

CIVIL SOCIETY

in the digital age in Africa
IDENTIFYING THREATS AND MOUNTING PUSHBACKS

Civil society in the digital age in Africa

identifying threats and mounting pushbacks

© 2020

Centre for Human Rights, University of Pretoria,
and the Collaboration on International ICT Policy
in East and Southern Africa (CIPESA)

Civil society in the digital age in Africa: identifying threats and mounting pushbacks

Authors:

Hlengiwe Dube (Egypt)
Marystella A. Simiyu (Uganda)
Tomiwa Ilori (Sierra Leone and Zambia)

ISBN: 978-1-920538-84-2

© 2020

Centre for Human Rights, University of Pretoria, and the
Collaboration on International ICT Policy in East and Southern Africa (CIPESA)

Photo acknowledgments:

Cover © sdecoret / Shutterstock
Page 11 © MidoSemsem / Shutterstock
Page 24 © Tarek Ezzat / Shutterstock
Page 43 © robertonencini / Shutterstock
Page 51 © robertonencini / Shutterstock
Page 52 © Mechmet0 / Shutterstock
Page 65 © themorningglory / Adobe Stock

Printed by Minit Print Hatfield, Pretoria, South Africa
Designed by Yolanda Booyzen, Centre for Human Rights

About the Centre for Human Rights

The Centre for Human Rights, Faculty of Law, University of Pretoria, is an internationally recognised university-based institution combining academic excellence and effective activism to advance human rights, particularly in Africa. It aims to contribute to advancing human rights, through education, research and advocacy.

www.chr.up.ac.za

About the Collaboration on International ICT Policy in East and Southern Africa (CIPESA)

The Collaboration on International ICT Policy in East and Southern Africa (CIPESA) is one of two centres established under the Catalysing Access to Information and Communications Technologies in Africa (CATIA) initiative, which was funded by the UK's Department for International Development (DfID). CIPESA focuses on decision-making that facilitates the use of ICT in support of development and poverty reduction.

www.cipesa.org

This work was carried out in the context of the Africa Digital Rights Fund with support from the Collaboration on International ICT Policy for East and Southern Africa (CIPESA).



ACRONYMS AND ABBREVIATIONS

ACHPR	African Charter on Human and Peoples' Rights
AHRLA	Association of Human Rights and Legal Aid
AMP	Accelerated Mobile Pages
AOA	Administrative Oversight Authority
AU	African Union
CAT	Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment
CEDAW	Convention on the Elimination of All Forms of Discrimination Against Women
CHRDI	Campaign for Human Rights and Development International
CMCC	Central Monitoring and Coordination Centre
CSOs	Civil Society Organisations
DCF	Development Cooperation Framework
DPI	Deep Packet Inspection
HRD	Human Rights Defenders
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICT	Information and Communication Technologies
LGBTQI	Lesbian, Gay, Bisexual, Transgender, Queer (questioning) and Intersex
MOI	Ministry of Interior
MoPED	Ministry of Planning and Development
MOSS	Ministry of Social Solidarity
NGO	Non-governmental organisations
NTRA	National Telecommunication Regulatory Authority
OAS	Organisation of American States

OAU	Organisation for African Unity
OSCE	Organisation for Security and Cooperation in Europe
RICA	Regulation of Interception of Communication Act
SCAF	Supreme Council of the Armed Forces
SMRC	Supreme Media Regulatory Council
SMS	Short Message Service
SSI	State Security Intelligence
SSL	Secure Socket Layer
SSP	State Security Prosecution
TRD	Technical Research Department
UN	United Nations
VPN	Virtual Private Network
ZICTA	Zambia Information and Communication Technology Act



TABLE OF CONTENTS

EXECUTIVE SUMMARY	7
SECTION 1: INTRODUCTION TO STUDY	9
1.1 Introduction and background	9
1.2 International law framework on civil society in Africa	12
1.2.1 The United Nations framework	12
1.2.2 The African Union human rights framework	18
SECTION 2: CASE STUDY – EGYPT	25
2.1 Country background	25
2.2 National legislative framework	27
2.3 Digital threats to civil society	33
2.3.1 Access to internet and network disruptions	33
2.3.2 Infringements on freedom of expression online and online violence	35
2.3.3 State surveillance	38
2.4 Egypt summary table	39
2.5 An analysis of the country context in Egypt	40
2.6 Recommendations for Egypt	41
SECTION 3: CASE STUDY – SIERRA LEONE	43
3.1 Country background	43
3.2 National legislative framework	44
3.3 Human rights and the civic space online in Sierra Leone	47

3.4	Sierra Leone summary table	47
3.5	An analysis of the country context in Sierra Leone	48
3.6	Recommendations for Sierra Leone	50
SECTION 4:	CASE STUDY – UGANDA	53
4.1	Country background	53
4.2	National legislative framework	54
4.3	Digital threats to civil society in Uganda	62
4.4	Uganda summary table	64
4.5	Recommendations for Uganda	64
SECTION 4:	CASE STUDY – ZAMBIA	67
4.1	Country background	67
4.2	National legislative framework	68
4.3	Human rights and the civic space online in Zambia	70
4.4	Zambia summary table	71
4.5	An analysis of the country context in Zambia	71
4.6	Recommendations for Zambia	73
SECTION 5:	OVERALL CONCLUSION AND RECOMMENDATIONS	75
5.1	Overall conclusion	75
5.2	Overall recommendations	76



EXECUTIVE SUMMARY

The digital age has created immense opportunities to enhance civic engagement by creating new frontiers for the exercise of freedom of association and peaceful assembly. These rights are recognised in seminal human rights instruments including articles 20 and 21 of the International Covenant on Civil and Political Rights, article 20 of the Universal Declaration of Human Rights, and articles 10 and 11 of the African Charter on Human and Peoples' Rights. The digital space has had monumental influence on landmark human rights movements in Africa such as the Arab Spring and Sudan's 2018-2019 popular uprising, and it has steadily been promoting the democratic agenda driven by civil society across Africa.

Unfortunately, these developments have not escaped the notice of oppressive governments that are increasingly adopting undemocratic measures to restrict the exercise of right to freedom of association and peaceful assembly, as well as interdependent rights such as freedom of expression, right to access of information, and right to privacy in the digital space. This is witnessed in increased state sponsored online and offline surveillance, internet shutdowns, network disruptions, online harassment, remote intrusion of civil society websites, censorship and other measures that seek to further shrink the civic space.

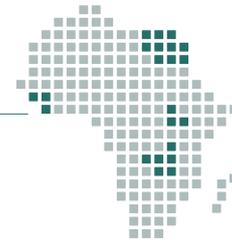
The report documents the threats to civil society in the digital age by examining the legislative and regulatory framework in four countries in Africa: Egypt, Sierra Leone, Uganda and Zambia. These countries were selected from the four main geographic regions of Africa, in order to provide a sense of the state of civic engagement in the digital age across the continent. The case studies are clearly not representative of what is happening on the continent, but are illustrative of some prominent trends. The recommendations emanating from the research call for the states to revise and repeal identi-

fied restrictive laws and align them with international standards. Civil society organisations and human rights activists are also encouraged to enhance their individual and organizational digital knowledge and expertise to more robust counter disruptive state measures. This expertise should be enhanced through a human rights lens and should extend to other stakeholders including judicial officers, legislators, law enforcement and the general public through sustained multi-stakeholder engagement.

It is this state of affairs that motivated the development of this research on *Civil Society in the digital age: identifying threats and mounting pushbacks*. The research was conceived from the partnership between the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) and the Expression, Information and Digital Rights Unit of the Centre for Human Rights, University of Pretoria. The expertise of Tawanda Mugari, a digital security expert, as well as select professionals and human rights defenders responsible for the country case studies, was invaluable to the substance of this report.

It is hoped that the report will not only build on existing research on digital rights in Africa, but also inspire further research to develop a substantive literary database for advocacy for protection, promotion and fulfilment of human rights and fundamental freedoms in the digital age in Africa.

Prof Frans Viljoen
Director, Centre for Human Rights, University of Pretoria



SECTION 1

INTRODUCTION TO STUDY

1.1 Introduction and background

The civil society is essential in a functioning democracy.¹ They can also be referred to as the formal or informal structures that exist either offline or online with the aim of pursuing democratic development but outside the state structure. Although they vary in form, what is generally referred to as civil society includes registered non-governmental organisations (NGOs), human rights defenders, social movements, faith based organisations, labour movements, community-based organisations, and online activists.² The role of civil society includes connecting citizens with various stakeholders, facilitating civic engagement and participation.³ It is generally described as the 'third space' where citizens converge for various but common aspirations.⁴ Some African countries such as Côte d'Ivoire, Burkina Faso and Mali have acknowledged the importance of civil society through the adoption of laws that promote and protect the human rights of civil society including human rights defenders (HRD).⁵

1 L Bernholz 'Philanthropy and Digital Civil Society: Blueprint' (2018) <https://pacscenter.stanford.edu/publication/philanthropy-and-digital-civil-society-blueprint-2018/> (accessed 16 August 2019).

2 World Economic Forum's 'The Future Role of Civil Society' http://www3.weforum.org/docs/WEF_FutureRoleCivilSociety_Report_2013.pdf (accessed 15 August 2019).

3 W Gumede 'Democracy Works Foundation: Policy Brief 16: African Civil Society under Fire' (2017) <https://democracyworks.org.za/policy-brief-16-african-civil-society-under-fire/> (accessed 15 August 2019).

4 Bernholz (n 1 above).

5 D Kode 'Civic Space Restrictions in Africa How does civil society respond?' (2018) <https://www.aaccord.org.za/conflict-trends/civic-space-restrictions-in-africa/> (accessed 16 August 2019).

However, despite this generally accepted role of civil society, this ‘third space’ is under threat.⁶ Some studies have shown that civil society faces impediments even in countries that are generally regarded as leading democracies. The clampdown on civil society is either overt or covert through restrictive laws, policies and regulations, network disruptions, state-sponsored digital and offline surveillance, arrests of activists, social media monitoring, and online violence. In Africa, the situation is more pronounced as the civic space continues to shrink faster than in other continents.⁷ This occurs in the form of attacks and threats that are exacerbated by existing restrictive regulatory frameworks in most African states. Clampdowns on civil society are often government-sanctioned through state officials, national intelligence, government institutions, terrorist groups and the private sector.⁸ Generally, civil society and HRDs, particularly those focusing on civil and political rights and democracy-oriented programmes are perceived with suspicion; hence, the curtailment of their freedom. Therefore, in light of the issues that have been raised, this research focused on state-sponsored threats to civil society activities including digital threats that curtail the work of civil society in Egypt, Sierra Leone, Uganda and Zambia. The research further assessed legislative and other measures that pose threats to civic engagement and the overall operations of civil society by infringing on their rights.

Violations against civil society can be analysed according to the respective rights being infringed upon - violations of freedom of association and freedom of peaceful assembly. Violations associated with the freedom of association include raiding premises, attacks on activists and NGO staff, adoption of anti-NGO legislation, policies and regulations, seizure of assets such as computers, organisation documents, equipment (cameras for example), public denunciations, targeting and deregistration of organisations or individuals.⁹ The infringement of freedom of expression of civil society involves denial of access to information, restrictive laws, closure of media houses, assaults on journalists and other media practitioners, blocking of newspaper circulation, censorship of social media and news sites, and criminalisation of free speech.¹⁰ The violations of freedom of peaceful assembly take the form of unlawful and excessive use of force by police or military; arrests of protestors; denial to conduct peaceful protests or gatherings; adoption and use of anti-terrorism and state security laws.¹¹

6 Bernholz (n 1 above).

7 CIVICUS ‘US Monitor, Tracking Civic Space’ (2004) <https://monitor.civicus.org/> (accessed 16 August 2019).

8 Kode (n 5 above).

9 CIVICUS ‘Civil Society Watch Report’ (2016). https://www.civicus.org/images/CSW_Report.pdf (accessed 12 August 2019).

10 As above.

11 As above.



Egyptians protest against President Morsi in Sidi Gaber, Alexandria, Egypt on June 30, 2013
© MidoSemsem / Shutterstock

While national constitutions generally recognise the freedoms of expression, association, and assembly as fundamental rights, they usually exist alongside restrictive legislation. There is existence of laws that strengthen states' restrictive strategies against civil society. These laws, often garbed with the cover of public order, national security, cybersecurity and anti-terrorism laws, compromise operations of civil society through strategies such as digital threats, limiting foreign funding, among others.¹² These laws trample on the right to privacy, impede on the right to protest, criminalise free speech especially by dissenting voices, government critics, bloggers, pro-democracy activists and journalists.¹³ In some instances, there is reliance on archaic colonial legislation that were used by former colonisers to clampdown on civil society activists and organisations. Consequently, democracy-enabling human rights such as the right to protest and assembly are criminalised and arrests and imprisonment of civil society activists, journalists, bloggers and other human rights defenders are often carried out based on these laws.¹⁴ Civil society activists including human rights defenders who organise protests are usually harassed for criticising government officials (especially the head of state), speaking against the deteriorating human rights situation and any other acts considered to be threatening to national security or public order by the state.

1.2 International law framework on civil society in Africa

African states have binding commitments on the protection and promotion of human rights under human rights treaties, which provide for civil and political rights that are pertinent to the work and existence of civil society. These human rights instruments include the African Charter on Human and Peoples Rights (ACHPR), the International Covenant on Civil and Political Rights (ICCPR) and other instruments that have been adopted by the different special procedure mechanisms of the United Nations (UN) and the African human rights systems to strengthen the protection of the aforementioned rights. Nevertheless, the status quo affirms that states are renegeing on these obligations and are failing to create conducive environments for civil society to operate. These rights, under the relevant frameworks are further considered below.

1.2.1 The United Nations framework

The promotion, respect and fulfilment of human rights is critical to the work of civil society. Various international and regional human rights instruments, as well as declarations, resolutions, principles and guidelines developed by the international human

12 Bernholz (n 1 above).

13 CIVICUS (n 9 above).

14 Amnesty International 'Egypt arrested 19 human rights activists in 1 day' 3 November 2018 <https://www.middleeastmonitor.com/20181103-amnesty-egypt-arrested-19-human-rights-activists-in-1-day/> (accessed 14 August 2019).

rights community have articulated these rights. The right to peaceful assembly is recognised under article 21 of the ICCPR. Article 22 of the ICCPR further provides that, '[e]veryone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests.' Both articles add that any limitations to the right of association and peaceful assembly should meet the threefold standard of being provided by law, necessary and proportionate in a democratic society, and serve a legitimate aim, such as national security or public safety, public order, public health or morals, or the protection of the rights and freedoms of others.¹⁵ The Covenant places the primary responsibility on states to respect and ensure the respect for the rights therein, and to take legislative and other measures to give effect to human rights and fundamental freedoms.¹⁶

Article 20 of the Universal Declaration of Human Rights (Universal Declaration) also provides for the right to freedom of assembly and association, adding that no one should be forced to join an association. The right to association and peaceful assembly is similarly reiterated in other human rights documents under the UN human rights framework as well as regional bodies.¹⁷ All countries in Africa have signed and ratified the ICCPR except Comoros that is only a signatory and South Sudan that has neither signed nor ratified the ICCPR.¹⁸ However, the ICCPR and the Universal Declaration have attained the status of customary international norms and therefore these countries are still bound by their provisions.¹⁹

Increasingly, the right to association and peaceful assembly has come under attack in both emerging and established democracies.²⁰ The joint cooperation of the international community, civil society, and individuals involved in human rights work is essential to addressing the assault on human rights and fundamental freedoms. This is acknowledged in the Preamble of the Declaration on the Right and Responsibility of

15 Art 22 (2) ICCPR.

16 Art 2 ICCPR.

17 Art 15 of the International Convention on the Rights of the Child; Art 7(c) of the Convention on the Elimination of All Forms of Discrimination Against Women; Art 15 of the International Convention on the Rights of the Child; Art 15 of the Convention Relating to the Status of Refugees; Art 24(7) of the International Convention for the Protection of All Persons from Enforced Disappearance; Arts 26 & 40 of the International Convention on the Protection of the Rights of All Migrants Workers and Members of Their Families; Art 29 of the Convention on the Rights of Persons with Disabilities; 2008 Declaration of the Committee of Ministers on Council of Europe action to improve the protection of human rights defenders and promote their activities; 2008 European Union Guidelines on Human Rights Defenders; 2016 Guidelines on the Protection of Human Rights Defenders; Resolution 68/181 Promotion of the Declaration on the Right and Responsibility on Individuals, Groups and Organs of Society to Promote and Protect Universally Recognised Human Rights Fundamental Freedoms: Protecting Women Human Rights Defenders 2013; and Model Law for the Recognition and Protection of Human Rights Defenders, 2017.

18 OHCHR 'Status of ratification interactive dashboard' <http://indicators.ohchr.org/> (accessed 27 August 2019).

19 Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye' (22 May 2015) A/HRC/29/32 para 15.

20 Freedom House 'Democracy in retreat: Freedom in the World 2019' 2019 <https://freedomhouse.org/report/freedom-world/freedom-world-2019/democracy-in-retreat> (accessed 8 August 2019).

Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms (Declaration on the Rights of Human Rights Defenders).²¹ Every person has a right to promote human rights and fundamental freedoms.²² Article 5 of the Declaration provides that with the aim of promoting and protecting human rights and fundamental freedoms, individuals and associations have the right to peaceful assembly, the right to association, and the right to engage with non-governmental or intergovernmental organizations. Given the indivisibility and interdependence of human rights, the Declaration additionally recognises the importance of the right of access to information, freedom of expression and opinion, and meaningful participation in public affairs to the work of human rights defenders.²³

The Declaration also underscores the duty of individuals, groups, and associations towards 'safeguarding democracy, promoting human rights and fundamental freedoms and contributing to the promotion and advancement of democratic societies, institutions and processes.'²⁴ Similarly to the ICCPR, any limitations to the rights encapsulated in the Declaration should meet the international standards of legality, necessity and proportionality, and legitimate aim.²⁵ States also have the primary responsibility to put in place legislative, administrative and other measures that protect the rights of human rights defenders.²⁶

As articulated in the Declaration, CSOs and HRDs cannot meaningfully undertake their mandate when their freedom of expression and opinion is stifled. Article 19 of the Universal Declaration and the ICCPR provide for freedom of expression and opinion without interference. In exercise of this right, a person has the 'freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.'²⁷ The person has a concurrent duty to respect the rights and reputation of others. Further, the realisation of this right should not endanger national security or public order, public health or morals. Noteworthy, the provision of the exercise of freedom of expression and access to information 'through any other media' may be said to be forward-looking as it accommodates media such as the internet that were not developed during the drafting of the Convention.²⁸

21 Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms Resolution adopted by the General Assembly on 8 March 1999 A/RES/53/144.

