human rights laws and standards, and it sets out the conditions under which the processing of personal information is considered acceptable. States will be required to report to the ACHPR on their compliance with this provision, so it is a promising indication that more states in Africa may soon be expected to adopt comprehensive data protection frameworks that recognise the right to privacy.

## PART II: JURISPRUDENTIAL TRENDS ANALYSIS

As noted above, both the ICCPR and the African Charter prescribe that the three-part test for a justifiable restriction must be applied in order for a restriction on a fundamental human right, including freedom of expression, to be permissible. A recent report published by the APC, which mapped trends on freedom of expression in SADC, found that across these countries the requirements were not being complied with in a number of ways.<sup>355</sup> Some of the following trends were identified:

- Non-compliance with the principle of legality.
- Reliance on national security as a ground of justification.
- Lack of necessity or proportionality.
- Laws not being fit for purpose.
- High costs to communicate.
- Stifling of dissent.

The present report has identified similar trends, including in East and West Africa as well. As discussed above, regional and sub-regional courts have continued to play an important role as bastions for the defence of the right to freedom of expression in various issues related to digital rights. They should therefore be considered as fora for litigation based on the three-part test for a justifiable limitation in many of the thematic areas discussed above.

Importantly, when considering litigation in regional courts, it must be noted that cases may only be brought to the African Court by individuals or NGOs when the state against which the complaint is brought has made a declaration in terms of article 5(3) of the Court's Protocol accepting the competence of the Court to receive such complaints. In 2018, only 9 states had made the declaration. In 2020, both Benin and Cote d'Ivoire announced their intention to follow the lead of Rwanda in withdrawing their acceptance of the Court's jurisdiction over human rights complaints by individuals and NGOs.<sup>356</sup> The African Court is therefore becoming a less welcoming arena for individuals seeking to challenge rights violations, relative to the ECOWAS Court and the EACJ.

Therefore, the role of the African Court appears likely to continue to fade, with the growing number of states that do not recognise the competence of the Court to hear cases brought by individuals and NGOs. Nevertheless, the EACJ, ECOWAS Court and the ACHPR remain important fora for digital rights litigation and complaints, particularly in countries where access to the domestic courts is considered limited.

The leading role of the ECOWAS Court, in particular, is likely at least partly because of the Court's acceptance that claims for the enforcement of human rights cannot be caught by statutes of limitation. This role was demonstrated decisively in *Amnesty International Togo*. Although the EACJ has proven more difficult because it does not do so, it has still indicated its willingness to rule against states and advance powerful jurisprudence on freedom of

---

<sup>355</sup> APC, 'The Struggle For The Right To Freedom Of Expression In Southern Africa' (2021) at p. 94 (accessible [here](#)).

<sup>356</sup> International Justice Resource Center, 'Benin And Côte D'Ivoire To Withdraw Individual Access To African Court', (2020) (accessible [here](#)).

expression, as in *Media Council of Tanzania*. SADC has unfortunately remained a fairly weak regional economic community in terms of influencing the realisation of freedom of expression and impacting ICT policy development, and the SADC Tribunal still fails to offer a reprieve or redress for individuals following its *de facto* suspension in 2010.<sup>357</sup>

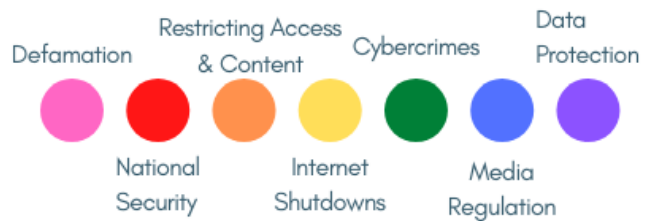
The following timeline sets out a number of the most notable judgments that are relevant to digital rights from 1994 to the present day. This analysis includes cases relevant to offline freedom of expression and the press as they have formed the foundation for litigation today that deals with similar fundamental issues of rights but on new platforms and fora of communication. It should be noted, of course, that this does not necessarily represent a comprehensive view of all case law in the region but rather a subset based on availability of judgments and influence over subsequent judgments in the same and other jurisdictions.

