institute of development studies

# Digital Rights in Closing Civic Space: Lessons from Ten African Countries

February 2021

Tony Roberts (ed.)

The Institute of Development Studies (IDS) delivers world-class research, learning and teaching that transforms the knowledge, action and leadership needed for more equitable and sustainable development globally.

For more information visit: **www.ids.ac.uk**







First published by the Institute of Development Studies February 2021

Editor: Tony Roberts

Citation: Roberts, T. (ed.) (2021) *Digital Rights in Closing Civic Space: Lessons from Ten African Countries*, Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2021.003**

ISBN: 978-1-78118-762-3

DOI: **10.19088/IDS.2021.003**

A catalogue record for this publication is available from the British Library



**Funder acknowledgements**

The African Digital Rights Network (ADRN) and this publication are generously funded by the Global Challenges Research Fund (GCFR) through the UK Research and Innovation (UKRI) Collective Fund for Digital Innovation for Development in Africa.

The authors would also like to thank Kevin Hernandez, Andrea Jimenez Cisneros, Becky Faith, and Pedro Prieto Martín for reviewing and helping improve earlier versions of these reports, David Haddock for the graphics, Production Editor Beth Richard, and copy editors James Middleton and Dee Scholey.

Available from:
Institute of Development Studies, Library Road
Brighton, BN1 9RE, United Kingdom
+44 (0)1273 606261
**ids.ac.uk**

IDS is a charitable company limited by guarantee and registered in England
Charity Registration Number 306371
Charitable Company Number 877338

# Digital Rights in Closing Civic Space: Lessons from Ten African Countries

February 2021

Tony Roberts (ed.)

# Contents

# Notes on Contributors

**Abrar Mohamed Ali** is a development practitioner and digital rights researcher in Khartoum, Sudan. She holds an MA in Development Studies from the Institute of Development Studies, UK. Abrar's research interests include digital rights in Africa and, more specifically, internet shutdowns in Africa.

**Tanja Bosch** is Associate Professor of Media Studies and Production in the Centre for Film and Media Studies, University of Cape Town. She teaches multimedia production, social media, and qualitative research methods. Her book *Broadcasting Democracy: Radio and Identity in South Africa* was published by HSRC Press in 2017. Her second book, *Social Media and Everyday Life in South Africa* (2021, Routledge), explores how South Africans use social media for personal and group identity formation. Tanja is at the forefront of publishing in the area of social media activism in Africa, most notably on #RhodesMustFall and #FeesMustFall.

**Atnafu Brhane** is a digital rights activist based in Ethiopia. In 2012, he co-founded the blogging collective Zone9 Bloggers and conducted extensive social media campaigns on rule of law, constitutionalism, and freedom of expression. In 2016, the collective accepted awards from Reporters Without Borders, Human Rights Watch, Martin Ennals, and Committee to Protect Journalists. In 2014, Atnafu was arrested and charged with Ethiopia's anti-terrorism proclamation and was imprisoned for 18 months. From 2018–19, Atnafu was Digital Integrity Fellow at Open Technology Fund and worked with human rights defenders and human rights organisations in Ethiopia on creating awareness in digital literacy, privacy, and security. He co-founded the Network for Digital Rights in Ethiopia and is Programme Director and co-founder of the Center for Advancement of Rights and Democracy.

**Mohamed Farahat** is an Egyptian-based legal practitioner, trainer, and political researcher. He works as Legal Analyst for HUMENA for Human Rights and Civic Engagement, as Legal Consultant for International Organization for Migration Egypt, as Legal Expert for the Center for Migration and Refugees Studies, and as Research Fellow for ICT Policy Centre for Eastern and Southern Africa (CIPESA). He is also member of the Internet Rights and Principles Coalition steering committee and of the North Africa Internet Governance Management Advisory Group. Mohamed holds a law degree from Cairo University, and postgraduate diplomas in human rights and civil society, international negotiation, African studies, parliamentary studies, and international law. Currently, he is an MA researcher in the Faculty of High African Studies, Cairo University.