22 Art 1 Declaration on the Rights of Human Rights Defenders.

23 Arts 6, 7 and 8 Declaration on the Rights of Human Rights Defenders.

24 Art 18 Declaration on the Rights of Human Rights Defenders.

25 Art 17 Declaration on the Rights of Human Rights Defenders.

26 Art 2 Declaration on the Rights of Human Rights Defenders.

27 Art 19 (2) ICCPR.

28 Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (10 August 2011) A/66/290 para 14.

States have often used the restrictions outlined in article 19(3) of the ICCPR to justify restrictions on freedom of expression and target government critics including CSOs. Under General Comment 34, the Human Rights Committee asserted that when a state invokes a restriction, it should not in effect render the exercise of the right impossible. It reiterated that 'relation between right and restriction and between norm and exception must not be reversed.'²⁹ General Comment 34 further provides that these limitations:³⁰

...may never be invoked as a justification for the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights. Nor, under any circumstance, can an attack on a person, because of the exercise of his or her freedom of opinion and expression, including such forms of attack as arbitrary arrest, torture, threats to life and killing, be compatible with article 19.

This implies the provision of an enabling environment for not only CSOs and other activists but also media, and political opposition members whose advocacy for democratic ideals may lead them to clash with government. Further, in relying on any ground for restricting the right to freedom of expression, a state must show in a specific way the precise nature of the threat.³¹

The digital age has introduced innovative ways to exercise the right to freedom of association and peaceful assembly, and freedom of expression by providing both a means and a platform for political and civil organising, and information gathering and dissemination.³² In contrast, the digital age has also increased challenges to the work of activists with reports of government using digital technologies in bad faith to frustrate the work of civil society. This is in violation of the negative obligation of states not to interfere in the exercise of human rights and fundamental freedoms. This has been seen in increased reports of government-sponsored surveillance, cyber-attacks, online harassment, restrictive legislation, blocking websites of CSOs, network disruptions, internet shutdowns, and online content regulation.³³ The interference of the exercise of these rights, particularly through arbitrary and unlawful surveillance of civil society organisations and activists prompted the UN General Assembly to condemn such actions.³⁴

29 Human Rights Committee General Comment 34 on Article 19: Freedoms of opinion and expression (12 September 2011) CCPR/C/GC/34 para 21.

30 General Comment 34 (n 69 above) para 23.

31 General Comment 34 (n 69 above) para 36.

32 Human Rights Council 'Rights to freedom of peaceful assembly and of association. Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association' (17 May 2019) A/HRC/41/41 para 11 & 21; Human Rights Council 'Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association' (13 June 2018) A/HRC/38/34; Human Rights Council 'Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association' (29 June 2017) A/HRC/35/28; Human Rights Council 'Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai' (21 May 2012) A/HRC/20/27.

33 Human Rights Council (n 72 above) A/HRC/41/41 para 29.

34 General Assembly resolutions 68/167 and 71/199 on the right to privacy in the digital age.

This status quo raises questions whether the existing international legal framework is sufficient for protecting the right to association in the digital age or if there is a need for re-regulation, or increased self-regulatory measures by digital technologies companies. Clément Nyaletsossi Voule, the Special Rapporteur on the rights to freedom of peaceful assembly and of association, asserts that ‘existing international human rights norms and principles should not only dictate State conduct, but also be the framework that guides digital technology companies’ design, control and governance of digital technologies.’³⁵ However, outside this framework, resolutions passed by the Human Rights Council and the General Assembly underscoring the obligation of states to protect, promote and respect the right to freedom of peaceful assembly and association, and freedom of expression both online and offline have created awareness for these rights by recognising the unique challenges presented by digital technologies.³⁶ Therefore, the right to association and related human rights should be realised in equal measures on both platforms.³⁷

The interconnectedness of the rights to freedom of association and expression and the right to privacy has become increasingly evident in the digital age. The right to privacy is articulated under article 17 of the ICCPR which provides that ‘[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.’ The article further requires legal protection from such attacks. This right is echoed under article 12 of the Universal Declaration.

Freedom of expression and privacy are more vulnerable to interference in the digital age, particularly against CSOs and HRDs who are a targeted group when it comes to online surveillance.³⁸ As the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression notes, there is hardly a protection framework for the violation of human rights and fundamental freedoms with the use of digital technologies such as targeted surveillance systems.³⁹ Unfortunately, targeted surveillance systems may lead to disproportionate self-censorship so as to avoid the repercussions of surveillance even that which is unlawful.⁴⁰ Noting these risks to the exercise of human rights, the General Assembly stated:⁴¹

35 Human Rights Council ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue’ (16 May 2011) A/HRC/17/27 paras 53-59 & A/HRC/41/41 para 66.

36 Human Rights Council ‘The promotion, protection and enjoyment of human rights on the Internet’ (17 July 2018) A/HRC/29/32 & General Assembly ‘Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association’ (17 December 2018) A/RES/73/173.

37 Human Rights Council ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression’ (28 May 2019) A/HRC/41/35 para 24 & A/HRC/29/32 para 24.

38 Human Rights Council (n 77 above) A/HRC/41/35 para 1.

39 Human Rights Council (n 77 above) A/HRC/41/35 para 46.

40 Human Rights Council (n 77 above) A/HRC/41/35 para 21.

41 General Assembly resolution 73/179 on the right to privacy in the digital age.

Surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory.

Given that it may not always be enough to rely on states to fulfil their obligations under international law, CSOs and HRDs are increasingly embracing the use of encryptions and anonymity to create the necessary privacy that allows them to freely exercise their right to freedom of expression, association, and peaceful assembly.⁴² This has not escaped the notice of governments, but as is the standard, any restriction to the use of encryptions and anonymity systems should be assessed based on whether it is provided by law, necessary and proportionate and serves a legitimate aim.

The need to include the private sector as a key actor in the human rights movement is increasingly becoming necessary given the application of digital technologies to both advance as well as restrict human rights and fundamental freedoms. The private sector needs to ensure their operations do not only focus on the profit margin but are also human rights oriented. The Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework articulates the duties of states and businesses in this regard.⁴³ States have a duty to protect their citizens and territory from infringement of their rights by third parties.⁴⁴ On the other hand, business enterprises have a duty to respect human rights.⁴⁵ The Guiding Principles call for human rights due diligence that entails an assessment of the actual or likely human rights impact of their work and relevant action to address these impacts.⁴⁶

In the event that a right under the ICCPR is infringed, whether through the fault of the state or third parties such as business enterprises, state parties have a duty to ensure the wronged party has access to an effective remedy.⁴⁷ This is reiterated under the *Guiding Principles on Business and Human Rights*. Relevant third parties should learn from cases where their products are used to infringe on human rights to improve on their systems.⁴⁸ The international community as well as civil society have gone further to develop other guidelines on the exercise of business rights in a human rights-oriented

42 Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye' (22 May 2015) A/HRC/29/32 para 16 & General Assembly resolution 68/167.

43 The Human Rights Council endorsed the Guiding Principles in its resolution 17/4 of 16 June 2011, A/HRC/17/4.

44 Principles 1 & 2.

45 Principle 16.

46 Principles 17-21.

47 Article 2 (3) of the ICCPR & the Human Rights Committee General Comment 16 and General Comment 31 on the nature of the general legal obligation imposed on States parties to the Covenant.

48 Principle 31.

approach.⁴⁹ Access to the internet is also essential to the exercise of the rights discussed above. While access to the internet is not recognised as a right, states have a positive obligation to take measures to promote the enjoyment of human rights, and in this context, ensure access and openness of the internet, as well as avoid arbitrary and disproportionate limitations to it.⁵⁰

1.2.2 The African Union human rights framework

In what became the most definitive regional human rights policy during the Organisation for African Unity (OAU), the African Charter for Human and Peoples' Rights (the African Charter) also known as the Banjul Charter rose from the ashes of the flagrant human rights violations during the 1970s.⁵¹ So, it could be said that the African Charter came about as a curative and preventive instrument to right several human rights wrongs that the continent has become synonymous with in which civil society played an important role. One of the earliest impacts of civil society and HRDs as regional human rights stakeholders in Africa is seen when their role became well defined in the establishment of special procedures by the African Commission on Human and Peoples' Rights (the African Commission) in 1995 to tackle pronounced human rights violations in the region. Subsequently, in 1999, the Grand Bay Declaration features prominently among AU legal instruments as testimony to the recognition of human rights defenders by African leaders.⁵² According to the Special Rapporteur on Human Rights Defenders, civil society is mostly made up of Human Rights Defenders (HRDs) and in this regard, it is important to retain a tentative definition of human rights defenders who, according to the United Nations, are people who, individually or with others, act to promote or protect human rights.⁵³

The importance of civil society in the activation of the African Charter as an effective human rights document can be seen in its use since it was adopted in 1981 and came into force five years after. Articles 10 and 11 of the African Charter provides for the rights to association and assembly. These provisions directly offer protection for civil society and HRDs in Africa. Matching the period most African states witnessed their third wave of democratisation, civil society and HRDs became a *de facto* arm of government whose re-

49 Global Network Initiative's Principles on Freedom of Expression and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights and the Telecommunications Industry Dialogue Guiding Principles; the International Principles on the Application of Human Rights to Communications Surveillance and the Global Principles on National Security and the Right to Information. Telecommunications Industry Dialogue Guiding Principles.

50 Human Rights Committee General Comment 34 on Article 19: Freedoms of opinion and expression (12 September 2011) CCPR/C/GC/34 para 15 & Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (11 May 2016) A/HRC/32/38 para 49.

51 U Umzurike *Five years of the African Commission on Human and Peoples' Rights* (1992) 3.

52 https://archives.au.int/bitstream/handle/123456789/2058/Grand%20Bay%20Declaration_E.pdf (accessed 12 August 2019).

53 Special Rapporteur report <https://www.achpr.org/sessions/sessionsp?id=140> (accessed 3 August 2019).

sponsibility was to ensure that the hangover of military governments does not taint the spirits of the new constitutions and their interpretations.⁵⁴ In instances where military governments were still in power, civil society and HRDs were often used as scarecrows to chill dissent into silence towards impunity and arbitrariness.

More recently, in 2017, the African Commission on Human and Peoples' Rights (African Commission) adopted the Guidelines on Freedom of Association and Assembly which provides for a framework to strengthen the obligations required for the promotion and protection of the rights to freedom of association and assembly.⁵⁵ The preamble of the Guidelines states that the African Commission in its promotion and protection mandate under the African Charter, shall have regard to various political, technological and security development impacting the enjoyment of rights. Its definition section conceptualises assembly as:

... an act of intentionally gathering, in private or in public, for an expressive purpose and for an extended duration. The right to assembly may be exercised in a number of ways, including through demonstrations, protests, meetings, processions, rallies, sit-ins, and funerals, *through the use of online platforms*, or in any other way people choose.

Section 35 of the Guidelines provides that associations shall have the right to privacy and such shall not be subjected to undue surveillance. It also states that surveillance on associations may only be carried out on a reasonable suspicion of a crime which must be court-ordered with a warrant. It further provides that there shall be a form of redress for associations and individuals (most likely human rights defenders) who have been surveilled illegitimately.

In addition to the provisions of Articles 10 and 11, the African Charter also provides for the right to freedom of expression and access to information under Article 9. The provisions of Article 9 also provide for a clawback clause which states that the right can be limited under the law. The law being referred to under section 9 as 'within the law' is international law and not national laws as it concerns the limitation of the right to freedom of expression as stated above.⁵⁶ Described as one of the most important rights in any modern democracy, the right to freedom of expression is closely knitted to the realisation of civil rights as well as safeguarding the activities of civil society and HRDs in Africa. Civil society and HRDs undertake their work through shaping of public policy as

54 See generally E Gyimah-Boadi 'Civil society in Africa' (1996) 7 *Journal of Democracy* <https://muse.jhu.edu/article/16739> (accessed 29 July 2019); M Bratton 'Civil society and political transition in Africa' (1994) 11 *IDR Reports* 6 <https://www.issuelab.org/resources/19673/19673.pdf> (accessed 29 July 2019).

55 Guidelines on Freedom of Association and Assembly in Africa

56 AO Salau 'The right of access to information and national security in the African regional human rights system' (2017) 17 *African Human Rights Law Journal* 385.

well as ensuring that this influencing is done properly. To achieve this, they need access to information mostly from the state. This reality is what makes addressing the protection of civil society in Africa more than guaranteeing just the freedom of association and assembly but also that of expression in Africa.

Even though the African Charter does not provide for the right to privacy, the African Union Convention on Cybersecurity and Personal Data Protection was created pursuant to the African Union Constitutive Act of 2000.⁵⁷ The Preamble of the Convention makes specific references to state parties to the Convention to respect and protect the privacy of their citizens. Article 8 of the Convention specifically places the responsibility to fulfil the right to privacy on the states which includes strengthening of fundamental rights and public freedoms. While the Convention is not in force yet, with only seven member states signing the Convention and six countries (Ghana, Senegal, Mauritius, Guinea, Namibia and most recently, Rwanda) who have ratified it, the Convention provides a general direction for states to follow to ensure that citizens' right to privacy, including those of the civil society are fully respected, protected and fulfilled.

Perhaps, the most definitive proposal by the African Union on internet governance and rights and other information and communication technologies (ICT) tools is the African Union Declaration on Internet Governance adopted in Kigali in 2018.⁵⁸ The preamble of the Declaration recalls the commitment of member states to securing the right to freedom of expression and access to information online and offline and other human rights provided for in the African Union and the United Nations' instruments while laying emphasis on the United Nations General Assembly Resolution of 2011 that these rights must be upheld online as well as offline.

However, the path of the civil society in Africa has been defined by the political environment they found themselves. This also required having to adapt to debilitating situations of jail terms, being hounded by the state, deployment of state security to threaten and several other silencing tactics.⁵⁹ These challenges among others were the motivation for the then new African human rights architecture which was formed through the instrumentality of the African Charter. The African Commission and the African Court for Human and Peoples' Rights and the African Children's Rights Committee much later formed the three key tripods of upholding human rights values and development on

57 AU Convention on Cybersecurity and Data Protection https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 1 September 2019).

58 African Union Declaration on Internet Governance https://www.afigf.africa/sites/default/files/DeclarationonInternetGovernance_adoptedAUSummit2018.pdf (accessed 5 September 2019).

59 n 17 above.

the continent even when implementation of these values by states were bleak.⁶⁰ The symbiotic relationship between these three institutions and civil society in articles 10, 11, 30 and 55 of the African Charter is tightly knotted such that it sets the stage for the former to perform its functions as supranational human rights institutions that shine the light on states' human rights violations, the latter being ever-ready to hand them the torch.⁶¹ The agreement to infuse civil society and HRDs in the realisation of the mandate of the African Charter would prove revolutionary for the protection of human rights especially for HRDs in Africa.

Sifting through the mandates of the African Commission, it is not surprising that given the relationship between these two, civil society are involved in both the protective and promotional mandates of the Commission.⁶² In its promotional mandate, the two-pronged system of state reporting and special rapporteurs involve indispensable input of civil society and HRDs. The state reporting mechanism is such that each member states is enjoined to submit reports on the implementation of the human rights provided for under the African Charter. This traditionally gives opportunity to member states to render reports that may not be factually correct. As a result, upon the formalisation of 'shadow' reports in the Rules of Procedure of the African Commission in 2010, civil society have been encouraged to serve as a 'check' for the facts presented by states in their reports to the Commission before adoption. This is one of the several revolutionary ways through which HRDs have began to ensure the protection of human rights in Africa.

Additionally, in its promotional mandate, the Commission allows for special rapporteur mechanism in six key areas: extrajudicial, summary or arbitrary executions in Africa; prisons and conditions of detention in Africa; rights of women in Africa; refugees, asylum seekers and internally displaced persons in Africa; freedom of expression and access to information in Africa, and human rights defenders in Africa. The mechanism of the Special Rapporteur on Human Rights Defenders in Africa was established by Resolution ACHPR 69 (XXXV) 04 of 4 June 2004. The Special Rapporteur receives, examines and acts upon information about human rights defenders while also engaging

60 F Viljoen 'The African Union human rights architecture' in F Viljoen (ed) *International human rights law in Africa* (2012) 169; *Zongo v Burkina Faso* No. 013/2011, Judgment, African Court on Human and Peoples' Rights (28 March 2013).

61 Articles 10, 11, 30 and 55 of the African Charter provide for the right to freedom of association, assembly, establishment of the African Commission and the consideration of individual communications other than those from member states. These provisions work together to strengthen the influence of civil society and HRDs on human rights development in Africa. The substantive rights in articles 10 and 11 are implemented through the promotional and protective mandate of the African Commission by the input of civil society and HRDs.

62 The African Commission adopted its first Rules of Procedure in 1988 (1st Annual Activity Report) which allowed communications other than those of member states to be considered by the African Commission, Annex V; 2010 Rules of Procedure, rule 74(2) provides for civil society members to contribute to state reports; CE Welch *Protecting human rights in Africa: Strategies and roles of non-governmental organizations* (1995) 156.

government in dialogue. Depending on the circumstances, the Special Rapporteur has the power to send urgent appeals to heads of state on behalf of human rights defenders while also ensuring that human rights defenders' rights are protected.

An important aspect of the African Commission's protective mandate is receiving individual communications with respect to human rights issues over which it has jurisdiction. An individual or organisation that is not a state member may send a communication to the African Commission alleging violation of one or two more rights provided for under the African Charter or any other international human rights treaty. An individual communication in this case is usually civil society. Throughout the history of the African Commission, most communications to it have been through individual communications. This therefore reinforces the importance of civil society in the realisation of human rights in Africa.

Additionally, in the preamble of the African Commission's *Guidelines on Freedom of Assembly*, focus was placed on the impacts of technological development in the enjoyment of human rights. This focus was also tied to the growing incidents of state-sponsored restrictions of civil society and HRDs and why states must respect and protect the human rights through the civic space. Also, noting the indivisibility that is necessary in the enjoyment of all human rights,⁶³ the African Commission in its Declaration of Principles on Freedom of Expression in Africa considered and noted the role of media communications in making informed decisions and how information and communication technologies are now capable of realising human rights. The Commission also recognised the importance of digital communications and online participation as a means of preserving the civic space in Africa.⁶⁴

In the past, several civil society organisations and HRDs have had not only their physical space violated but also their online activities threatened and in some instances compromised.⁶⁵ In these instances, their rights to freedom of association and assembly online becomes violated while also infringing their rights to freedom of expression, access to information and privacy in the process. In several instances, websites of these civil society and HRDs have either been blocked or throttled by governments using electronic means of communications also that are also usually compromised usually by the state.⁶⁶

63 *Media Rights Agenda and others v Nigeria* Communication 105/93, African Commission on Human and Peoples' Rights, Twelfth Annual Activity Report (2000).