---

<sup>357</sup> Southern African Development Community, 'SADCAT' (accessible [here](#)).

# DIGITAL RIGHTS LITIGATION

IN WEST, EAST AND SOUTHERN AFRICA



**1994**

**National Media Ltd v Bogoshi** – recognised the defence of “reasonable publication” for the media in defamation cases

**1998**

**Constitutional Rights Project v Nigeria** – banning newspapers and detaining journalists is a violation of FoE

**2008**

**Manneh v The Gambia** – the arbitrary, incommunicado detention and disappearance of a journalist violated the right to liberty and to a fair hearing

**2013**

**Konaté v Burkina Faso** – threw out Burkina Faso’s criminal defamation law and advanced the necessity and proportionality test

**2014**

**Zongo v Burkina Faso** – by failing to investigate a journalist’s murder, Burkina Faso chilled the FoE of other journalists

**1994**

**Mukong v Cameroon** – protecting national unity could not be achieved by muzzling the press

**2000**

**Chavanduka v Minister of Home Affairs** – criminal law on false news is unconstitutional as it is too vague

**2010**

**TrustCo Group v Shikongo** – advanced the reasonable publication defence in defamation cases to apply in Namibia

**Hydara Jnr v The Gambia** – failing to investigate the killing of a journalist violated the right to life

**Chimakure v Attorney General** – held a law dealing with publishing or communicating false statements prejudicial to the State unconstitutional



**Burundi Journalism Union v Attorney General** - EACJ accepted jurisdiction to hear cases relating to FoE and the press and defended source anonymity



**MISA v Minister of Justice** - declared criminal defamation unconstitutional and inconsistent with FoE in Zimbabwe



## 2016

**Andare v Attorney General** - Kenya's ICT law and provisions against false statements were vague and unconstitutional



**SANEF v Black Land First** - granted an interdict in favour of the media broadly, prohibiting their harassment, intimidation and assault



**KS v AM** - granted an interdict against publishing sexual video footage and photographs on social media



**Federation of African Journalists v The Gambia** - ordered the repeal of laws on criminal defamation, sedition, and false news



**Gambian Press Union v Attorney General** - upheld provisions relating to sedition and the publication of false news



## 2015

**CORD v Republic of Kenya** - held that anti-terrorism laws justified using national security were unconstitutional for violating freedom of expression and the media



**Alai v Attorney General** - the offence of undermining the authority of a public officer is unclear and unjustified, and public officers have to tolerate criticism



**Ebrahim v Ashleys Kenya Ltd** - awarded damages for the dissemination of non-consensual intimate images



**Okuta v Attorney General** - Kenyan High Court found criminal defamation unconstitutional

## 2017



**JamiiMedia v Attorney General** - upheld provisions of Tanzania's Cybercrimes Act



**Okoti v Communications Authority of Kenya** - defended the right to privacy by finding a device management system overly restrictive




## 2018


**Peta v Minister of Law** - held Lesotho's criminal defamation law unconstitutional



**Mseto v Attorney General** - voided the banning order of a newspaper




**Zimbabwe Lawyers for Human Rights v Minister of State** – the government had no authority to order an internet shutdown



**Brown v Economic Freedom Fighters** – harassment, intimidation or threats by political parties against journalists breached the electoral code



**Media Council of Tanzania v Attorney General** – false news provisions were too vague and broad and criminal defamation infringes FoE and the media



**Nubian Rights Forum v Attorney General** – a digital identity program could not be implemented until an appropriate data protection framework was in place and exclusionary elements had been mitigated



**2020**  
**Amnesty International Togo v the Togolese Republic** – ruled the internet shutdown implemented by the Togolese government in 2017 in violation of the African Charter and that internet access is a “derivative right”



**amaBhungane v Minister of Justice** – held an interception law lacked safeguards and were unconstitutional and journalistic communications demanded special protections



**Andama v Director of Public Prosecutions** – declared provisions in the Penal Code dealing with “alarming publications” unconstitutional