DOI: 10.19088/IDS.2021.004

**Iginio Gagliardone** is Associate Professor in media and communication at the University of the Witwatersrand, and Associate Research Fellow in new media and human rights in the Programme in Comparative Media Law and Policy, University of Oxford. He holds a PhD from the London School of Economics. Iginio has been living between Italy, Ethiopia, the UK, and South Africa, researching the relationship between new media, political expression, and human development, and exploring the emergence of distinctive models of the information society in the global South. Recent publications include *China, Africa, and the Future of the Internet* (2019, Zed Books), *World Trends in Freedom of Expression and Media Development* (2018, UNESCO), and *The Politics of Technology in Africa* (2016, Cambridge University Press).

**George Hamandishe Karekwaivanane** is a lecturer in African Studies at the University of Edinburgh. He received his doctorate from the University of Oxford and his research focuses on socio-legal studies and digital cultures. His recent publications include a Special Issue in the *Journal of Eastern African Studies* on 'Publics in Africa in a Digital Age' and *The Struggle Over State Power in Zimbabwe: Law and Politics Since 1950* (2017, Cambridge University Press).

**Natasha Msonza** is an information security analyst, trainer, and privacy advocate. She is cofounder of the Digital Society of Africa, a distributed network of technologists that applies holistic approaches to supporting human rights defenders, marginalised communities, and everyday technology users in becoming more resilient and secure in their use of digital tools online and offline. Natasha has interests in internet governance and research. For several years, she has produced the *State of Internet Freedom in Zimbabwe* country report commissioned by CIPESA. Natasha holds a Master's degree in Human Development Studies.

**Ayobami Ojebode** is Professor of Applied Communication in the Department of Communication and Language Arts, University of Ibadan, Nigeria. His research interests are in community communication, community governance, new media, and political communication. Ayobami has led and participated in research into the online advocacy and empowerment by the Bring Back Our Girls movement in Nigeria, social and political action for energy rights, voices and experiences of retiring migrants, and community media and governance. He is a member of the African Digital Rights Network and other professional and academic associations.

DOI: 10.19088/IDS.2021.004

**Oyewole Adekunle Oladapo** is a lecturer in the Department of Communication and Language Arts, University of Ibadan, Nigeria. He received his doctoral degree in 2018 from University of Ibadan. His doctoral thesis examined variations in online and offline audiences' deconstruction of newspaper representation of Nigeria's unity. Oyewole's areas of interest include media and development, protests and politics on social media, and media and identity. He has authored and co-authored book chapters and articles in both local and foreign journals.

**Juliet Nanfuka** has a background in journalism and new media. She works with the Collaboration on ICT Policy in East and Southern Africa (CIPESA) where she works on digital rights research, advocacy, and projects related to the advancement of internet freedom in Africa. Juliet has a keen interest in freedom of expression, access, digital content, and the digital economy.

**Nanjala Nyabola** is an independent writer and researcher based in Nairobi, Kenya. Her work focuses on the intersection between technology, media, and society. She has held research associate positions with the Centre for International Governance Innovation, the Overseas Development Institute, the Oxford Internet Institute, and is a Digital Civil Society Fellow at Stanford University. Nanjala has published in several academic journals, including *African Security Review* and *Women's Studies Quarterly*, and contributed to numerous edited collections. She also writes commentary and is the author of *Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya* (2018, Zed Books) and *Travelling While Black: Essays Inspired by a Life on the Move* (2020, Hurst Books).