64 The African Commission on Human and Peoples' Rights adopted a revised Declaration of Principles on Freedom of Expression in Africa. Special Rapporteur on Freedom of Expression and Access to Information for Africa revised the Declaration to incorporate development in the freedom of expression and access to information spectrum and also in the digital age.

65 L Kuo 'African governments are stepping up surveillance of their own people' 16 October 2016 *QUARTZ* (New York) <https://qz.com/africa/525946/african-governments-are-stepping-up-surveillance-of-their-own-people/> (accessed 1 September 2019); B Okunoye & A Adegoke 'Internet freedom is the new press freedom' (2018) <https://paradigmhq.org/download/policy-brief-010-internet-freedom-is-the-new-press-freedom-an-africa/> (accessed 1 September 2019).

66 Paradigm Initiative & OONI 'Tightening the noose on freedom of expression' (2018) <https://paradigmhq.org/wp-content/uploads/2018/06/Nigeria-Report-v2.pdf> (accessed 1 September 2019).

In addition to these violations, state parties to the African Charter also do carry out indiscriminate surveillance of journalists, civil society members and HRDs.⁶⁷ Several millions of dollars are allocated to the procurement of spying machines without any meaningful details of its use.⁶⁸ Most arguments by state parties, in this regard, are that in order to safeguard national security, the state must carry out surveillance. However, how these measures of spying are carried out are not made clear.

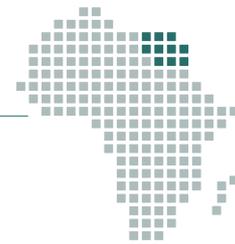
Given the several organisations and campaigns that have ran online to activate offline policy and political changes towards democratisation in Africa, it is only important that the civic space in Africa does not only require offline protections but also the online space where it is possible to achieve more democratic mobilisation in Africa. With these positions at the international and regional level on the need to protect the civil space, not only have there been pushbacks by the state through legislative restraints but also documented digital attacks that affect civil society and HRDs in carrying out their responsibilities across African countries. In order to substantiate these claims on the risks being faced by civil society in the region, the following country context are considered in this report.

67 B Abdul Razzak et al 'Hide and seek: Tracking NSO Group's Pegasus to 45 countries' 18 September 2018 <https://citizenlab.ca/2018/09/hide-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> (accessed 1 September 2019); See generally LA Abdulrauf 'The challenges for the rule of law posed by the increasing use of electronic surveillance in sub-Saharan Africa' 18 *African Human Rights Law Journal*.

68 Privacy International 'For God and my President: State of surveillance in Uganda' (2015) https://privacyinternational.org/sites/default/files/2018-02/Uganda_Report.pdf (accessed 1 September 2019); T Ilori 'Status of surveillance in Nigeria: Refocusing the beams' 2017 <https://qz.com/africa/525946/african-governments-are-stepping-up-surveillance-of-their-own-people/> (accessed 1 September 2019).



Cairo, Egypt, 4 February 2011 -
Egyptian revolution, flags in Tahrir Square
© Tarek Ezzat / Shutterstock



SECTION 2

Case study: Egypt

2.1 Country background

Egypt is party to international human rights instruments such as the African Charter), ICCPR, Convention against Torture and Other Cruel Inhuman or Degrading Treatment or Punishment (CAT), Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), International Covenant on Economic, Social and Cultural Rights (CESCR), among others. Egypt has had successive governments with almost similar approaches toward the civil society except during the Gamal Abdel Nasser administration, the second Egyptian President in 1956. Nasser's presidency embodied values of freedom and dignity. The assassination of President Anwar El Sadat in 1981 ushered in Hosni Mubarak as Egypt's fourth President until the 2011 revolution. President Mubarak subjected Egypt to an uninterrupted state of emergency throughout his tenure. The State Security Investigations Sector under Ministry of Interior habitually scrutinised NGOs although these powers were stipulated in the law. Under the President's emergency powers, critics were silenced, and fear spread amongst citizens as security forces arrested, detained and sentenced those suspected of being a threat to national security and public order.⁶⁹

President Mubarak was forced to step down in 2011 following demonstrations that were precipitated by calls for protests through social networks and eventually led to labour

69 S Brechenmacher 'Civil Society Under Assault: Repression and Responses in Russia, Egypt, and Ethiopia (2017) *Carnegie Endowment for International Peace* 38.

strikes and sit-ins that escalated into full-blown public protests. Grievances were mainly socio-economic -poverty, unemployment, corruption, social inequality and human dignity and calls for political and constitutional reform.⁷⁰ President Mubarak's stepping down, was followed by a transitional period (2011–2013) under the Supreme Council of the Armed Forces (SCAF) and the visible influence of the Muslim Brotherhood. This period was envisaged to transition Egypt to an open and democratic society. The SCAF undertook measures such as the adoption of constitutional reform and laws regulating political parties, disbanding the State Security Intelligence (SSI), issuing the constitutional declaration, and initiating a national dialogue on constitutional reforms. Other issues of national interest addressed by the SCAF include electoral law reform, adoption of pro-freedom of association measures and media related reforms such as appointment of new editors.⁷¹ However, there were concerns by the civil society that the SCAF did not adequately consult and open up space for civil society in initiating the reforms which undermined the right to participation in decision-making processes. The brief period following the revolution was a short-lived relief for the civil society as the environment flipped back to the repressive practices under the current presidency of Abdel Fattah el-Sisi.

The post-2013 phase under the current presidency of Abdel Fattah el-Sisi has seen Egypt being at the forefront of the global phenomenon of the shrinking of civic space.⁷² The atmosphere is characterised by authoritarianism with extreme restrictions on civil liberties. As a result, the general operating environment for civil society is dangerous with a solid government campaign against its critics. There are several digital attacks which intensify as citizens criticise the government particularly when the country is in election period. HRDs are targeted online as the legal framework is tailored to intimidate activists and HRDs, suppress freedom of expression, and undermine such rights as the right to privacy that are sacrosanct to the work and function of civil society. Concepts such as cyber security are misconstrued to attack activists online and what is otherwise legitimate behaviour, such as criticizing the government, is criminalised.

Typically, these digital threats against members of civil society are coded as anti-terrorism mechanisms.⁷³ The digital threats ultimately result in intimidation, forced disappearances, arrests, harassment, mostly by state security authorities. Categories of those that are mostly affected include bloggers, trade unionists, students, opposition political activists, lawyers, LGBTIQ and women's rights activists, and civil society organisations

70 Report of the Office of the United Nations High Commissioner for Human Rights (OHCHR) Mission to Egypt 27 March – 4 April 2011 https://www.ohchr.org/Documents/Countries/EG/OHCHR_MissiontoEgypt27March_4April.pdf (accessed 22 October 2019).

71 As above.

72 Brechenmacher (n 69 above).

73 International Service for Human Rights 'Let human rights defenders work for a better future' 18 October 2019 <https://www.ishr.ch/news/egypt-let-human-rights-defenders-work-better-future> (accessed 22 October 2019).

in general. The types of digital threats experienced in Egypt include digital surveillance, website blocking and internet shutdowns. These digital threats are happening at a time when the UN Human Rights Council has called on states to “respect and fully protect the rights of all individuals to assemble peacefully and associate freely, online as well as offline.”⁷⁴

2.2 National legislative framework

The Constitution

The Constitution guarantees basic human rights that are pertinent to the civil society such as freedom to form political parties, freedom of assembly, freedom of publication, freedom of the press, freedom of thought and freedom of association, right to form syndicates and join trade unions.⁷⁵

Non-Governmental Organisation laws

Law 348 of 1956 was enacted during the reign of Gamal Abdel Nasser. It restricted and controlled NGOs. According to this law, NGOs were expected to register with the Ministry of Social Solidarity (MOSS) and foreign funding for NGO was banned as NGOs could be closed for violating this law.⁷⁶ Law 162 of 1958 also known as the Emergency Law augmented state security powers, suspended constitutional rights and tremendously restricted fundamental rights and freedoms, banned strikes, restricted funding for NGOs, and suppressed government opponents through detention and torture mostly without any judicial protections.⁷⁷

Law 32 of 1964 was adopted following social and economic transformations that transpired in the 1950s and 1960s leading to steps being adopted to control NGOs. The law was in existence for about 40 years and gave the MOSS authority over the functioning of NGOs such that registration and deregistration of NGOs was at the benevolence of this ministry.⁷⁸ The criteria for deregistration was determined by factors such as threat to national security or engagement in activities that the ministry deemed undesirable

74 UN Human Rights Council Resolution on the rights to freedom of peaceful assembly and of association A/HRC/RES/24/5 (2013) para. 2.

75 International Centre for not for Profit Law 'Civic Freedom Monitor: Egypt' <http://www.icnl.org/research/monitor/egypt.html> (accessed 22 October 2019).

76 MM Abdelrahman 'Civil Society Exposed: The Politics of NGOs in Egypt' (2004) *Library of Modern Middle Eastern Studies* 40

77 Report of the Office of the United Nations High Commissioner for Human Rights (OHCHR) Mission to Egypt 27 March – 4 April 2011. https://www.ohchr.org/Documents/Countries/EG/OHCHR_MissiontoEgypt27March_4April.pdf (accessed 22 October 2019).

78 Abdelrahman (n 76 above).

for the community.⁷⁹ The ministry also had control over assets of NGOs, the nomination of boards and foreign funding. Penalty for violating this law was about six months' imprisonment.

Law 153 of 1999 was passed in 1999 supposedly to support civil society in Egypt. Only 13 NGOs participated in the drafting and the final law was criticised for not reflecting their recommendations. On the one hand, the government intensified control of NGOs by coercing organisations registered as civil companies to register as NGOs or face criminal penalties. On the other hand, the government relinquished some control by eliminating the MOSS' authority over NGO assets, its discretion on the desirability of NGO activities and authority over the appointment of NGO boards and power to dissolve NGOs without a court order.⁸⁰ Under Article 17, the law permitted foreign funding subject to the ministry's approval. The law was vehemently condemned by NGOs and was eventually annulled.

Law 84 also known as the Law on Associations and Community Foundations was adopted in 2002 with inadequate involvement of the civil society. It was an improved version preceding laws regulating NGOs but the challenge with the law was that the ministry maintained its grip on NGOs. In terms of article 11, registration of an organisation could be denied on the grounds of national security, morality, public order or engaging in trade union or political activities. This violated the freedom of association as stipulated in international human rights law and standards. According to article 7, appeals against the ministry's decisions were adjudicated before the Administrative Court while other disagreements were decided by a committee comprising a representative of the Court of Appeal and two government officials. This arrangement inevitably favoured the ministry.

In terms of articles 8 and 23, the ministry could reject NGOs laws or board decisions. The ministry required a 60-day notice prior to an organisation's board elections and could eliminate candidates from the elections. The law also permitted the ministry to disband an organisation albeit with a court order. In 2007, the Association of Human Rights and Legal Aid (AHRLA) was closed for working on cases of torture.⁸¹ Some procedural provisions included: the requirement for the organisation board to meet four times a year and an annual generally assembly for the organisation's members; the requirement to seek approval of an NGO's agenda from the ministry prior to holding a meeting and approval of foreign funding. There were also restriction concerning creating alliances with either local or international organisations. Benefits under this law included exemptions in paying customs duty, contracts registration fees, property tax, reduced phone charges, reduced transportation fees by rail, and subsidised utility charges or an oppor-

79 As above.

80 As above.

81 H Handoussa 'Egypt's Social Contract: The Role of Civil Society' (2008) *United Nations Development Program*.

tunity to have civil servants to work for NGOs at government cost. The provisions were vague and, thus, could be arbitrarily interpreted.⁸² Attempts to amend this law in 2013 were unsuccessful as the proposals were more repressive to NGOs.

Law 107 known as the Protest Law was enacted in 2013 under interim president Adly Mansour.⁸³ The law was designed to regulate public meetings, processions and demonstrations. The law gave security authorities the power to terminate or reschedule a demonstration for security reasons. Due to the law's vague provisions, security services thwarted demonstrations and protests using violent means. In addition, the 2014 presidential decree also extended the army's control over civilian infrastructure such that demonstrations outside public buildings were not allowed except by permit. A violation of this decree resulted in arrests and trials in military court.⁸⁴ Law 14 of 2017 amended Law 107 on the Right to Public Meetings, Marches and Peaceful Demonstrations. The amendments created more constraints on the governance, funding, and activities of the civil society locally and internationally. The authority to grant permission to protest is now under the judiciary instead of the Ministry of Interior.⁸⁵

Law 70 on Associations and Other Foundations Working in the Field of Civil Work regulates local and foreign (NGOs). Its provisions are on NGO funding, oversight, activities, monitoring and penalties for violations of the law. This law replaces jail time with fines, if the law is contravened. The law also eliminates the National Agency to Regulate the Work of Foreign NGOs that was in the previous NGO Law for monitoring NGOs especially their funding. In terms of the law, NGOs exist for social development only. Registration of organisations lies with the Ministry of Social Solidarity and can be cancelled in case of violation of the law. Opening of an NGO bank account is facilitated by the Ministry of Social Solidarity. The ministry also approves and registers foreign NGOs in liaison with the Ministry of Foreign Affairs. The law prohibits NGOs from conducting activities that infringe on national security, public order, public morals, and specifically outlaws prohibits activities that involves foreign liaisons, conducting surveys and polls or even use foreign expertise. Participating in international activities like workshops requires the ministry's approval. In terms of this law, foreign funding is approved by the Ministry of Social Solidarity. The law also establishes a Central Unit for Associations and Civil Work under the Ministry of Social Solidarity. The function of this entity is to provide oversight to NGOs and monitor them. In terms of this law the minister can suspend or dissolve an NGO activity for violating the law on national security reasons. The order can be reviewed through a court process.

82 C E Herrold 'NGO Policy in Pre- and Post-Mubarak Egypt: Effects on NGOs' Roles in Democracy Promotion Nonprofit Policy Forum Report' (2016) 196.

83 Brechenmacher (n 69 above) 43.

84 As above.

85 International Centre for Not for Profit Law 'Civic Freedom Monitor: Egypt' 30 October 2019 <http://www.icnl.org/research/monitor/egypt.html> (accessed 22 October 2019).

Anti-terrorism laws

Egypt's antiterrorism agenda surged and the government enacted Law 8 of 2015, Anti-Terrorism Law 33 of 2015 and Law 94 of 2015 on Combating Terrorism. Their provisions are similar. Law 8 of 2015 regarding the organization of terrorist entities and terrorists prohibits the infringement on national unity, peace, security, public order, safety, and impeding national laws. In terms of article 1, terrorist entities include an 'association, organization, group, gang, cell or other grouping that, through any means, either inside or outside the country, calls for the harming of individuals; the spreading of terror; or the endangering of the lives, freedoms, rights, or security of the people.'⁸⁶ The list also includes organisations that call for or involve themselves in harming the environment, natural materials, antiquities, the communication infrastructure, and land, air, or sea transportation, or harming or seizure of public or private funds, buildings, or properties. The article bans organizations that call for or are involved in the obstruction of public authorities, judicial agencies or bodies, government interests, local clinics, places of worship, hospitals, academic institutions, science institutes or other public facilities, or diplomatic missions.⁸⁷

Article 2 of the Law grants the Prosecutor-General the authority to create a list of organisations condemned as terrorist organisations and a list of individuals labelled as threats to national security. According to Article 3, the Court of Appeal has the authority to augment the list as and when it deems fit. In terms of article 6, those on the list can file petitions before the Court of Cassation for remedy. Article 7 provides for the freezing of bank accounts, dissolution and confiscation of property of local organisations and individuals on the list.⁸⁸

NGOs criticised the laws arguing that they could be used to arbitrarily target NGOs.⁸⁹ The broad and vague definitions contained in the law infringe on freedom of expression, freedom of assembly as acts such as criticizing the government and protests that could easily fall within definition of terrorism provided by the these laws.⁹⁰ The judiciary has applied the anti-terrorism laws broadly and as of January 2017, 1 538 citizens had been categorized as terrorists for alleged connections with the Muslim Brotherhood and slapped with travel bans, freezing of assets, and passport cancellations, with no

86 G Sadek 'Egypt: NGOs Protest Decree Defining Terrorist Organizations' 5 May 2015 *Global Legal Monitor* <https://www.loc.gov/law/foreign-news/article/egypt-ngos-protest-decree-defining-terrorist-organizations/> (accessed 22 October 2019).

87 As above.

88 As above.

89 E Hamed 'Egypt's terrorism law whittles down opposition' 2 March 2015 <https://www.al-monitor.com/pulse/en/originals/2015/03/egypt-sisi-anti-terrorism-law-opposition.html> (accessed 22 October 2019).

90 Sadek (n 86 above).

option of appeal.⁹¹ Such convictions affect one's right to participate in public life such as engaging in politics.

The challenge with the counterterrorism law is the overly broad definitions of what constitutes terrorism.⁹² It is in these broad terms that civic space is shrinking through restrictions on freedom of expression, undermining of the right to privacy, intimidation and harassment of journalists, HRDs and other activists under the ambit of counterterrorism endeavours. The ongoing state of emergency was imposed by the government in 2017 after terrorist attacks increased across the country, hence the intensification of the existing digital threats including internet shutdowns, surveillance, even restrictions to NGO funding from overseas.