**Okedara v Attorney General** – dismissed a challenge to Nigeria’s Cybercrime Act




**2019**



**Qwelane v SAHRC** – vague hate speech provisions were unconstitutional and a violation of FoE




**Manuel v Economic Freedom Fighters** – applied defamation law to online publications and extended the reasonable publication defence to ordinary members of the public



**Andama v Director of Public Prosecutions** – criminalising the publication of “obscene information in electronic form” amounts to an unjustifiable violation of FoE



**BAKE v Attorney General** – upheld Kenya’s Cybercrimes Act, including provisions that criminalised the publication of false news



**Kahui v Mutua** – confirmed the ban on content relating to same sex relations imposed by the Kenya Film Classification Board



**Mineral Sands v Reddell** – recognised the SLAPP defence in defamation suits for the first time

**2021**





A number of trends are clear from this review, which further highlight additional opportunities for litigation. First, litigation on media freedom, specifically those challenging regulations and abuses against journalists, has arguably been the most robust field for some time in East, West and Southern Africa out of those analysed. Some of the foundational cases dealing with press freedom that date back to the 1990s and 2000s, such as *National Media v Bogoshi* and *Constitutional Rights Project v Nigeria*, have formed the basis on which further litigation on other freedom of expression issues has taken place. It is also hopeful that they can form a solid foundation for further litigation related to online freedoms, interrogating questions such as how defamation on social media should be treated, whether bloggers and journalists posting on social media must abide by the same regulations as traditional publications, and to redefine the notion of a journalist in the online age.

Second, this timeline demonstrates that litigation against false news provisions and other related restrictions on content began to pick up steam significantly in 2019, with a flurry of challenges occurring in that year and 2020. This is likely a reflection of the increase in the number of such laws passed at the same time and it is promising – and hopefully, a reflection of the improving health and robustness of the eco-system – that litigation efforts appear to respond relatively quickly to the changing trends and new challenges in digital rights.

Third, challenges against cybercrimes legislation increased between 2016 and 2018, with mixed results. While progress was made in defining certain online crimes such as online gender-based violence, several laws considered restrictive with regards to freedom of expression and privacy were upheld by the courts. This indicated the continued work to be done in litigating cybercrimes legislation in Africa in order to define the guardrails of appropriate regulation of online crimes. It is also important that litigation on data protection issues has not kept pace to provide a counterweight to advancement in the area of cybercrimes, creating the prospect that the definition of online crimes will continue rapidly without adequate protections for privacy and data protection in consideration.

Fourth, jurisprudence against criminal defamation statutes is arguably one of the most established areas of freedom of expression law on the continent, having been definitively thrown out by various courts at both the domestic and regional levels in recent years. There are no grounds on which countries can legitimately continue to defend criminal defamation, and this is, therefore, an area ripe with opportunities to bring legal action in order to challenge the last remaining criminal defamation and insult laws in the region. There is also scope to further advance jurisprudence as it relates to online defamation specifically, with few courts having directly addressed the particular issue of social media and online publications.

Finally, litigation relating to data protection and internet shutdowns is only just getting started. This will be an important area for litigators to pay attention to in scoping out the boundaries of how human rights can be protected in the digital age. With ground-breaking judgments on internet shutdowns such as *Amnesty International Togo* under the belt, there is scope to advance additional legal challenges against internet shutdowns to build further progressive jurisprudence on the issue.

As demonstrated by this analysis and the thematic review, there is greater understanding and recognition of digital rights and the importance of safeguarding them than ever before. A number of high-profile scandals such as Cambridge Analytica, data breaches by private

companies, and the controversial use of digital technologies in elections have brought attention to the importance of human rights in the digital realm. This creates new opportunities to support willing litigants to leverage the courts to defend their rights. It has also resulted in the growth of the community of civil society organisations and lawyers working on these issues, which raises further prospects for beneficial partnerships.

There is also greater political will and genuine interest amongst governments to enact legislation responding to the new digital age. Although this has in some cases resulted in problematic legislation such as false news laws and overly vague and repressive cybercrimes laws, it creates an opening to engage with lawmakers about responsible and rights-respecting legal frameworks for the digital sphere.