**Kathleen Ndongmo** is a leading African strategist and communications specialist. A digital rights advocate, she was one of the leading voices against the Cameroonian internet shutdown of 2017, actively contributing to the #BringBackOurInternet campaign. She has authored several regional digital rights reports, including the Cameroon update for the 2016 and 2017 *Digital Rights in Africa Report*, and the 2019 Cameroon country report for the *State of Internet Freedom in Africa* report, commissioned by CIPESA. She is also a co-author to the *Open Internet for Democracy Advocacy Playbook*, which serves as a companion piece to *Democratic Principles for an Open Internet*. Kathleen is an Open Internet for Democracy Fellow, and alumna of the prestigious International Visitor Leadership Program.

DOI: 10.19088/IDS.2021.004

**Sam Phiri** is a member of faculty in the Department of Media and Communication Studies at the University of Zambia where his research focuses on strategic intelligence, political communication, strategy and planning. His publications include *Political Dis-Empowerment of Women by ICTs: The Case of the Zambian Elections* (2016, IGI Global) and *Of Elephants and Men: Understanding Gender-Based Hate Speech in Zambia's Social Media Platforms* (2020, IGI Global).

**Tony Roberts** is a Research Fellow in the Digital Cluster at the Institute of Development Studies. His research focuses on digital rights, digital citizenship, and digital inequalities. He has worked at the intersection of digital technologies, international development, and social justice since 1988. After lecturing in New Technology and Education at the University of East London, Tony founded and lead two international development agencies, Coda International and Computer Aid International for a decade each before completing a PhD in digital development. A full list of publications, blogs and podcasts is available on his website **Appropriating Technology** or on **Google Scholar**.

DOI: 10.19088/IDS.2021.004

# Opening and Closing Online Civic Space in Africa: An Introduction to the Ten Digital Rights Landscape Reports

Tony Roberts and Abrar Mohamed Ali

 DOI: 10.19088/IDS.2021.005

# Abstract

This report introduces findings from ten digital rights landscape country reports on Zimbabwe, Zambia, Uganda, Sudan, South Africa, Nigeria, Kenya, Ethiopia, Egypt, and Cameroon. They analyse how the openings and closings of online civic space affect citizens' digital rights. They show that:

a. When civic space closes **offline** citizens often respond by **opening civic space online**.
b. When civic space opens **online** governments often take measures **to close online space**.
c. The resulting reduction in digital rights makes it **impossible to achieve** the kind of inclusive governance defined in the Sustainable Development Goals (SDGs).

We know far more about openings and closings of online civic space in the global North than we do in the global South. What little we do know about Africa is mainly about a single country, a single event, or single technology. For the first time, these reports make possible a comparative analysis of openings and closings of online civic space in Africa. They document 65 examples of the use of digital technologies to **open** online civic space and 115 examples of techniques used to **close** online civic space. The five tactics used most often to close online civic space in Africa are digital surveillance, disinformation, internet shutdowns, legislation, and arrests for online speech.

The reports show clearly that any comprehensive analysis of digital rights requires consideration of the wider political, civic space, and technological contexts. We argue that countering the threats to democracy and digital rights discussed in the reports requires new evidence, awareness, and capacity. We propose applied research to build capacity in each country to effectively monitor, analyse, and counter the insidious impact of surveillance and disinformation; and a programme to raise awareness and mobilise opinion to open civic space and improve citizens' ability to exercise, defend, and expand their digital rights.

 DOI: 10.19088/IDS.2021.005

# 1. Introduction

**Civic space remains open in only two of Africa's 54 countries**,[1] according to CIVICUS (2020). The reduction in safe public spaces in which democratic debate can take place represents a breach of citizens' digital rights and makes achievement of the Sustainable Development Goals (SDGs) impossible. This report presents the literature review used by the African Digital Rights Network[2] to provide the conceptual framing for the commissioning of digital rights landscape country reports on ten African countries. It also presents preliminary findings and makes tentative recommendations designed to enhance the ability of citizens to exercise, defend, and expand their digital rights.