Media laws

There are a number of laws that have been adopted that directly impact the work of civil society in that they infringe on freedom of expression. Egypt is one of those countries whose governments sought to silence independent and dissenting voices based on the conception that 'only the state can be trusted to separate truth from fiction'.⁹³ Such measures restrict freedom of expression. Law 92 of 2016 establishes the Supreme Council for Media Regulation which is an independent body that is responsible for media regulation. Its specific functions are to ensure the existence of a regulatory framework and standards for the media, ensure proper standards for media reports, imposing sanctions on those who violate the established rules. According to the Law Regulating the Press, Media, and the Supreme Council for Media Regulation (Law No. 180 of 2018), it is illegal to publish or broadcast content which is discriminatory, instigates racism, extremism or considered to be in violation of public order and security, professional ethics, country's morals and the constitution. It also gives the Media Regulation body the authority to block publications from outside the country for national security reasons. It also prohibits publishing of false news. Platforms such as personal websites, blogs or social media accounts with at least 5,000 subscribers are categorised as media outlets and

91 Brechenmacher (n 69 above) 47.

92 'Digital Authoritarianism in Egypt: Digital Expression Arrests' 2011-2019 (2019) *Open Technology Fund* 46. The Counter-terrorism laws defines terrorism as "any use of force, violence, threat, or intimidation domestically or abroad for the purpose of disturbing public order, or endangering the safety, interests, or security of the community; harming individuals and terrorizing them; jeopardizing their lives, freedoms, public or private rights, or security, or other freedoms and rights guaranteed by the Constitution and the law; harms national unity, social peace, or national security or damages the environment, natural resources, antiquities, money, buildings, or public or private properties or occupies or seizes them; prevents or impedes public authorities, agencies or judicial bodies, government offices or local units, houses of worship, hospitals, institutions, institutes, diplomatic and consular missions, or regional and international organizations and bodies in Egypt from carrying out their work or exercising all or some of their activities, or resists them or disables the enforcement of any of the provisions of the Constitution, laws, or regulations".

93 A Shahbaz Freedom on the Net 2018: The Rise of Digital Authoritarianism :Fake news, data collection, and the challenge to democracy <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism> (accessed 22 October 2019).

required to register.⁹⁴ The presidential decree issued in February 2018 authorized the prosecutor-general to monitor websites and social media accounts; identify

false news and other content that threaten national security, inculcate fear or jeopardise public interest and those found in violation of the decree will be criminally liable. Under the decree citizens are expected to report any violations to the Public Prosecution.⁹⁵

Law 175/2018, the Anti-Cyber and Information Technology Crimes Law

The law is directed at internet users and service providers and it regulates online activities. It covers aspects such as privacy, national security, confidentiality, content and data offences. In terms of Article 7, investigating authorities have the power to block websites whose content is a threat to the economy or nation.⁹⁶ The order to block a website has to be validated by a judge. According to article 9, a travel ban may be imposed by the public prosecutor on those suspected of contravening this law.⁹⁷ In terms of article 6, service providers are expected to make available users' information upon request by state authorities for investigating crimes under this law.⁹⁸ Under article 3, non-Egyptians can be held liable for crimes committed outside Egypt but punishable under this law on condition that the crime in question is also punishable in the country in which it was committed.⁹⁹ In terms of article 25, it is illegal to contravene national principles, family values or to invade privacy.¹⁰⁰

The Penal Code

The Penal Code is one of the laws that contributes to the closing of civic space in Egypt, and even more repressive than the NGO Law. Under the penal code, assets could be frozen and travel ban imposed for vague criminal charges mostly associated with terrorism.¹⁰¹ Article 78 as amended by the 2014 presidential decree provides for penalties of up to 25 years in prison for receipt of foreign funding for undertaking activities deemed

94 TIMEP 'The Law Regulating the Press, Media, and the Supreme Council for Media Regulation' 15 May 2019 <https://timep.org/reports-briefings/timep-brief-the-law-regulating-the-press-media-and-the-supreme-council-for-media-regulation/> (accessed 22 October 2019).

95 As above.

96 Anti-Cyber and Information Technology Crimes Law 2018 art 7.

97 As above, art 9.

98 As above, art 6.

99 As above, art 3.

100 As above, art 25.

101 CIVICUS 'interview with Mohamed Zaree, a human rights activist and legal expert' <https://www.civicus.org/index.php/fr/component/tags/tag/egypt> (accessed 22 October 2019).

detrimental to national security.¹⁰² The amendment incapacitates NGOs as it criminalises their public and peaceful activities and jeopardizes possibilities of liaison with international counterparts.¹⁰³

Case No. 173 of 2011

In late 2011, Egyptian authorities raided democracy and human rights-focused local and international NGOs. Only foreign workers from international organisations were charged and convicted. In 2013, several international NGOs were closed for operating illegally. Since 2015, President al Sisi's regime has also resuscitated the case and targets prominent human rights organisations. The trial of Egyptian organizations, NGO workers and lawyers was initiated in a case that has been referred to as Case No. 173 (2011). A number of organisations were persecuted under this case mostly on issues related to foreign funding.¹⁰⁴ Other organisations were raided, surveyed, interrogated, and subjected to travel bans as well as freezing of assets.¹⁰⁵

2.3 Digital threats to civil society

Digital security experts interviewed during this study confirmed that there is a general belief that the Egyptian government is willing to implement stringent laws and measures to enhance surveillance and censorship. Since its elections in 2015, Egypt has heavily invested in technology for online surveillance and website blocking and throttling when necessary.

2.3.1 Access to internet and network disruptions

As of 2018, internet penetration was at 39.2%. The prominent Internet Service Providers (ISPs) are Orange, Vodafone Egypt, Etisalat Misr and Telecom Egypt while the Egyptian telecommunications Regulator is the National Telecom Regulatory Authority (NTRA).¹⁰⁶ The special mechanisms of the UN, ACHPR, Organization of American States (OAS) and the Organization for Security and Co-operation in Europe (OSCE) have reiterated that access to internet is a facilitator in the enjoyment of human rights such as the right

102 'Egypt: Events of 2016' *Human Rights Watch* (2016) <https://www.hrw.org/world-report/2017/country-chapters/egypt> (accessed 22 October 2019).

103 A Hamzawy 'Egypt's anti protest law: Legalising authoritarianism: How the Egyptian regime used the law to crack down on opposition and isolate voices of dissent 24 Nov 2016 <https://www.aljazeera.com/indepth/features/2016/11/egypt-anti-protest-law-legalising-authoritarianism-161107095415334.html> (accessed 22 October 2019).

104 E Miller and M Suter 'Case No. 173: The State of Egypt's NGOs', 29 March 2016 <https://www.atlanticcouncil.org/blogs/menasource/case-no-173-the-state-of-egypt-s-ngos/> (accessed 22 October 2019).

105 Brechenmacher (n 69 above) 45.

106 'Legislating Restrictions: How African Governments Use Repressive Laws' (2018) *Paradigm Initiative Digital Rights Africa Report* 16.

to freedom of peaceful assembly.¹⁰⁷ Thus, undue restrictions on the internet are inconsistent with international human rights standards and norms. Internet controls and restrictions impact human rights negatively, particularly on the civil society as they rely heavily on the internet for information dissemination and mobilization.

Network disruptions are a common occurrence in Egypt's digital landscape and violate the right to freedom of expression and access to information. From the beginning of 2017 and February 2018, about 500 websites mostly run by political parties, human rights organisations, private media entities and influential bloggers had been blocked.¹⁰⁸ In addition to websites authorities also blocked VPNs and other tool used to circumvent network disruptions.¹⁰⁹ In addition, Accelerated Mobile Pages (AMP) have also been blocked.¹¹⁰ AMPs make it easy for publishers to create mobile-friendly content that will instantly load on a mobile phone. The main media regulatory body, the Supreme Media Regulatory Council (SMRC), has the power to license, block or halt the activity of websites and this restricts freedom of expression and access to information. The same body monitors personal blogs, personal profiles or personal web pages that have more than 5000 followers, mainly targeting social media influencers.¹¹¹ Under this law, the punishment for press violations has increased since it includes revocation of licensing, blocking and payment of fines.¹¹² Visiting banned websites is also a crime.

The Counterterrorism Law, Penal Code, Telecommunications Law, Cybercrime Law and the Media Regulation Law provisions on "spreading false news," "joining a banned group" and "misuse of social media" are used to arrest HRDs and other activists for expressing themselves online. The curtailment of the freedom of expression online undermines the potential of the internet to be a safe space for the civil society; and this then undermines the freedoms of association and assembly online, as they are dependent on the freedom of expression.

107 UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and African Commission Special Rapporteur on Freedom of Expression and Access to Information, Joint declaration on freedom of expression and the Internet, 1 June 2011, para. 6(b).

108 Freedom House report (2018) <https://freedomhouse.org/country/egypt/freedom-net/2018> (accessed 10 November 2019).

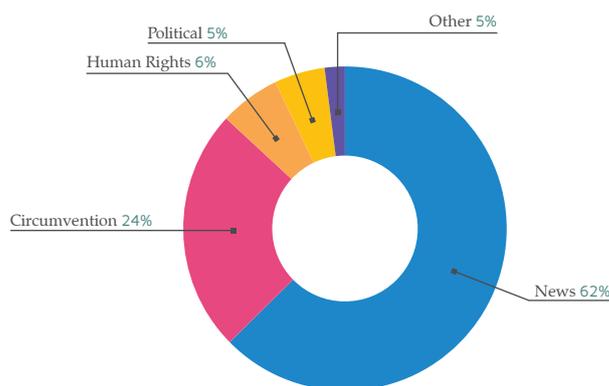
109 As above.

110 Y Auf 'The state of emergency in Egypt: An exception or rule?' (2018) <https://www.atlanticcouncil.org/blogs/menasource/the-state-of-emergency-in-egypt-an-exception-or-rule> (accessed 10 November 2019).

111 R Mamdouh 'Egypt new media law rearranging legislative building blocks to maximize control' (2018) <https://madamasr.com/en/2018/07/17/feature/politics/egypts-new-media-laws-rearranging-legislative-building-blocks-to-maximize-control/> (accessed 10 November 2019).

112 L Bird 'Egypt is seizing control of the internet' (2018) *Popular* <https://popula.com/2018/10/23/egypt-grabs-control-of-independent-media/> (accessed 10 November 2019).

Blocked websites in Egypt Categories of blocked websites



Source: The State of Internet Censorship in Egypt, 2nd July 2018

2.3.2 Infringements on freedom of expression online and online violence

Freedom of expression is guaranteed under the Egyptian constitution. It provides that ‘the state shall protect the rights of citizens to use all forms of public means of communication, which may not be arbitrarily disrupted, stopped or withheld from citizens, as regulated by the law.’¹¹³ However, there are no enabling laws to facilitate its enjoyment. Instead, the constitution exists alongside repressive laws that are used to threaten, harass, intimidate and persecute human rights defenders, lawyers, journalists and other media practitioners for expressing themselves. These laws are the Penal Code, Telecommunications Regulation Law, the Counterterrorism Law, the Assembly Law, and the Protest Law. Laws governing NGOs, restrict freedom of expression. The defamation and insult laws, as captured under the Penal Code impose criminal penalties against activists and government critics. This affects mostly those in the civil and political movements as that work is defined as that of a political nature, which is prohibited. While the negative effects of terrorism are acknowledged, it is unfortunate that the government is using counterterrorism methods as a legal basis for the infringement of citizens’ freedom of expression.¹¹⁴ Anti-government sentiments are viewed through the lens of terrorism. Repressive legislation such as the Anti-Terrorism Law of 2015 have been deployed to gag free speech.¹¹⁵

113 2014 Constitution of the Republic of Egypt, art 70 & 71.

114 Committee to Protect Journalists ‘Egypt- new anti-terrorism law deepens crack dawn on the press’ <https://cpj.org/2015/08/egypts-new-anti-terrorism-law-deepens-crackdown-on.php> (accessed 22 October 2019).

115 As above.

Publishing of false news is said to have the potential to disturb public security, terrorise people or harm the public interest and those guilty of violating the law shall be liable to imprisonment and a fine.¹¹⁶ The crime of spreading false news affects poets, journalists, digital rights activists and other categories of the civil society who are often branded as terrorists in terms of the counter-terrorism laws.¹¹⁷ According to Amnesty International, in 2018 alone, at least 111 individuals were detained for denouncing sexual harassment, tweeting, criticising the president or speaking about the deteriorating human rights situation in the country. Although some are not physically in prison, they are not free to exercise their rights.¹¹⁸ As of February 2019, 19 journalists had been reportedly imprisoned under Sisi's presidency and many civil society activists and HRDs have been banned from travelling and civil society organisations' assets were frozen.¹¹⁹ As a result, Reporters Without Borders labelled Egypt as 'one of the world's biggest prisons for journalists'¹²⁰

Organisers of demonstrations and protests that are initiated through social media platforms such as Facebook are obvious targets.¹²¹ The Anti-Cyber and Information Technology Crimes Law essentially penalises activists for using digital technologies. Through this law, the government can block websites that are deemed a threat to state security or incite violence through digital platforms.¹²² According to a research conducted under the Open Technology Fund, from the beginning of 2016 to mid-2019, about 333 instances of digital expression-related violence were reported and the figure continues to rise.¹²³ According to this research, those arrested were mostly journalists and other media practitioners such as bloggers, vloggers, satirists and social media personalities.

The Counter-terrorism laws muzzle independent media. Under this law, prosecutors can prosecute private media houses and entities using vague terrorism charges and police have expansive mandate to monitor online content that is considered a threat to state security and block websites that publish material that jeopardizes national security.¹²⁴ Also, the prolonged state of emergency tightens the government's grip on the

116 Penal Code Art 102.

117 JC York and M Hunasikatti 'Egypt's Draconian New Cybercrime Bill Will Only Increase Censorship' (2018) Electronic Frontier Foundation <https://www.eff.org/deeplinks/2018/07/draconian-new-cybercrime-bills-vietnam-and-egypt-will-only-increase-censorship> (access 28 October 2019).

118 'Egypt: Unprecedented crackdown on freedom of expression under al-Sisi turns Egypt into an open-air prison (2018) *Amnesty International* <https://www.amnesty.org/en/latest/news/2018/09/egypt-unprecedented-crackdown-on-freedom-of-expression-under-alsisi-turns-egypt-into-openair-prison/> (accessed 2 November 2019).

119 E Sayadi 'More Than 500 Sites Blocked Ahead of the Presidential Election' (2018) *Accessnow* <https://www.accessnow.org/egypt-more-than-500-sites-blocked-ahead-of-the-presidential-election/> (accessed 2 November 2019).

120 One of the world's biggest prisons for journalists' (2019) *Reporters Without Borders* <https://rsf.org/en/taxonomy/term/156> (accessed 6 November 2019).

121 'Digital Authoritarianism in Egypt: Digital Expression Arrests' 2011-2019 (2019) *Open Technology Fund* 53.

122 York and Hunasikatti (n 117 above).

123 Digital Authoritarianism in Egypt (n 121 above).

124 UN experts urge Egypt to end crackdown on protesters and human rights defenders <https://www.ohchr.org/EN/>

media disguised as protection against terrorist attacks.¹²⁵ The use of State Security Prosecution (SSP) to investigate digital expression cases instead of the regular courts condemns suspects to long periods of pre-trial detention and heavy punishments as they will be under a body whose jurisdiction is mainly national security and terrorism cases which have their own special procedures.¹²⁶ The UN has condemned the use of counter-terrorism laws to clamp down on government critics or activists and promoting human rights. It is basically incompatible with human rights norms and standards.¹²⁷

Women and sexual minorities activists face online harassment by state agents who monitor their online behaviour.¹²⁸ Police target gay dating apps such as Grindr and Hornet to arrest those who belong to the LGBTIQ community. An estimated 230 of such arrests were made between October 2013 and March 2017 as documented by the Egyptian Initiative for Personal Rights.¹²⁹ Women's rights activists also face persecution for the activities that they conduct in the digital space such as posting messages on social media platforms. A case in point is that of a women's rights activist, Amal Fathy, who was arrested for a video posted on Facebook criticising the government for its failure to curb sexual harassment and address the general human rights situation in the country. She was accused of promoting terrorism, disturbing peace, spreading false news and publicly inciting to overthrow the government through disseminating a video on social media.¹³⁰ Mona el-Mazboh, a Lebanese tourist, complained of sexual harassment, theft and poor restaurant service in a video she had uploaded on Facebook. She was arrested and sentenced to eight years in prison. She was charged with "*deliberately spreading false rumours that would harm society, attacking religion, and public indecency*".¹³¹

NewsEvents/Pages/DisplayNews.aspx?NewsID=25217&LangID=E (accessed 2 November 2019).

125 E Sayadi (n 119 above).

126 Digital Authoritarianism in Egypt (n 121 above).

127 UN Experts (n 124 above).

128 A Aboulenein 'Egypt "hunting down" gays, conducting forced anal exams' (2017) <https://www.reuters.com/article/us-egypt-rights/egypt-hunting-down-gays-conducting-forced-anal-exams-amnesty-iduskcn1c50d3> (accessed 10 November 2019).

129 Privacy International 'Communities at risk: How security fails are endangering the LGBTIQ+ community' 15 April 2019 <https://privacyinternational.org/news-analysis/2782/communities-risk-how-security-fails-are-endangering-lgbtq-community> (accessed 10 November 2019).

130 Freedom House Report (2018) <https://freedomhouse.org/country/egypt/freedom-net/2018> (accessed 10 November 2019).

131 H Ahmed 'Egypt set to release Lebanese tourist jailed over Facebook post' (2018) <https://www.reuters.com/article/us-egypt-politics/egypt-set-to-release-lebanese-tourist-jailed-over-facebook-post-idUSKCN1LP0ME> (accessed 10 November 2019).

2.3.3 State surveillance

Surveillance is a significant concern in Egypt and the country is intensely investing in surveillance technologies for digital surveillance and website blocking and throttling. The security equipment and surveillance technologies are sourced from European companies such as Blue Coat¹³² to boost the state's surveillance powers. The surveillance activities, hacking and malware as well as other forms of attacks on civil society activists mostly online, creates a repressive environment that restricts online expression.¹³³ The legal framework is designed to enable surveillance activities by security authorities.¹³⁴ Constitutionally, private communications "may only be confiscated, examined, or monitored by causal judicial order, for a limited period, and in cases specified by the law."¹³⁵ However, there is lack of transparency in the surveillance regime and this inevitably violates the right to privacy as guaranteed in the Constitution.¹³⁶

The Telecommunication Regulation Law governs the interception of telecommunications and establishes the National Telecommunication Regulatory Authority (NTRA) whose mandate is to regulate internet service providers (ISPs) and mobile network service operators. In terms of this law, telecommunications operators are required to provide all technical and software necessities for surveillance purposes by the army and law enforcement agencies. The same law prohibits encryption. The Cybercrimes Law of 2018 also facilitates surveillance activities. It makes it mandatory for ISPs to retain data and avail it to security agents upon request. There are several intelligence-gathering entities - Homeland Security (or Keta' El Amn El Watani), the Egyptian Military Intelligence, the Administrative Oversight Authority (AOA), Technical Research Department (TRD) and the Ministry of the Interior (MOI) which is mostly responsible for mass surveillance and social media monitoring.¹³⁷

Types of surveillance

a) Cerebro Software

This is one of the main softwares that the Egyptian government purchased since 2017 for surveillance. The software enables Egyptian authorities to conduct comprehensive surveillance of communications through the Deep Packet Inspection,

132 J Porup, "European spy tech sold to ultra-secret branch of Egyptian gov't, claims new report," *Ars Technica*, 25 February 2016, <http://arstechnica.co.uk/security/2016/02/european-spy-tech-sold-to-secret-branch-of-egyptian-intelligence-claims-new-report/> (accessed 10 November 2019)

133 Joint Motion for a Resolution http://www.europarl.europa.eu/doceo/document/RC-9-2019-0138_EN.html (accessed 2 November 2019).