Finally, there is increasing pressure on states to comply with international human rights standards, a positive impulse in the push for greater protection of freedom of expression online. The African Declaration is a promising development in this regard which provides a platform on which to push for progress and to hold governments accountable for inaction or regressive steps in the field of digital rights and freedom of expression online.

## CONCLUSION

It is clear that a useful body of jurisprudence focused on digital rights and freedom of expression online is beginning — albeit slowly — to appear across the continent. While some issues such as cybercrimes and media regulation have received significant attention in recent years, others such as data protection and internet shutdowns are just beginning to be considered by the courts. This creates a window of opportunity for those willing to support strategic litigation to contribute to defining a progressive body of jurisprudence that advances human rights across Africa and protects fundamental rights in the face of rapidly evolving new technologies.

Prospective litigants can further benefit from consulting comparative jurisprudence from other jurisdictions on digital rights, particularly the European Union, the United States and India, where digital rights litigation has become more established.

Strategic litigation can have impact not only directly, by securing a progressive judgement, but also indirectly, even in the absence of full compliance. For example, litigating cases can serve to monitor and flag human rights violations, contribute to the development of new norms, and set the boundaries for what constitutes acceptable state conduct.<sup>358</sup> They can also serve as an ‘early warning system’ to garner attention for cases that would likely not have received any if filed in a domestic context, in which the opportunities for state control are greater.

It is therefore of crucial importance to the advancement of the digital rights field generally that litigators continue to bring cases in both domestic and regional courts in Africa in order to define the guardrails of human rights in the digital age at this crucial time of technological change and social development.

However, it bears mention that litigation – while an important tool to achieve social justice – should not be seen in isolation. Complimentary strategies around advocacy campaigns, research, education, and awareness-raising should also be deployed together with any litigation strategy, so as to fully and meaningfully realise digital rights for all persons in the region.

---

<sup>358</sup> Rahina Zarma, ‘Book Review: The Performance Of Africa’s International Courts: Using Litigation For Political, Legal And Social Change’, *Afronomics Law* (2021) (accessible [here](#)).

# APPENDIX A

## QUESTIONNAIRE: MAPPING DIGITAL RIGHTS AND ONLINE FREEDOM OF EXPRESSION IN EAST, WEST AND SOUTHERN AFRICA

1.	Name:	
2.	Organisation:	
3.	Designation:	
4.	E-mail address:	
5.	In which country/ies is your organisation based?	In which country/ies does your organisation operate?
6.	What do you consider to be the most significant <b>changes/developments</b> in the digital rights landscape of the country/ies you operate in the past 3-5 years?	
7.	Have there been any <b>newly proposed or adopted laws</b> or policies relating to digital rights or online freedom of expression in the country/ies in which you operate since 2018? If so, please provide any relevant information, such as current status of the laws or policies, the public response, and the rationale for it.	
8.	Have there been any <b>recent judgments</b> , or any anticipated or ongoing litigation, in relation to digital rights and online freedom of expression in the country/ies in which you operate? If so, please provide any relevant information, such as judgments or other court documents.	
9.	What do you consider to be the <b>primary driving force/s</b> for the developments you referenced in Q. 6?	
10.	What <b>role</b> do you think <b>litigation</b> played in driving these developments, or should have played? Where do you think it could have been used to do more?	

11.	What do you consider to be the biggest <b>remaining challenges</b> or threats to digital rights and online freedom of expression in the country/ies in which you operate?
12.	What do you consider to be the <b>most significant opportunities</b> for law reform or litigation in respect of digital rights and online freedom of expression in the country/ies in which you operate?
13.	Please provide any suggestions for <b>other individuals or organisations</b> working on digital rights and online freedom of expression who you would recommend we contact.
14.	Are there any particular <b>resources</b> that you recommend we consult for this report, which speak to the above questions?
15.	<p>May we acknowledge in the research report that you and your organisation were consulted for input? Please check the appropriate box below.</p> <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> <p>Note that we only intend to include your name, the name of your organisation, and a link to your organisation's website. We will not attribute specific viewpoints to you in the report.</p>

**Published by**

# **Media Defence**

**August 2021**



**MEDIA  
DEFENCE**