**Civic space refers to the public places where citizens can freely exercise their human rights.** This includes the right to freedom of opinion and expression. Civic spaces can be **offline** physical locations, such as village halls or public squares, or **online** virtual spaces for digital discussion, online petitions, or hashtag campaigns. Online civic space can provide a refuge for marginalised or opposition groups, particularly in offline contexts where such voices are disciplined or oppressed. Civic space is crucial for any open and democratic country in which citizens and civil society are free to hold power-holders accountable, draw attention to neglected issues, and foster inclusive decision-making at all levels (Kode 2018).

**Digital rights are human rights in online spaces.** These rights include, but are not limited to, the right to privacy, freedom of opinion and speech, freedom of information and communication, gender rights, and the right to freedom from violence (APC 2006; Abraham 2014; UN 1948). Citizens' digital rights are breached if they are the subject of digital surveillance; if they are covertly targeted with disinformation to manipulate their beliefs and behaviour; if their mobile or internet connection is restricted; or if they are arrested or attacked for expressing political opinion online (Jorgensen 2006; GISWatch 2014; GISWatch 2019; Zuboff 2019). Examples of digital rights breaches include online gender-based violence perpetrated by misogynist groups; mass interception of digital communications by state spy agencies; or private sector actors trading citizens' digital profiles to enable covert voter disinformation campaigns.

**As governments close civic space *offline*, citizens often open civic space *online*** (Buyse 2018; Roberts 2019). Mechanisms used to close offline civic space have included laws, regulations, limits on funding, threats and

1 The two island states of Cabo Verde and São Tomé and Principe.
2 **African Digital Rights Network**.

 DOI: 10.19088/IDS.2021.005

violence, arbitrary arrest, and detention (Dupuy, Ron and Prakash 2014; Hossain *et al.* 2017, 2019). Although research on closing **offline** civic space is beginning to receive the attention that it deserves (PartnersGlobal *et al.* 2017; Hossain *et al.* 2018), there has been much less research attention on the openings and closings of **online** civic space in Africa.

**When citizens open online civic space, governments often act to close it down.** For example, since citizens used SMS (short message service) text messages to organise politically in Tunisia and Egypt in 2011, governments in 50 African countries imposed compulsory SIM (subscriber identity module) card registration (Privacy International 2019). Then, when citizens used social media to voice opposition, some governments blocked it or introduced price rises to make accessing it unaffordable (Nanfuka 2019). Zeynep Tufekci's book *Twitter and Tear Gas* (Tufekci 2017) is a comprehensive account of how citizen use of digital tools in Egypt was met with concerted state repression to close democratic space. Tech-savvy activists initially gained an advantage over established political actors by using mobile and internet campaigning to create online civic spaces. However, governments are now rapidly building their own capabilities to dominate these online spaces using digital surveillance, disinformation and intentional internet disruptions including shutdowns, bandwidth throttling (slowing down), bans and blocking (CIPESA 2016; Freyburg and Garbe 2018; Freedom House 2018; Taye 2020).

**Use of online civic space has its own limitations and risks.** The ability to access and make productive use of digital technologies is uneven across gender, income, and ethnic groups, such that its patterns of use reflect, reproduce, and amplify existing intersectional inequalities (Hernandez and Roberts 2018; Roberts and Hernandez 2019). Women activists and politicians often face sustained abuse and violence if they are vocal online, creating a chilling effect (Faith and Fraser 2018). The use of mobile devices and online spaces involves leaving digital traces that enable systematic surveillance (Bradshaw and Howard 2019; Zuboff 2019). This digital surveillance is used to target covert voter disinformation and manipulation (Nyabola 2018; Howard 2020); to disrupt internet access to information and communications (Taye 2018); and to mark individuals for arrest, torture or even murder (Ibrahim 2020).