134 Digital Authoritarianism in Egypt: Digital Expression Arrests 2011-2019 (2019) *Open Technology Fund* 3.

135 'Statement opposing Egypt's legalisation of website blocking and communications surveillance' September 2018 <https://www.apc.org/fr/node/34884> (accessed 2 November 2019).

136 Freedom House Report (2018) <https://freedomhouse.org/report/freedom-net/2018/egypt> (accessed 10 November 2019).

137 n.92 above, 53.

including voice calls, text messages, emails, instant messages, social networks, and search histories.¹³⁸

b) Pegasus Spy Software

This software is used by the Egyptian government to gain access to one's device and stored data (passwords, calendar, contacts, SMS records, browsing history and direct call applications). A phishing link is sent to the target person who when they click it, it downloads and installs Pegasus in the background without the user knowing which then bypass all the digital protection features that might have been set up on the mobile device.

c) Bank Transactions

It is also believed that the Egyptian government is monitoring the bank accounts for the various CSOs and HRDs within the country. This enables the government to monitor the money coming in or out of the bank account and gives them the power to ask the CSO or HRD where the funds are coming from and for what purpose. If necessary, the government has the power to close or freeze these funds through the bank itself.

d) Use of Deep Packet Inspection (DPI) equipment

It was noticed that the internet service providers (ISP) were interfering with Secure Socket Layer (SSL) encrypted traffic between Cloudflare's Point-of-Presence which is in Cairo and the backend servers of sites which are located outside Egypt.

Thus, using the abovementioned framework and tools, the government conducts surveillance that targets citizens in general and the civil society in particular. The surveillance practices become the basis for arresting activists as Facebook demonstrations and videos are closely monitored and targeted.¹³⁹

2.4 Egypt summary table

YES Hacking	YES Digital Surveillance	YES Website Throttling or Website Blocking	YES State sponsored attacks on CSOs and HRDs
-----------------------	------------------------------------	--	--

138 I Oribabor and P Micek 'Shutdowns, surveillance, and censorship: UPR reviews highlight threats to digital rights' 20 May 2019 <https://www.accessnow.org/shutdowns-surveillance-and-censorship-upr-reviews-highlight-threats-to-digital-rights/> (accessed 11 November 2019).

139 n.92 above, 8.

2.5 An analysis of the country context in Egypt

As indicated in the African Commission's Guidelines on Freedom of Association and Assembly in Africa, limitations on the rights to freedom of association and assembly weaken the full potential of civil society, undermines the potential for a free civic space in an open democratic society, hampers the functions of HRDs and ultimately compromises the enjoyment of human rights.¹⁴⁰ Egypt has experienced various political and security developments that have negatively impacted civil society as an important constituent in a state. The legal framework and practice in Egypt are in violation of its own constitutional provisions that guarantee fundamental rights pertinent to civil society - freedom of political participation, freedom of assembly and freedom of expression. However, the successive laws regulating the activities of NGOs, for example, sought to suppress civil society. This is also in violation of instruments such as the African Charter, the ICCPR and other international standards that Egypt is party to. These instruments are explicit of such rights. The African Commission's resolution on 5/1992 on the Right to Freedom of Association, places emphasis on the need for authorities to recognise the importance of civil society and to be cognizant of the obligation under the African Charter in terms of the enjoyment of the right to freedom of association.¹⁴¹

It is now generally accepted and recognized that the rights that people have offline should also be applied online. In Egypt, adoption of laws such as the Cybercrime Law and Media Regulation Law are curtailing human rights online.¹⁴² The law permits surveillance by state and security authorities and data retention by telecom service providers. In essence, the right to privacy is undermined. If authorities have unfettered control and access online, critics of the government are not safe. This is exacerbated by the strong regulation on encryption as provided for under the Telecommunication Regulation Law.¹⁴³ Such laws 'restrict digital rights and interfere with activists' freedoms online'.¹⁴⁴ Concerning privacy and surveillance, the Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa state that:

Measures used to counter terrorism that interfere with privacy (in particular body searches; house and property searches; bugging; telephone tapping; surveillance of correspondence and metadata; electronic monitoring; use of undercover agents; and receipt, collection, access, use, storage, maintenance, examination, disclosure, destruction, and intra- and interstate dissemination and sharing of privacy information, including through the use of databases) must

140 Guidelines on Freedom of Association and Assembly in Africa Preamble.

141 African Commission's resolution on 5/1992 on the Right to Freedom of Association.

142 Privacy International "State of Privacy Egypt" <https://privacyinternational.org/state-privacy/1001/state-privacy-egypt> (accessed 2 November 2019).

143 As above.

144 As above.

be provided for by law, strictly proportionate with and absolutely necessary for achieving a legitimate goal, conducted in a manner consistent with human dignity and the right to privacy, and as otherwise permitted under international human rights law.

As observed in the research findings, the government has unlimited access to communicated data. Associations and individuals whose rights to freedom of association and privacy have been violated through illegitimate surveillance should be afforded appropriate redress. Locking of websites mostly under the pretext of preventing the spread of false news and national security is also not in line with international human rights norms and standards and a violation of freedom of expression and access to information in particular. The vague and excessively broad provisions in the laws inevitably places CSOs, HRDs and activists - in general - at risk online and offline considering that their activities could be interpreted as violating the laws when viewed from the lens of public order, national security or even morals. For example, HRDs working on political participation could be persecuted as their activities fall within prohibited activities under the counter-terrorism laws.

2.6 Recommendations for Egypt

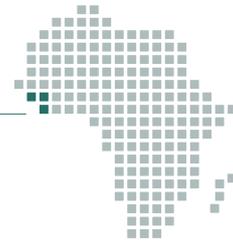
Government should fulfil its international human rights obligations through adoption of legal and other measures that protect and promote human rights and where rights are limited, the three-part test of legality, necessity, and proportionality should be the standard to justify any restrictions to human rights.

Specifically, the government should:

- Repeal or revise laws and practices that curtail the existence and functioning of civil society such as the NGOs and align counter-terrorism initiatives with international standards;
- Adopt measures that promote internet freedom and promote human rights online in line with international human rights standards;
- Align surveillance regime with the UN Principles on surveillance;
- Promote dialogue on the role of civil society in a democracy include civil society consultations in Government should;
- Promote access to reliable information and tackle disinformation through research, digital literacy and promote multi-stakeholder dialogue on curbing disinformation; and
- Promote capacity building for various stakeholders including regulators, law enforcement, judicial authorities, legislative bodies on human rights in the digital age.



People along the Makeni highway
in Sierra Leone
© Roberto Nencini / Shutterstock



SECTION 3

Case study: Sierra Leone

3.1 Country background

Sierra Leone gained independence in 1961 and had her first post-independence elections in 1962. There was relative democratic development until 1967 when three military coups ousted elected governments. This lasted until 1968 when promises of a multi-party democracy dissolved Sierra Leone into a one-party state. Within this period, Sierra Leone witnessed several political upheavals including a rebellion, military coup and authoritarian regimes. This was the case until 1991 when the civil war broke out. During the civil war, democratic power was briefly restored from 1996-1997 until the military coup in 1998.¹⁴⁵ For more than four decades, Sierra Leone struggled with its democracy and also went through a protracted civil war which ended in 2002 during which several human rights violations were committed. During these political challenges, Sierra Leone enacted its Constitution in 1991 which also provided for fundamental rights. Since 2002, the country has had four elections to nurture its democratic development.¹⁴⁶ Economically, in the 2018 Human Development Index, Sierra Leone was ranked 184 out of 189 countries with an estimated 53% of Sierra Leoneans living below the poverty line.¹⁴⁷

¹⁴⁵ D Harris *Sierra Leone: A political history* (2014) 63-101.

¹⁴⁶ Electoral Institute for Sustainable Democracy in Africa (EISA) 'Election Observation Mission to the 2018 Elections in Sierra Leone - Preliminary Statement' (2018) 2 <https://www.eisa.org.za/pdf/sie2018eom1.pdf> (accessed 10 November 2019).

¹⁴⁷ <https://www.wfp.org/countries/sierra-leone> (accessed 12 October 2019).

3.2 National legislative framework

In what is regarded as the constitutional protection of individual fundamental human rights in Sierra Leone, section 15 of the *Constitution of Sierra Leone of 1991* as amended provides for a cluster of human rights. They include freedom of expression, association and assembly broadly qualified by the right of others and public interests. These qualifications are also part of the more substantive provisions of the right to privacy, freedom of expression and the press and association and assembly in sections 22, 25 and 26 of the Constitution, respectively. While these constitutional provisions are not markedly different from the requirements under international human rights law, laws that are enacted to restrict these constitutionally guaranteed rights are also required to be in compliance with the Constitution and international human rights norms and standards as explained above.¹⁴⁸ There are however laws and policies in Sierra Leone that require legal analysis against this requirement. Sections 2 and 3 of the Public Order Act of 1965 criminalises public insult, provocation and insulting conduct. Anyone who uses words that are ‘insulting’, ‘abusive’, ‘offensive’ or sends or delivers ‘obscene writing’, ‘picture or other representation’ or calls any person by a name or description other than his own with ‘intent to insult or annoy’ is liable to twenty Leones or imprisonment for a period of three months or both. Section 27 of the Act provides for the offence of false defamatory libel and anyone found guilty of the offence is liable to a jail term of three years or 1000 Leones or both.

The Act in Section 32 provides for the offence of false news which criminalises ‘false statement, rumour or report which is likely to cause fear or alarm to the public.’ The offense is punishable by three hundred Leones or twelve months in jail or both. This punishment also extends to anyone who seeks to bring to disrepute any person whose office is constitutionally provided for and the reputation of the government of Sierra Leone through false news. Section 33 of the Act also provides for punishment of seditious libel and intention which includes exciting disaffection against the government of Sierra Leone and raising discontent among Sierra Leoneans for a period of three months in jail or a fine of one thousand Leones or both.

In the new Development Cooperation Framework, (DCF) to be implemented from 2019 to 2023 by the Ministry of Planning and Economic Development (MoPED) in Sierra Leone, the Government of Sierra Leone recognises the opportunities in international partnerships including the AU Agenda 2063. This suggests a recognition of supra-national policy direction of the African Union which includes ensuring the protection and promotion of the rights provided for under the African Charter to which Sierra Leone

¹⁴⁸ n 25 above.

is party.¹⁴⁹ Part of the principles underpinning the DCF is also the need to recognise the important roles of NGOs in Sierra Leone.¹⁵⁰ Part Five of the DCL provides for requirements for the establishment of NGOs in Sierra Leone. It requires NGOs to align their objectives with the development policies of the government of Sierra Leone.¹⁵¹ It defines the scope and number of categories NGOs are required to operate and how they must obtain approval from MoPED before engaging in any other objective even if it may be related to their scope of work. There is also the requirement that NGOs must have a local bank account and the ability to secure funds for its operations is a criterion for renewing an NGO's license.¹⁵²

Another requirement for NGOs registering with the government of Sierra Leone through the Framework is the monitoring of funds, budget and costs for the NGOs by the government.¹⁵³ It also requires an NGO to have at least four staff members excluding messengers and drivers.¹⁵⁴ It places restrictions on the number of expats that may work in an NGO while also requiring that work permits must be renewed for each new NGO that an expat is to work with. Furthermore, a Service Level Agreement (SLA) prepared by the relevant Ministry must be signed and agreed to by NGOs willing to operate in Sierra Leone.¹⁵⁵ Such SLA is provided by the respective sector or ministry the NGO is willing to operate. Failure to comply with these requirements results to disqualification of the NGO's application.¹⁵⁶ For new International Non-Governmental Organisations (INGOs), they are required to pay a registration fee of US\$2 500 and for local NGOs, Le 2 500 000 (US\$260).¹⁵⁷

Additionally, when the MoPED refuses a new application on the second try, there is no right of appeal.¹⁵⁸ NGOs are required to renew their registration every two years together with compliance reporting and audit requirements.¹⁵⁹ Other parts of the Framework limit the scope of NGOs to improving social and economic well-being within Sierra Leone.¹⁶⁰ These suggest that there is a pre-existing template of operations that NGOs must conform to. Failure to comply with these requirements and other restrictions may result into criminal prosecution and final suspension of an NGO's activities.¹⁶¹

149 Sierra Leone ratified the African Charter in 1983, <https://www.achpr.org/statepartiestotheafricancharter> (accessed 15 August 2019).

150 Development Cooperation Framework, 4.

151 as above, 10-11.

152 n 150 above.

153 n 150 above, 16.

154 n 150 above, 12.

155 as above.

156 n 150 above, 22.

157 n 150 above, 13.

158 as above.

159 as above.

160 as above, 14.

161 n 154 above.

In comparison to the laws and policies above, on 29 October 2013, the government passed the Right of Access to Information Act. The Act is a positive step towards making the government more open and its information more accessible. This right to access information also includes those of private bodies. In sharp contrast to these laws that adversely impact on NGOs and HRDs, the Human Rights Defenders Network of Sierra Leone developed a draft bill for the protection of HRDs and civil society in Sierra Leone called the *Human Rights Defenders bill*.¹⁶² This bill which has already been presented to the Office of the Attorney-General of Sierra Leone is yet to go through any meaningful review both by the Attorney-General's Office or the legislative arm of the government of Sierra Leone.¹⁶³

The bill defines HRDs as persons acting individually or together with others to seek protection and promotion of human rights at national, regional and international level. It also defines HRDs to include organisations with the mandate to protect and promote human rights at all levels as the same as HRDs.¹⁶⁴ Sections 1 to 6 of the draft provides for the rights of HRDs which include rights to freedom of association and assembly, access to information and freedom to communicate with and cooperate with international and regional human rights mechanisms, freedom of expression, privacy, solicit, receive and utilise resources, rights of women human rights defenders, respectively. Section 7 of the draft bill proposes that the limitation of the rights provided be in compliance with international human rights norms of reasonableness, necessity and proportionality, recognition and respect of the human rights and fundamental freedoms of others and meeting the requirements of public order and general welfare in a democratic society.

Section 15 of the bill provides for an internal administrative mechanism called 'the Human Rights Defenders Steering Committee' which shall see to the operationalisation of the bill. The bill also provides for collaboration between human rights defenders, national regulatory bodies and international human rights mechanisms.¹⁶⁵

3.3 Human rights and the civic space online in Sierra Leone

There are more than 900 000 internet users in Sierra Leone making up 11.4% of the population.¹⁶⁶ Many of this number use popular social media platforms like Facebook, Twitter and WhatsApp. While the internet penetration in the country may be minimal, human rights protection and promotion online has nonetheless been vibrant. However, due to this vibrancy among the online population in Sierra Leone, there have been documented cases of digital surveillance, website throttling and blocking during protests

162 Interviewee from Sierra Leone.

163 as above.

164 Part I of the draft bill.

165 Part V of the draft bill.

166 <https://www.slideshare.net/DataReportal/digital-2018-sierra-leone-january-2018> 8 (accessed 15 August 2019).

and elections in Sierra Leone. While not all the four categories of state-sponsored threats are documented in Sierra Leone, some are, which further raises challenges on how the government of Sierra Leone complements offline legal and physical threats with online attacks of civil society and HRDs.

Digital surveillance

The government of Sierra Leone in November 2016 stated that it shall be monitoring the use of ‘social media platforms’ as a way to make sure that these platforms are adhering to the values and ethics of the country, and not undermining the stability of the country. However, there is no actual confirmation of the technology that the government is using but it is assumed that a number of general digital surveillance techniques are being used which could be:

- Random search of key words that the government is looking for on social media platforms;
- Monitoring influencers’ post, followers and respondents online and
- General overview eye to monitor news trending on social media and/or any calls for anti-government protests.¹⁶⁷

Website throttling or website blocking

The blockages of websites and social media platforms in Sierra Leone has been noticed to be triggered only by events which are mainly during the general elections or national protests. The interviewed experts within the country also confirmed that the blocking of social media platforms is the most common especially during elections. In 2018 during the general election run-off, there were two network disruptions one just before and just after the country’s runoff elections. A detailed report was done by OONI in collaboration with Campaign for Human Rights and Development International (CHRDI).¹⁶⁸

3.4 Sierra Leone summary table

NO	YES	YES	NO
Hacking	Digital Surveillance	Website Throttling or Website Blocking	State sponsored attacks on CSOs and HRDs

¹⁶⁷ Digital security expert report on Sierra Leone.

¹⁶⁸ <https://ooni.org/post/sierra-leone-network-disruptions-2018-elections/> (accessed 15 October 2019).

3.5 An analysis of the country context in Sierra Leone

Most constitutions in African countries often reflect the international human rights standard on limitation of human rights, including that of Sierra Leone. However, when laws and policies are made with respect to the limitative aspect of these human rights, these two standards – the constitution and international human rights law are often side-stepped.¹⁶⁹ Taking the Constitution of Sierra Leone, for example, one recurring proviso in the rights affecting civil society and HRDs is that limitative laws must be such that they are justifiable in a democratic society.¹⁷⁰ Considering the limitation placed on the right to association and assembly, especially by the *Public Order Act of 1965*, not only are the vague use of words highlighted in the law above problematic, they are being used arbitrarily while encouraging state-sponsored violence and violation of human rights.¹⁷¹ Also, a 54-year old law is matured enough for a review given the several human rights developments that have occurred since its enactment. For example, provisions of the law on criminalisation of libel, false news and sedition are impediments to realising a free and democratic society; these have been decided against by courts and cannot be justified under any circumstances.¹⁷² The chilling effect this causes on the freedom of expression and the impacts they have on the enjoyment of rights are therefore far-reaching for democratic development in Sierra Leone.

Some provisions of the law seeks to insulate the government from criticisms. For instance, sections 32 and 33 of the law cannot be said to be justifiable in a free and democratic society thereby placing the Public Order Act not only in direct contravention of the Constitution but also in direct violation of international human rights law to which Sierra Leone is party.¹⁷³ This is so when comparing the Act with the three-part test of whether it pursues a legitimate government objective, is propositioned by law of general applicability and is proportional to the ends sought. Nothing in the Act strengthens the government of Sierra Leone's position that the Act pursues a legitimate government objective, nor does it show that the overboard provisions are proportional to ensuring public order.

169 *Constitutional Rights Project v Nigeria*, Communication 102/93, 57-58.

170 Constitution of Sierra Leone, Sections 15, 22, 25 and 26.

171 Interviewee from Sierra Leone: Edmond Abu, the Executive Director of Native Consortium was arrested for leading a peaceful protest for fuel increment. Also, some members of the Bar Association were also arrested for staging a peaceful protest on the sacking of the Vice President of Sierra Leone.

172 *Federation of African Journalists and Others v The Gambia* ECW/CCJ/APP/36/15 <https://www.mediadefence.org/sites/default/files/blog/files/FAJ%20and%20Others%20v%20The%20Gambia%20Judgment.pdf> (accessed 19 July 2019); *Gambia Press Union and Others v Attorney General* SC Civil Suit No. 1/2014; Interviewee from Sierra Leone: 'I was forcefully detained for a night with my passport seized for 45 days because I raised questions centered on endemic corruption and the lack of public accountability in the government in 2017.'

173 Sierra Leone ratified the ICCPR on 23 August 1996 https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=156&Lang=EN (accessed 5 September 2019).

Furthermore, with respect to the DCF, there is no justifiable argument why considering the provisions of the Framework, they are in compliance with the Constitution and international human rights law. The Framework singles out NGOs which also include civil society and HRDs for a special regime of policies and guidelines automatically violates the international law requirement that a law must be ‘necessary’ to restrict rights.¹⁷⁴ Also, in ensuring accountability, the restrictions on foreign funding does not only fail to use the least restrictive means in ensuring transparency, it is not proportional as other civil society actors will be left out in the enforcement of such requirement. The capping of foreign staff for civil society may also be injurious to the functionality of NGOs and HRDs as it may starve them of the effectiveness necessary to operate in the country. This does not in any way comply with the proportionality requirement under international human rights law.¹⁷⁵

The tethering of the civil society to state impulses especially as demonstrated under the DCF portends a great danger to what may be regarded as reasonably justified in an open and democratic society. An important source of this danger is requiring NGOs to register with the state rather than the international law requirement that the state is merely notified of their existence in order to reduce the possible grip on civil society by the state.¹⁷⁶ This helps the state with an overreaching and unjustifiable scrutiny in Sierra Leone which places the civil society at the cusp of the state and does not cater to the need for rational criticisms, limitation of state power, personal development, protection of freedoms, negative utilitarianism all of which are the pillars of an open and democratic society.¹⁷⁷

In assessing both the legal and digital threats against civil society and HRDs in Sierra Leone, the recurring factor is that the government is capable of justifying both offline and online attacks through the use of the laws and policies discussed above.¹⁷⁸ The only ray of hope for civil society and HRDs in Sierra Leone remains strict adherence to the Constitution, the Right to Access Information Act of 2013 and the passage of the Human Rights Defenders bill into law. The complementarity of both policies will help a great deal to enhance the prospects of good governance in Sierra Leone. Even though the bill is currently at its draft stage, it presents an opportunity to redraft it for the purpose of addressing emerging challenges like online rights in the civic space in the bill to have it cater for the problematic provisions of the Public Order Act and the DRF. The government cannot claim to commit to human rights and public interest on one hand and,

174 n 25 above.

175 as above, 17.

176 n 25 above, 14.

177 See, generally, K Popper *The Open Societies and its Enemies* (2002).

178 Interviewee from Sierra Leone: The arrest of journalist, Dr David Bayoh, Jonathan Leigh and others demonstrates how the government of Sierra Leone uses these laws to clampdown on the civil society in the country. So also, is the arrest, detention and prosecution of 19 Environmental and Land Rights Defenders of the Malen Affected Land Owners and Users Association (MALOA) by the state government.

use problematic laws to curtail freedoms in the other hand. Moreover, considering the laws and policies analysed above, the interest of protecting freedoms and ensuring socioeconomic justice obviously outweighs the unproven importance for censorship and indiscriminate surveillance through these laws and policies.

3.6 Recommendations for Sierra Leone

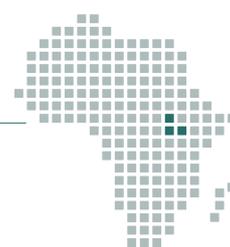
- The government of Sierra Leone must embark on a rights-respecting campaign on laws adversely affecting the civil society and HRDs;
- The legislative arm of the government must step up to amend the problematic laws that do not comply with both the Constitution and international human rights law;
- The government of Sierra Leone must ensure the passage of the *Human Rights Defenders bill* to fulfil its commitment to the promotion and protection of human rights under the Constitution;
- The civil society and HRDs in Sierra Leone should engage in digital security training in the sector; and
- The civil society and HRDs should make more prominent the online components of the rights protected under the *Human Rights Defenders bill*.



People along the Makeni highway
in Sierra Leone
© Roberto Nencini / Shutterstock



View over the central bus station in Kampala, Uganda
© MechmetO / Shutterstock



SECTION 4

Case Study: Uganda

4.1 Country background

Uganda is considered as not free under the 2019 Freedom of the World rankings.¹⁷⁹ It holds an aggregate score of 36 where zero is least free and 100 is most free.¹⁸⁰ This poor ranking stems from the continued assault on human rights under the current government. The incumbent president of Uganda, Yoweri Museveni, has been in power since 1986 and he intends to run for a 6th term in 2021 following a contentious constitutional amendment that removed the presidential age limit of 75 years.¹⁸¹ Uganda has a robust civil society movement championing for democratic consolidation and against human rights violations. However, CSOs have been victim of sustained harassment and intimidation from government which has employed both legislative and other means to reign in the activism of civil society.¹⁸² Specifically, CSOs that handle human rights issues such as governance, land, extractive industries and LGBTQI are most vulnerable to government harassment and intimidation.¹⁸³ With the introduction and expansion of new frontiers to exercise freedom of expression, association and peaceful assembly in the digital age, CSOs and HRDs in Uganda have embraced this platform for their activ-

179 Freedom House 'Freedom in the world 2019: Uganda' (2019) <https://freedomhouse.org/country/uganda/freedom-net/2019> (accessed 15 November 2019).

180 As above.

181 CIVICUS 'Museveni endorsed for 6th term, as opposition leaders continue to face harassment' *Daily Monitor* (30 April 2019) <https://monitor.civicus.org/newsfeed/2019/04/30/museveni-endorsed-6th-term-opposition-leaders-continue-face-harassment/> (accessed 15 November 2019).

182 Freedom House (n 179 above).

183 HRW Curtailling criticism intimidation and obstruction of civil society in Uganda (2012) 2.

ism. This has attracted the ire of the President who is increasingly intolerant of online criticism and has thus adopted digital means to curtail these freedoms with increased reports of surveillance, censorship, and online harassment of HRDs as well as the arrest and detention of critical voices.¹⁸⁴

4.2 National legislative framework

Uganda has a progressive constitution with guarantees for the promotion and protection of human rights and fundamental freedoms. These constitutional provisions are crucial to providing an enabling environment for CSOs and HRDs.¹⁸⁵ However, the enactment of certain laws call into question the commitment of the government towards the respect, protection and fulfilment of these rights. The analysis below examines the legislative framework that affects the work of CSOs and HRDs in Uganda with a particular focus on laws that centre on digital rights. It also evaluates the specific digital threats experienced by CSOs and other HRDs in Uganda.

Having ratified the ICCPR in 1995 and the African Charter in 1986, the government of Uganda has an international obligation to give effect to the rights contained in these treaties, including the right to freedom of peaceful assembly and association, freedom of expression, and right to privacy, among other rights.¹⁸⁶

The Constitution

Article 29 of the Constitution of the Republic of Uganda provides for freedom of conscience, expression, assembly and association. The article provides that:

Every person shall have the right to: (a) freedom of speech and expression which shall include freedom of the press and other media; (b) freedom of thought, conscience and belief which shall include academic freedom in institutions of learning... (d) freedom to assemble and to demonstrate together with others peacefully and unarmed and to petition; and (e) freedom of association which shall include the freedom to form and join associations or unions, including trade unions and political and other civic organisations.

These rights, crucial to the operation of CSOs in Uganda, are further boosted by other interdependent and intersecting rights including: equality and freedom from discrim-

184 Freedom House 'Freedom of the Net 2018: The rise of digital authoritarianism' (2018) 22.

185 HRW 'Curtailed criticism. Intimidation and obstruction of civil society in Uganda' <https://www.hrw.org/report/2012/08/21/curtailing-criticism/intimidation-and-obstruction-civil-society-uganda> 21 August 2012 (accessed 15 November 2019).

186 UN 'Treaty collection' https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en (accessed 15 November 2019); AU 'African Charter on Human and Peoples' Rights' <https://au.int/en/treaties/african-charter-human-and-peoples-rights> (accessed 15 November 2019).

ination, right to life, protection of personal liberty, respect for human dignity and protection from inhuman treatment, right to privacy, right to a fair hearing, civic rights, economic rights, right of access to information, and right to just and fair treatment in administrative decisions.¹⁸⁷ Further, for the purposes of this report, emphasis is made on article 38(2) which provides that, 'Every Ugandan has a right to participate in peaceful activities to influence the policies of government through civic organisations.

Regulation of Interception of Communications Act

The Regulation of Interception of Communications Act (RICA) came into force on 3 September 2010. The Act has come under criticism for some of its provisions that have been seen as a threat to the exercise of the constitutionally guaranteed right to freedom of speech and expression as well as the right to privacy.¹⁸⁸ The objective of the Act as provided in its preamble is:

...to provide for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Uganda; to provide for the establishment of a monitoring centre; and to provide for any other related matters.

The Act sets three conditions for the interception of communication sent via telecommunication or radio systems. For an interception to be considered lawful, the interceptor must be party to the communication, have the consent of the sender or recipient of the communication, or act under an authorised warrant. For the interception of communication sent by post, the interceptor must meet the last two conditions.¹⁸⁹

Emphasis is made on the third condition for a legal interception on the basis of an authorised warrant. Section 5(1) of RICA sets out the grounds that will guide a designated judge in issuing a warrant for the interception of communication to an authorised person. A designated judge in this case is one appointed by the Chief Justice to perform specific functions under RICA.¹⁹⁰ The grounds include:

- an offence which may result to loss of life or threat to life has been or is being or will probably be committed;
- an offence of drug trafficking or human trafficking has been or is being or will probably be committed;

187 Constitution of Uganda, Arts 21, 22, 23, 24, 27, 28, 38, 40, 41, 42.

188 Amnesty International 'Uganda Amnesty International memorandum on the Regulation of Interception of Communications Act' <https://www.amnesty.org/en/documents/AFR59/016/2010/en/> 14 December 2010 (accessed 15 November 2019).

189 Section 2 RICA. However, these provisions are subject to Part VII of the Anti-Terrorism Act 2002 on interception of communications and surveillance in relation to terrorist investigations.

190 RICA, Section 1.

- the gathering of information concerning an actual threat to national security or to any national economic interest is necessary;
- the gathering of information concerning a potential threat to public safety, national security or any national economic interest is necessary; or
- there is a threat to the national interest involving the State's international relations or obligations.

This section has been criticised for its broad terminologies that may give room for misuse of power by authorities.¹⁹¹ This goes against international standards that disapprove unchecked discretion given to authorities charged with implementing a law.¹⁹² While national security is considered a legitimate aim for the restriction of a right, the Act's definition of national security as 'including matters relating to the existence, independence or safety of the State', has been criticised for being overly broad and giving authorities too wide a discretion to limit a human right based on this ground.¹⁹³

Further, under section 5(1) (c) & (d), 'national economic interest' is listed as one of the grounds for the issue of a warrant for the interception of communication. Two challenges arise from these provisions. Firstly, RICA does not provide a definition for what constitutes a national economic interest.¹⁹⁴ Secondly, 'national economic interest' is not an internationally recognised legitimate aim for the limitation of a human right.¹⁹⁵ Additionally, the section fails to instruct the judge on the procedures as well as the considerations he or she should have before granting the warrant, particularly whether the issue of such a warrant will adversely impact the exercise of human rights as set by international standards.¹⁹⁶

RICA also establishes a Monitoring Centre tasked with the interception of communications, and to be administered by the Minister of Security or any other minister appointed by the President for such purpose.¹⁹⁷ Section 3(1)(c) requires that the Minister in consultation with other relevant ministers shall 'acquire, install and maintain connections between telecommunication systems and the Monitoring Centre.' While these powers are given to the executive arm, the Act does not provide for an independent and impartial oversight mechanism over the Minister in case of abuse of his or her powers.¹⁹⁸

191 Unwanted Witness 'Repressive: Uganda's worst cyber laws threatening free expression and privacy' 12-13. See also Unwanted Witness <https://www.unwantedwitness.org/ugs-most-threatening-cyber-laws-to-freedom-of-expression-privacy-online-named/18-January/2017> (accessed 15 November 2019).

192 General comment 34 'Art 19: Freedoms of opinion and expression' para 25.

193 Unwanted Witness (n 191 above).

194 As above, 15.

195 General comment 34 'Art 19: Freedoms of opinion and expression' para 21.

196 Amnesty International 'Uganda Amnesty International memorandum on the Regulation of Interception of Communications Act, 2010' (2010) 6.

197 RICA, Section 3 (1) & (2).

198 Amnesty International (n 196 above) 7.

Section 9 of the Act tasks telecommunications companies to register the SIM cards of existing as well as new subscribers and keep proper records of the personal details of their subscribers. Required details for this registration include names, business, postal and residential address, and ID number for individuals, and in the case of a business, the business name, address and incorporation or registration details. It is unclear what data protection measures are in place to protect the information of the subscribers from the undue infringement of their right to privacy. Further, in the event that the relevant Minister requests telecommunications services for particular information, expecting that it serves a legitimate aim, the Act does not provide measures to ensure transparency and accountability in the process.

Another critique of RICA is its failure to unequivocally state that all interceptions must be made pursuant to a judicial warrant to prevent the abuse of this power by rogue public officials of the executive arm.¹⁹⁹ For example, sections 8 and 11 of the Act tasks postal and telecommunications service providers to ensure their systems can support lawful interceptions.²⁰⁰ Further, the service providers are required to ensure that the 'intercepted communications are transmitted to the monitoring centre via fixed or switched connection' as well as provide 'access to all the interception subjects.'²⁰¹ Additionally, the section requires that the service provider ensures the interception can be done in such a way that is unidentifiable to the subject or any other unauthorised person.²⁰² This section provides the leeway of interception of communications without judicial approval. Further, the wide discretion given to authorities under this section fails to meet the standards set out under section 2 of the Act that controls interception of communications. There is need for stronger monitoring and evaluation measures for the officials exercising these powers to prevent the abuse, threat or infringement of human rights.²⁰³ The section also appears to weaken the safety systems of these service providers that leave them vulnerable to interception by other malicious external agents.

Another section that fails to clearly indicate the requirement for judicial authorisation before interception of communications is section 10 of the Act that empowers an authorised person, by notice, to have access to protected information. In this context, protected information pertains to 'information that is encrypted by means of a key.'²⁰⁴ The Act does not clarify whether the authorised person is acting through judicial authorisation or otherwise. The section also includes national economic interest as a ground for requiring the disclosure of protected information, which is not a legitimate aim for the limitation of a right.²⁰⁵

199 Unwanted Witness (n 191 above) 14.

200 RICA, Art 8 (1) (a).

201 RICA, Art 8 (1) (f) & (g).

202 RICA Section 8(i).

203 Amnesty International (n 196 above) 8.

204 RICA, Section 1.

205 RICA, Section 10(b)(iv).

Section 16 of the Act empowers the Minister to make regulations to give effect to the provisions of the legislation. Such regulations can help clarify some of the gaps, challenges, and ambiguities revealed in the Act to ensure that the implementation of the law does not lead to a threat or infringement of human rights.²⁰⁶

The Anti-Terrorism Act

As of 2019, the Anti-Terrorism Act which came into force on 7 June 2002 has been the basis of at least 417 charges.²⁰⁷ Some provisions of the Act have raised concern on the broadness of application and their impact on exercise of certain human rights and fundamental freedoms. Under section 7(2) (g) of the Act, ‘serious interference with or disruption of an electronic system’ is included as an act of terrorism if it is done with the intention of ‘influencing the Government or intimidating the public or a section of the public and for a political, religious, social or economic aim, indiscriminately without due regard to the safety of others or property.’ This section has been criticised as too broad a definition for an act of terrorism.²⁰⁸ Worse still, any conviction for an act of terrorism under section 7 of the Act carries a harsh penalty of death. Additionally, section 8 criminalises aiding or abetting or financing, harbouring or rendering support to any stage leading to what constitutes a terrorist activity and equally carries a capital punishment.²⁰⁹

Section 9 of the Act also criminalises the establishment or support for an institution that promotes terrorism, publishes and disseminates news or materials that promote terrorism, or trains or mobilises any group of persons or recruits persons for carrying out terrorism or mobilising funds for the purpose of terrorism. The vagueness of this provision is concerning given how it can be twisted to criminalise legitimate media reporting of terrorist activities.²¹⁰ This offence similarly carries a harsh death penalty upon conviction. Upon amendment of the Act in 2017, section 9A of the Act introduced the offence of indirect involvement in terrorist activities also punishable by death. It can reasonably be argued that the harsh penalty of death attached to these offences does not match the seriousness of the offence, made worse by the lack of concise description of offences under the Act leaving provisions open to wide interpretations, and unduly interfere with the freedom of expression.²¹¹

The Act further empowers the Minister for Internal Affairs to appoint officers in charge of intercepting communications and conducting surveillance for ‘any’ suspected acts of

206 Amnesty International (n 196 above) 6.

207 Unwanted Witness ‘Cyber policy’ <https://www.unwantedwitness.org/cyberpolicy/> (accesses 14 November 2019).

208 Unwanted Witness (n 191 above) 17.

209 Section 8 The Anti-Terrorism Act 2002.

210 Unwanted Witness (n 191 above) 17.

211 Unwanted Witness (n 191 above) 18.

terrorism under the Act.²¹² The scope of power given to the officers is wide, extending to the:²¹³

- a) interception of letters and postal packages of any person;
- b) interception of the telephone calls, faxes, emails and other communications made or issued by or received by or addressed to a person;
- c) monitoring meetings of any group of persons;
- d) surveillance of the movements and activities of any person;
- e) electronic surveillance of any person;
- f) access to bank accounts of any person; and
- g) searching of the premises of any person.

The powers of the Minister as well as the authorised officers under these sections are not subject to judicial or other administrative oversight to prevent abuse. Section 19 (6) further empowers the authorised officers to not only detain and make copies of intercepted material and photographs of the subject, but also gives them broad and undefined powers to ‘do any other thing reasonably necessary for the purposes of this subsection.’ Such unchecked powers give leeway for unscrupulous officers to misuse the power and disrupt legitimate activities such as that of HRDs and CSOs in the name of preventing a potential act of terrorism.

The concerns on the provisions of the Anti-Terrorism Act and its impact on freedom of expression as well as press freedom are exemplified in the case of the arrest of journalist Joy Doreen Biira on November 2016. She was charged with ‘illegal filming of military raid’ that occurred at the Rwenzururu palace in Kasese town and resulted in death of over 50 civilians. She circulated the video online and commented on it. She was ultimately charged with the offense of abetting terrorism which carries the death penalty upon conviction.²¹⁴

Computer Misuse Act

The Computer Misuse Act has received varied support on its effectiveness towards addressing cyber security and cybercrimes without unduly interfering with the exercise of human rights and fundamental freedoms. As of 2019, 379 charges have been brought under this Act.²¹⁵ While the provisions of the Act can go a long way in preventing cybercrime, section 25 of the Act in particular has been criticised for its broadness and

212 The 2000 Anti-Terrorism Act, Section 19 (1) - (4).

213 As above, Section 19(5).

214 Moris Mumbere ‘Kasese clashes: KTN journalist charged with abetting terrorism’ *Daily Monitor* (28 November 2016) <https://www.monitor.co.ug/News/National/Kasese-clashes-KTN-journalist-terrorism/688334-3468084-5xnl8u/index.html> (accessed 15 November 2019).

215 Unwanted Witness ‘Cyber policy’ <https://www.unwantedwitness.org/cyberpolicy/> (accesses 14 November 2019).

potential for misuse and misapplication that might jeopardise the exercise of human rights, particularly the freedom of speech and expression.²¹⁶ The section in its harsh interpretation can lead to undue self-censorship that inhibits meaningful debate on matters of public interest. Section 25 introduced the offence of ‘offensive communication’ and provides that:

Any person who wilfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanour and is liable on conviction to a fine not exceeding twenty-four currency points or imprisonment not exceeding one year or both.

This section goes to great lengths to prevent persons from being offended by what can arguably be termed a ‘fair comment’ in matters of public interest.²¹⁷ It was under this section that Joseph Kabuleta, a former sports journalist, was charged for a Facebook post that criticised the presidency for his attempts at subverting democracy.²¹⁸ As Anne Tendo, a legal consultant at Cromwel Company Ltd, further pointed out, other people who share the post are also liable for prosecution under this section.²¹⁹

The vagueness of terms such as ‘disturb the peace, quiet and privacy’ of another person have been critiqued as problematic for the interpretation of this section. Offending a person is a subjective issue, yet the section does not offer much direction on what can constitute such an offence.²²⁰ This threatens the right to fair trial of a person charged under this provision.²²¹ There is a need for further guidelines on what constitutes ‘offensive communication.’²²²

Further, section 25 highly threatens the freedom of speech and expression given that the limitation it introduces does not serve a legitimate aim that is necessary and proportionate in a democratic society. As was decided in the case of *Onyango Obbo & Andrew Mujuni Mwenda v Attorney General*,²²³ information that offends, shocks or disturbs is protected under the Constitution of Uganda.

216 HRAPF ‘The Computer Misuse Act 2011: Yet another legal fetter to the basic rights and freedoms of marginalised persons’ (2011) 4 *The Human Rights Advocate* at 8.

217 R Musoke ‘Misusing computer misuse law’ *The Independent* (5 August 2019) <https://www.independent.co.ug/misusing-computer-misuse-law/> (accessed 15 November 2019).

218 As above.

219 As above.

220 HRAPF (n 216 above).

221 HRAPF (n 216 above) 8-9.

222 HRAPF (n 216 above) 9.

223 Constitutional Appeal 2 of 2002.

In 2017, Dr Stella Nyanzi, a former research fellow at Makerere University, was charged and later convicted under section 25 of the Act for referring to President Museveni as 'a pair of buttocks' on a Facebook post.²²⁴ A similar fate met Swaibu Nsamba, a political activist, for his social media posts that criticised the government.²²⁵

The constitutionality of section 25 is currently under determination in *Andrew Karamagi & Robert Shaka v Attorney General*,²²⁶ under which the petitioner Mr Shaka had been charged. As has been a common denominator in these kinds of cases, he was arrested for his social media posts criticising President Museveni. The petitioners are seeking orders for the invalidation of the section (as it threatens the freedom of speech and expression), the stay of prosecution of persons charged under the section, as well as the stay on enforcement of the section. Similar concerns over section 25 of the Computer Misuse Act were raised in *Gwogyolonga Swaibu Nsamba & 2 others v Attorney General*.²²⁷

The Anti-Pornography Act

Since its entry into force in 2014, at least 17 charges have been brought under the Anti-Pornography Act.²²⁸ While the object of the Act is to regulate pornography, it has been disproportionately used to target members of the LGBTI community whose advocacy can be misinterpreted under the Act as pornography.²²⁹ This is because of the vague provisions of the Act, as well as sweeping powers given to authorities such as the Pornography Control Committee with little oversight.²³⁰ For example, section 2 of the Act broadly defines pornography as:

any representation through publication, exhibition, cinematography, indecent show, information technology or by whatever means, of a person engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a person for primarily sexual excitement.

Section 13, on the other hand, criminalises the production, trafficking, broadcasting, procurement, importation, sale or abetting of pornography and imposes a fine of not more than five hundred currency points or imprisonment of not more than ten years or both.

224 *Uganda v. Stella Nyanzi Criminal Case 319 of 2017*.

225 Freedom House 'Freedom on the Net 2017: Uganda' (2017) <https://www.refworld.org/docid/5a547cfba.html> (accessed 16 November 2019).

226 *Andrew Karamagi & Robert Shaka v Attorney General Constitutional Petition 5 of 2016*.

227 *Gwogyolonga Swaibu Nsamba, Unwanted Witness-Uganda and Human Rights Enforcement Foundation v Attorney General Constitutional Petition 15 of 2017*.

228 Unwanted Witness (207 above).

229 Freedom House 'Freedom on the Net 2017: Uganda' https://freedomhouse.org/sites/default/files/FOTN%202017_Uganda.pdf (accessed 15 November 2019).

230 Anti-Pornography Act, Section 11.

The Non-Governmental Organisations Act

The Non-Governmental Organisations Act (NGO Act) is meant to create an enabling environment for the operations of civil society in Uganda. However, the NGO Act is seen to serve another purpose in increasing the power of the government to interfere with the constitutionally guaranteed rights of association and peaceful assembly.²³¹ Section 7 of the Act provides broad powers to the NGO Bureau to summon and discipline organisations through warnings, suspension, blacklisting, revocation of license, or public exposure.

The fact that the NGO Bureau is under the auspices of the Ministry of Internal Affairs that is responsible for monitoring issues that pose a threat to national security reveals the attitude that the government has towards the NGO sector.²³² Further, intelligence personnel are members of the NGO Bureau and given the prominent roles of intelligence agents in interception of communications and surveillance operations as seen in RICA, Computer Misuse Act, and the Anti-Terrorism Act, it calls into question the loyalties of these personnel whether towards promoting the legitimate interests of civil society or protecting the interests of government. This prevents the Bureau from legitimately addressing the issues of concern brought by legislation affecting digital rights and the work of civil society.

4.3 Digital threats to civil society in Uganda

The internet penetration in Uganda is approximately 35% representing approximately 13.5 million internet users.²³³ This is a sizeable section of the population in which civil society can engage with to promote human rights issues with the intention of leading to both online and offline action. This fact has not escaped the Ugandan government given the measures that have been put in place to obstruct online activism. Outside laws that seek to curtail the operation of civil society in the digital era, NGOs and other HRDs have also been subject to digital threats in their operations.

Hacking

The Ugandan government has been communicating with The Hacking Team and have allegedly done business with the organisation as far back as 2010. The government of Uganda is said to have purchased surveillance software that was used to target some LGBTI community members and activists. In 2014, some of the LGBTI members noticed

231 Freedom House (n 231 above).

232 HRW 'Curtailling criticism. Intimidation and obstruction of civil society in Uganda' (2012) 3.

233 CIPESA 'Social media tax cuts Ugandan internet users by five million, penetration down from 47% to 35%' <https://cipesa.org/2019/01/%EF%BB%BFsocial-media-tax-cuts-ugandan-internet-users-by-five-million-penetration-down-from-47-to-35/> (accessed 15 November 2019).

that their computers were responding slower than usual and that their mobile communications were sounding like they were being tapped.²³⁴ Besides the above mentioned there has not been any other verified and documented incident of hacking within Uganda.

Digital surveillance

Digital surveillance is currently active in Uganda and laws are in place to support the full implementation of internet surveillance. For example, the Ugandan government ordered the mobile telecommunications companies to have equipment that will allow them to monitor and record calls and messages. This form of surveillance is the most commonly used and is backed up by laws and regulations. Recently, Uganda has introduced an Over-The-Top tax of \$0.05 daily. The government justified the introduction of the controversial social media tax as a revenue collection measure, but critics have condemned it as a means of reducing the use of online platforms for free speech and expression against the establishment. As argued by critics, since the introduction of the tax in July 2018, there has been a reduction in the number of social media users by at least 5 million as at the beginning of 2019.²³⁵

On another note, there were serious suggestions that the Ugandan government used advanced 'spyware' in the 2016 elections to crush its opposition party. In an investigation report done by Privacy International, it states that '[t]he government's weapon of choice was a highly invasive form of spyware called FinFisher, produced by Gamma Group International, a UK-based company with affiliates in other countries.'²³⁶ Similar to Sierra Leone, Uganda is also found to be using basic means of digital surveillance that might include:

- Random search of key words that the government is looking for;
- Monitoring influencers' post, followers and respondents online; and
- General overview eye to monitor news trending on social media and/or any calls for anti-government protests.

The government has increasingly interacted with the Chinese government and officials to purchase the necessary surveillance and other technologies to implement the provisions of the restrictive cyber laws discussed above. This is of concern due to China's reputation in controlling information in violation of international human rights standards.²³⁷

234 S Frenkel 'These two companies are helping governments spy on their citizens' <https://www.buzzfeednews.com/article/sheerafrenkel/meet-the-companies-whose-business-is-letting-governments-spy> (accessed 15 November 2019).

235 CIPESA 'Social media tax cuts Ugandan internet users by five million, penetration down from 47% to 35%' <https://cipesa.org/2019/01/%EF%BB%BFsocial-media-tax-cuts-ugandan-internet-users-by-five-million-penetration-down-from-47-to-35/> (accessed 15 November 2019).

236 <https://www.theverge.com/2015/10/16/9549151/uganda-finfisher-surveillance-spyware-privacy-international>

237 Freedom House 'Freedom of the net: The rise of digital authoritarianism' (2018) 9.

Website throttling or website blocking

Uganda, just like the other countries under review, has proved to have blocked websites and social media platforms during an election or anti-government protest in the country. Internet Protocol (IP) blocking measurements done by OONI suggest that each time there was a blockage of a social media platform it was through IP blocking. IP blocking is simply a configuration that is done by the ISP to block a specific website/connection. In Uganda's case, they blocked the IP address of mainly WhatsApp and Twitter.

State sponsored attacks on CSOs and HRDs

In April 2018, the Ugandan government attempted and lost an appeal case against a ruling by the High Court of Ireland to block and reveal the true identity of Tom Voltaire Okwalinga (TVO), a critic of the government who publishes on Facebook using a pseudo name²³⁸.

Besides the above, there has been no other actual verified and documented incidents of any state sponsored attacks taking place within the country towards any CSO or HRD.

4.4 Uganda summary table

NO Hacking	YES Digital Surveillance	YES Website Throttling or Website Blocking	NO State sponsored attacks on CSOs and HRDs
----------------------	------------------------------------	--	---

4.5 Recommendations for Uganda

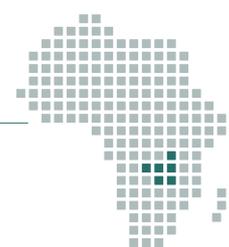
- Parliament should amend the vague and broad provisions in RICA, Anti-Terrorism Act and Anti-Pornography Act, and narrowly define the terms to ensure that offences are precisely defined and unequivocal as well as limit the unfettered power of authorities who implement the laws;
- Parliament should repeal section 25 of the Computer Misuse Act given its negative impact on free speech and expression;

238 Mary Carolan, 'Court refuses to compel Facebook to disclose blogger's identity and location,' April 19, 2018, <https://www.irishtimes.com/news/crime-and-law/courts/court-refuses-to-compel-facebook-to-disclose-blogger-s-identity-and-location-1.3467309> (accessed 15 November 2019).

- Parliament should amend the NGO Act to create an enabling environment for the operation of CSOs in Uganda with particular focus on transferring the NGO Board from the Ministry of Internal Affairs and the removal of intelligence agencies from the Board;
- Government should ensure that any actions taken to address genuine digital threats are done in alignment with international human rights standards and should not disproportionately discriminate against a group of persons with emphasis on the LGBTIQ community in Uganda;
- Government should appreciate the work of CSOs and HRDs in democratic development and develop channels for meaningful engagement such that human rights activism is not wrongly perceived as a threat to the continued existence of the establishment but important to democratic consolidation;
- Service providers should provide periodic reports detailing the number and nature of requests of information received and given to the government to promote transparency and accountability in their actions; and
- Civil society should boost their technical knowledge and skills to pushback against the threats to the right to freedom of association and peaceful assembly as well as freedom of speech and expression, and right to privacy through trainings on digital security and safety.



Aerial view of Lusaka, the capital and largest city in Zambia
© The Morning Glory / Adobe Stock



SECTION 5

CASE STUDY: ZAMBIA

5.1 Country background

Zambia gained its independence in 1964. The country was led by a single party for more than twenty years after gaining independence. It was until 1991 that a multi-party election was allowed but has since then oscillated between three-party and two-party systems. Zambia has had at least six general elections and eight presidential elections. There are currently eleven political parties in the country. The Constitution of Zambia was enacted in 1996 and there have been ongoing consultations for its amendment. This Constitution provides for fundamental human rights and freedoms including those of civil and political rights.²³⁹ As at November 2019, there were reports, partly corroborated by the President of Zambia, Edgar Lungu, that he may run for a third term in office as President.²⁴⁰ With regards to the economy, Zambia is 139 out of

239 See, generally, C Beyani and M Ndulo 'As tedious as a twice-told tale: The struggle for a legitimate and democratic constitution in Zambia' (2012); M Ndulo and R Kent 'Constitutionalism in Zambia: Past, present and future' (1996) 40 *Journal of African Law* 260.

240 M Chawe 'Zambian President's birthday wish: a third term' 11 November 2019 *The East African* <https://www.theeastafrican.co.ke/news/africa/Zambian-President-Lungu-s-birthday-wish--a-third-term/4552902-5345368-qtssfcz/index.html> (accessed 11 November 2019); Section 35 (2) of the *Zambian Constitution of 1996* (as amended) provides that a person shall not be eligible for the Office of the President of Zambia if they have already been elected twice. However, the Constitutional Court of Zambia has ruled that the President can stand for the upcoming elections in 2021 despite the constitutional term limit. See, generally, C Mfula 'Zambian court says Lungu can run for president in 2021, opposition cries foul' 7 December 2019 Reuters <https://www.reuters.com/article/uk-zambia-politics/zambian-court-says-lungu-can-run-for-president-in-2021-opposition-cries-foul-idUKKBN106118> (accessed 11 November 2019).

189 countries ranked under the Human Development Index as 63% of Zambians live below the poverty line.²⁴¹

5.2 National legislative framework

The Constitution of Zambia of 1996 as amended provides for a Bill of Rights in its Part III. Article 11 of the Constitution provides for civil and political rights including the rights to freedom of conscience, expression, assembly, association and privacy. These rights are qualified by the need to protect the rights of others and public interest. Articles 17, 20 and 21 provides for the rights to privacy, freedom of expression and association and assembly. These rights are also qualified by public interest and the right of others but none of these restrictions will be regarded as lawful except they are reasonably justifiable in a democratic society. It follows that any government policy or law that restrict the rights of Zambians must be reasonably justified in a democratic setting. There are currently several laws in Zambia that impact on the enjoyment of human rights especially those of civil society and HRDs.

Section 5(1) of the NGO Act of 2009 establishes the Non-Governmental Organisations' Registration Board (the Board). The powers of the Board in section 7 of the Act include the registration of NGOs, approval of scope, recommendation of audit process, receiving and discussing annual reports, and alignment of NGOs with Zambia's national policy and approval of a Code of Conduct for all NGOs. Section 10(1) makes registration a condition for establishing an NGO in Zambia and INGOs are not allowed to operate in Zambia without being registered. An NGO's certificate may be suspended or cancelled where it does not comply with the provisions of section 26 under section 17(b).

Section 29 of the Act establishes the Zambia Congress of Non-Governmental Organisation (the Congress). Section 30 further establishes a Council of Non-Governmental Organisations to be composed by the Congress. The members of the Council shall be twelve and they will be elected from the Congress. It is this Congress that will be part of the Board. For the Board, as provided for under section 6, the Minister appoints fifteen members, eight of which are government officials, while seven are to be elected by the Congress.

The Penal Code of Zambia of 1994 provides for various offences that may impact on the rights of NGOs and HRDs. Section 53 of the Act vests the power to prohibit any publication that is contrary to public interest in the President and leaves such powers to his absolute discretion. Anyone who publishes a prohibited publication is liable to two years of imprisonment or a fine of five hundred penalty units (four months that may be reduced by a fine prescribed by the Court) or both. Section 57 provides for the offence

241 World Food Programme Report: Zambia (2019) <https://www.wfp.org/countries/zambia> (accessed 12 October 2019).

of seditious practices with a jail term of seven years or six thousand penalty units (nine months or more that may be reduced by fine prescribed by the Court) or both. Sections 60(b), (e) and (j) defines seditious intention to include bringing contempt or exciting disaffection against the government of Zambia, raising discontent among the people of Zambia and inciting resistance, whether passive or active against any law in Zambia. Section 69 of the Act provides that insults or defamatory words, through any medium against the President are punishable by an imprisonment term of not less than three years with no option of fine. Section 71 also criminalises defamation of a private person or a foreign prince.

Article 42 of the Electronic and Communications Act of 2009 establishes principles for electronic collection of personal information. Principle 9 particularly vests data controllers with powers to compile profiles for statistical purposes in so far as they do not link back to the data subject. Article 64 provides for lawful interception of information which must be supported by a court order. Article 65 of the Act also creates a Central Monitoring and Coordination Centre (CMCC) vested with powers to aggregate interception of communications. Article 77 of the Act mandates service providers to actively monitor communications in Zambia while transmitting such communication to the CMCC.

Section 88 of the Cybersecurity and Cybercrimes draft bill of 2017 provides for the offence of 'harassment utilising through the means electronic communications', which includes the intent to 'harass' or 'cause substantial emotional distress to a person.' The offence is punishable by five hundred thousand penalty units or one year in jail or both.²⁴²

On 13 August 2018, the Zambian government introduced a tax of US\$0.03 on internet phone calls.²⁴³ The government claimed that the move is motivated to increase state revenue but civil society organisations in Zambia believe it is a way of clamping down on the freedom of expression and privacy of Zambians online.²⁴⁴ Perhaps a promising development, the Access to Information bill in Zambia was approved by the Zambian cabinet but is yet to be tabled before the Zambian parliament to commence the legislative process required for the bill to become law.²⁴⁵

242 The bill does not provide for the definition of penalty units. <https://www.lusakatimes.com/wp-content/uploads/2018/06/The-Cyber-Security-and-the-Cyber-Crimes-DRAFT-Bill-2017.pdf> (accessed 15 October 2019).

243 <https://www.lusakatimes.com/2018/08/13/zambia-slaps-a-30-ngwee-a-day-tariff-on-internet-phone-calls/> (accessed 17 July 2019).

244 CIPESA 'Zambia introduces daily tax on internet voice calls' (2018) <https://cipesa.org/2018/08/zambia-introduces-daily-tax-on-internet-voice-calls/> (accessed 12 August 2019); <https://www.news24.com/Africa/News/anger-as-zambia-announces-tax-on-internet-calls-20180820> (accessed 12 August 2019).

245 http://www.xinhuanet.com/english/2019-03/19/c_137907853.htm (accessed 12 August 2019).

5.3 Human rights and the civic space online in Zambia

There are more than 7.2 million internet users in Zambia making up 41% of the population according to the Zambia Information and Communications Authority (ZICTA).²⁴⁶ A total of 2.2 million users of this number are active on social media.²⁴⁷ The popular social media platforms in Zambia are Facebook, Instagram and Twitter.²⁴⁸ The growing number of internet users in Zambia shows a great potential in online participation in social, economic and political debates.²⁴⁹ This may be some of the motivation of the government of Zambia to threaten the online civic space in the country as Zambia was the first country in sub-Saharan Africa to carry out website blockage in 1996.²⁵⁰ While not all the four categories of state-sponsored threats are documented in Zambia, some are, which further raises challenges on how the government of Zambia complements offline legal and physical threats with online attacks of civil society and HRDs.

Hacking

There has been no actual verified and documented incidents of any hacking taking place within the country towards any CSO or HRD. The only noted pattern is the loss or theft of devices (computers or mobile phones) belonging to CSOs or HRDs just after particular events such as meetings where HRDs were involved.²⁵¹

Digital surveillance

It is possible that while the Zambian government may be able to surveil the citizens, the government is not yet advanced enough to collect information from CSOs without physical access to the devices. Zambian government has also over the years signed several deals with the Chinese government which also suggests that there can be other projects lined up where the Zambian government can be helped to upgrade their surveillance techniques and systems.²⁵² In 2016, it is reported that the Zambian government 'spent about USD 1.8 million on its partnership with Chinese companies, involving the installation of an internet monitoring facility and possibly the development of backdoors within networks.'²⁵³ In as much as there have been these suggestions of

246 <https://www.slideshare.net/DataReportal/digital-2019-zambia-january-2019-v01> 15 (accessed 15 August 2019).

247 as above.

248 n 246 above, 25.

249 In 2016, during the elections, civil society actors used social media platforms like Facebook to sensitize the prospective electorates on the political landscape in Zambia.

250 Freedom House 'Freedom on the net - Zambia' <https://freedomhouse.org/country/zambia/freedom-net/2018> (accessed 12 August 2019).

251 Digital security expert report for Zambia.

252 A Dahir 'Chinese firms are driving the rise of AI surveillance across Africa' QZ 18 September 2019 <https://qz.com/africa/1711109/chinas-huawei-is-driving-ai-surveillance-tools-in-africa/> (accessed 15 October 2019).

253 CIPESA 'State of internet freedom in Zambia 2016: Charting patterns in the strategies African governments use to stifle citizens' digital rights' (2016) https://cipesa.org/?wpfb_dl=244 (accessed 27 October 2019).

equipment being bought, there has not been actual incidents recorded and verified when these technologies are used.

Website throttling or website blocking

Very few cases of website and social media platform blocking have been recorded and documented in Zambia. In July 2015, a local Zambian grass roots online newspaper by the name *Zambianwatchdog.com* was being blocked only within Zambia using deep packet inspection.²⁵⁴ Similar to the other countries under review, Zambia faces some website blockages during election periods evident in the 2016 general elections when the government ordered the blocking of 10 websites as analysed in the OONI report.²⁵⁵

State Sponsored Attacks on CSOs and HRDs

A research by the Citizen Lab at the University of Toronto detailed the use of spyware by 45 governments across the globe to target civil society and HRDs. According to the report, the spyware called *Pegasus* is produced by an Israeli-based company called the NSO. *Pegasus* tricks a target into clicking a link through which it downloads itself on the device and begin to send all information on such device back to those who deployed it. An Operator *Mulungushi* is currently being deployed on MTN-Zambia, a major telecoms operator in Zambia. The report states that the attacks are often politically motivated especially considering the political context and theme in the affected country.²⁵⁶

5.4 Zambia Summary Table

NO Hacking	YES Digital Surveillance	YES Website Throttling or Website Blocking	YES State sponsored attacks on CSOs and HRDs
----------------------	------------------------------------	--	--

5.5 An analysis of the country context in Zambia

Despite the constitutional protection for civil and political rights in Zambia, there has been a challenge by the government to protect these freedoms both offline and online through the use of laws and policies. Considering the provisions of the NGO Act of

254 Digital security expert report for Zambia.

255 <https://ooni.io/post/zambia-election-monitoring/> (accessed 27 October 2019).

256 <https://citizenlab.ca/2018/09/hidden-and-see-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> (accessed 15 October 2019).

2009, the government has reduced civil society and NGOs to an appendage of the state. With the constitutional proviso that a limitation of any of the rights contained under the Constitution must be reasonably justifiable in an open and democratic society, the Act does not seem to have satisfied that requirement under the law; thereby, raising questions about its constitutional validity.²⁵⁷

As explained above, under the restrictive tests under international human rights law and in most countries' constitutions including that of Zambia, section 5 of the Act does not show for example that the government of Zambia took the least restrictive option of having NGOs merely notify the government in order to pass the test of necessity.²⁵⁸ Also, the requirement under international law that a law restricting rights must be necessary is not passed by the NGO Act.²⁵⁹ The law seeks to administer special rules with respect to regulating the freedom of association, which in effect adversely impacts the functionality of the civic space in Zambia.

Also, considering the functions of the Board and the self-regulatory mechanism of the Congress, the powers given to the Board by the Act are more and substantial compared to those granted the Congress. For example, the activities of both the Council and Congress which are composed mainly of NGOs still require the approval of the government of Zambia to be valid under the Act. This puts to doubt the efficacy and independence of the self-regulatory features of the Council and Congress under sections 31 and 32(4) of the Act. The Act strategically places the power of the Board over that of the Congress due to the majority composition of the government on the Board. This places the NGOs and HRDs in Zambia under the unfettered control of the government of Zambia.²⁶⁰

Under the Penal Code of Zambia, the powers of the President to ban any publication he may deem offensive does not satisfy the requirement of whether such provision is necessary. Also, the concentration of power in the President in such a circumstance gives a wide berth for arbitrariness and misuse. In essence, such arrogation of power is not reasonably justifiable in an open and democratic society as it is a legally conferred weapon of censorship and clamping down on dissent thereby impacting on the right to freedom of expression and other human rights.²⁶¹

Criticisms may also be at stake both offline and online in Zambia as the law punishes seditious words that may bring disaffection to the government of Zambia. Such provisions and state-sponsored limitations online like website blocking, surveillance and introduction of internet taxes do not comply with international standards on restriction

257 n 69 above.

258 n 210 above.

259 as above.

260 See, generally, Human Rights Council 'Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai' (21 May 2012) A/HRC/20/27.

261 as above.

of the right to freedom of expression.²⁶² Aside that it cannot be reasonably justified in an open and democratic society, the restriction does not seem proportionate to the harm being sought to be neutralised by the law as the government has not shown that the excessive surveillance and website blockages are in the interest of the public. It is also important to note that these limitative tests must be jointly applied as part-compliance with the test of legality does not mean that it has complied with all the limitative requirements.²⁶³

Anonymisation of data provided for under article 45 Electronic Communications and Transactions Act of 2009 does not factor into consideration that anonymised data are capable of being de-anonymised.²⁶⁴ While considering that Article 66 of the Act requires a Court order for interception of communications in Zambia, requiring service providers to actively monitor communications is in direct contravention of the Constitution of Zambia. A 'real-time' monitoring of communications of citizens does not pass the test of proportionality as it is not specific towards an aim but general in scope which is empowers the state to use dragnets across board.

In addition, as common with other cyber security and cybercrimes laws in most African countries, the provisions of an offence on cyber-stalking or sending of information through a computer in the proposed Cyber security and Cybercrimes draft bill is problematic given the use of vague and unclear words. As provided for under international law, laws limiting rights must be clear and unambiguous enough for those to be affected to easily construe the offence being criminalised. This words may be used to curtail online freedoms. Also, the creation of the CMCC in both the Electronic Communications and Transactions Act of 2009 and the proposed cyber security and cybercrimes draft law is a duplication of onerous limitation of online rights.

Given the evidence of online threats against the civic space in Zambia, the right to privacy is also under threat in Zambia. The procurement of Chinese monitoring machines does not only fail the three-limitative test on the right to privacy, it places the lives of many civil society actors and HRDs in danger.²⁶⁵ The Citizen Lab report on Zambia shows that privacy rights in Zambia is at risk and are in grave violations of international and constitutional law of the country.

262 See, generally, Human Rights Council 'The promotion, protection and enjoyment of human rights on the Internet' (17 July 2018) A/HRC/29/32.

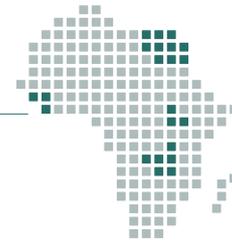
263 *Kenneth Good v Botswana*, Communication 313/05, 188.

264 M Miljanovic 'The false promises of data anonymization' (2015) <https://myshadow.org/false-promises-data-anonymisation> (accessed 15 October 2019).

265 n 256 above, 12.

5.6 Recommendations for Zambia

- The government of Zambia must review its laws and bills, especially those affecting the civil society and HRDs in line with international law and its Constitution. Particularly, the government must review the relevant sections of the NGO Act of 2009, the Penal Code of Zambia, Electronic Communications and Transactions Act of 2009, the Cyber security and Cybercrimes bill and its introduction of internet taxes in line with international law and its Constitution;
- The government of Zambia must work with relevant stakeholders to enact laws that protect the rights in the civil space both offline and online in Zambia including the Access to Information bill;
- The government of Zambia must investigate the violation of the rights of civil society actors and HRDs. It must also desist from use of online threats against civil society and HRDs in Zambia. Furthermore, the government must make transparent its relationship with foreign actors on the procurement of surveillance equipment; and
- The civil society and HRDs in Zambia should work with the government where possible to initiate the process for rights-respecting laws and policies in Zambia.



SECTION 6

OVERALL CONCLUSION AND RECOMMENDATIONS

5.1 Overall conclusion

This research focused on the shrinking civic space through the use of laws and digital attacks by governments in Egypt, Sierra Leone, Uganda and Zambia, describing different approaches and common trends. Considering the findings in the analysis of the countries under review, there is a growing connection between the use of laws that undermine human rights and digital threats to repress the civic space in Africa. Through a combined approach of legal analyses and digital security assessments, this report has shown that not only are governments complicit in the shrinking civic space in these countries, human rights in the digital age are becoming more at-risk than ever before. This shrinking civic space has become more prominent due to the relations between the state and civil society and this includes the current trend of state actors discrediting and delegitimising civil society through repressive policies. While contexts are different, governments are adopting common approaches against civil society across the continent. As discussed in this research, the civil society in Egypt, Uganda, Sierra Leone and Zambia have been caught up in this trend and civil society development have been under threat in these countries. These threats have taken different forms which for example are seen through barriers such as difficult funding requirements, intimidation of HRDs and professionals, physical and online threats to life and property and arbitrary arrests of HRDs.

These strategies by governments are as a result of the combination of legal and digital threats to counter legally permissible activities of the civil society in the countries under review. An example of laws used by governments is the antiterrorism laws that are

enacted as justification for countering terrorism, but which end up adversely impacting on the civic space and as a result disproportionately placing national security above all considerations. Matching this trend of bad laws are also state-sponsored online attacks against the civic space in the respective countries under review. In the digital age, the threats to civil society have become more sophisticated with governments embracing digital technologies, not only to increase efficiency in government business and serving their citizens but also in keeping opposition and dissent in check. The online civic space, especially in struggling democracies has become a vibrant environment which has resulted in greater demands for accountability. However, it has also become a space for state-sanctioned repression as well.

6.2 Overall recommendations

In light of the violations against civil society that have been mentioned, it is imperative that states implement and respect their obligations in international human rights instruments that they ratified. Thus, states are encouraged to take steps to secure the civic space to ensure that the civil society plays its role in ensuring good governance and holding the state accountable, without hindrance. The measures adopted have to be in compliance with international human rights norms and standards. The following recommendations are drawn from those standards through the work of the special mechanisms of the UN and AU.

Governments are urged to:

- **Repeal** all repressive laws that are inconsistent with constitutional and international human rights norms and standards, and adopt human rights-compliant laws and policies aligned with international human rights norms and standards. This will create an environment for the civil society to thrive;
- **Reform** the surveillance regimes in line with the International Principles on the Application of Human Rights to Communications Surveillance (the Necessary and Proportionate Principles);
- **Revise** and enact relevant national laws and policies to promote and protect the rights to privacy and freedoms of opinion, association, assembly and expression both offline and online bearing in mind the United Nations Human Rights Council Resolution HRC/RES/20/8 of 2012 stating that “the same rights that people have offline must also be protected online.²⁶⁶ Also, that these rights and freedoms are

²⁶⁶ United Nations Human Rights Council Resolution HRC/RES/20/8 of 2012.

mutually reinforcing rights and are essential for the enjoyment of other rights and pertinent in the work of civil society;

- **Implement** the African Commission's Guidelines on Freedom of Association and Assembly in Africa and the Guidelines on Principles of Freedom of Expression and Access to Information for Africa. These instruments encompass international human rights standards that will guide states in fostering a human rights culture even where civil society is concerned;
- **Adopt** multi-stakeholder approaches to ensure diversity, stakeholder-driven and user-centric policies. Adopting such an approach can maximise the potential for due diligence in human rights issues and full understanding of the various perceptions of stakeholders;
- **Adopt** measures towards increased digital and media literacy to ensure active public participation of citizens in the digital age;
- **Nurture** a culture of transparency in government business including on relationships with the private sector; and
- **Create** an environment for the judiciary to function independently and subject only to the Constitution and the laws of their countries as provided for by the International Principles on the Independence and Accountability of Judges, Lawyers and Prosecutors.

Civil society is urged to:

- **Advocate** for the repeal of repressive laws and adoption of human rights compliant legislation;
- **Participate** in law reforms;
- **Strengthen** advocacy on human rights in the digital age;
- **Engage** the government and private sector on human rights obligations;
- **Invest** in digital literacy and security trainings;
- **Engage** international human rights bodies in raising awareness on threats directed at civil society;
- **Submit** shadow reports during the state reporting process to enable human mechanisms to adequately engage the state parties;

- **Get** more involved with international human rights mechanisms for redress; and
- **Engage** in capacity building for the judiciary and law makers on digital rights.

Private sector should:

- **Work** with civil society actors and other stakeholders in developing and implementing human rights compliant policies;
- **Insist** on multi-stakeholder approaches on internet governance issues; and
- **Ensure** transparency in the policies, standards and actions that have an impact on human rights.

Funders should:

- **Support** civil society initiatives on digital and media literacy;
- **Incentivise** digital security; data protection and other capacity enhancing endeavours in the digital age.

International and continental human rights bodies should:

- **Develop** robust normative standards on human rights in the digital age and persistently condemn acts of repression by governments against civil society.



Centre for Human Rights, University of Pretoria, and the
Collaboration on International ICT Policy in East and Southern Africa (CIPESA)

www.chr.up.ac.za | www.cipesa.org

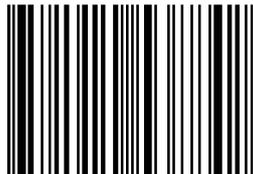
This report documents the threats to civil society in the digital age by examining the legislative and regulatory framework, as well as state action in four countries in Africa: Egypt, Sierra Leone, Uganda and Zambia. These countries were selected from the four main geographic regions of Africa, in order to provide a sense of the state of civic engagement in the digital age across the continent. The case studies are clearly not representative of what is happening on the continent, but are illustrative of some prominent trends. The recommendations emanating from the research call for the states to revise and repeal identified restrictive laws and align them with international standards. Civil society organisations and human rights activists are also encouraged to enhance their individual and organizational digital knowledge and expertise to more robust counter disruptive state measures. This expertise should be enhanced through a human rights lens and should extend to other stakeholders including judicial officers, legislators, law enforcement and the general public through sustained multi-stakeholder engagement.

It is this state of affairs that motivated the development of this research on *Civil Society in the digital age: identifying threats and mounting pushbacks*.



Centre for Human Rights, University of Pretoria, and the
Collaboration on International ICT Policy in East and Southern Africa (CIPESA)
www.chr.up.ac.za | www.cipesa.org

ISBN: 978-1-920538-84-2



9 781920 153884 2