**The repressive use of digital technologies by states and corporations has been characterised as 'digital authoritarianism'** (Freedom House 2018). The Egyptian and Zimbabwean governments are among those who are known to have imported artificial intelligence-based surveillance technologies from the US and China to spy on their own citizens' mobile and internet communications (Feldstein 2019). Governments are buying new mobile phone interception (Marczak *et al.* 2020) and internet shutdown and disruption technologies (Taye 2020). Politicians are using digital technologies to inflame

 DOI: 10.19088/IDS.2021.005

ethnic division and drown out democratic dialogue and debate (Nyabola 2018; Woolley and Howard 2019). This closes civic space and diminishes citizens' rights to freedom of opinion and expression.

**These tactics could threaten the integrity of elections in over 50 African countries that have elections scheduled in the next five years** (EISA 2020). They could also influence the outcomes of critical policy debates, including those on vaccines, climate change, gender, and sexual rights – all of which are known targets for digital disinformation and covert influence by powerful foreign and domestic lobbying interests (Jones 2019; Woolley and Howard 2019). In the 2017 elections in Kenya, political elites reportedly spent US$20m on fake news and covert disinformation campaigns designed to manipulate citizens' beliefs and voting behaviour (Brown 2019). In 2020, the number of intentional internet shutdowns by African governments rose from 21 to 25. They were often scheduled at the time of elections or popular protests (Taye 2020). Shutting down the internet reduces the rights to access information and to communicate freely, and the economic right of online traders to conduct business (Statista 2020).

**Existing research on the use of digital tools to close civic space is limited, ad hoc, and fragmented.** Currently, we know more about digital openings of civic space than we do about digital closings of civic space. We also know far more about the global North than we do about the distinctive features in the global South. The research evidence about African countries that does exist is typically about a single event, or single technology, in a single country. Technical studies are often divorced from consideration of explanatory political and civic contexts. There is currently little comparative analysis on openings and closings of civic space across Africa. Without more detailed empirical evidence about the dimensions and distinctive dynamics of the problem on the African continent, it is impossible for local actors to design effective remedies and countermeasures to restore civic space and secure digital rights.

**The ten country reports contained in this collection were commissioned to address these gaps.** The reports are from Zimbabwe, Zambia, Uganda, Sudan, South Africa, Nigeria, Kenya, Ethiopia, Egypt, and Cameroon. They are intended to provide an initial scoping of the digital rights landscape within each nation and across the African continent. Each report begins with three sections that review key developments between 2000 and 2020 in the country's political history, civic space dynamics and key technological changes. To aid cross-country comparison, each report contains two summary tables illustrating the timeline of key developments in the opening and closing of civic space, and the use of digital technologies by citizens and governments. The reports present preliminary findings and make tentative recommendations about how to open civic space and enhance citizens' ability to exercise, defend and expand their digital rights.

 DOI: 10.19088/IDS.2021.005

**Initial research results include 180 examples of the use of digital technologies to either open or close civic space.** The reports illustrate how wider political dynamics, and increasing availability of mobile and internet technologies, have shaped both openings and closings of civic space. In many of the country reports, the opening of civic space that characterised the years preceding the millennium has been replaced by closing civic space a decade later. The reports provide almost twice as many examples of digital technologies being used to close civic space as to open it. The current wave of surveillance and disinformation technologies has potentially serious implications for the possibility of inclusive dialogue and sustainable development. This **turn to digital authoritarianism** became especially pronounced in the wake of the so-called 'Arab Spring' in 2011, when citizen uprisings unsettled entrenched political elites, who then scrambled to build their own arsenal of digital tactics and techniques to control online discourse.

**The country reports show clearly that a comprehensive understanding of digital rights requires cognisance of the wider political, civic space and technological contexts.** Taken together, the reports identify the need for an applied research programme that addresses existing gaps in evidence, awareness, legislation, and capacity. We argue that a multi-sector network is necessary to enhance the domestic capacity in each African country to overcome closing civic space and breaches of digital rights. To this end, we recommend engaging with four key constituencies:

- **Researchers** – to produce new **evidence** about surveillance actors, tools, tactics and techniques.
- **Journalists** – to raise **public awareness** about the practices and consequences of surveillance.
- **Policymakers** – to map existing **legislation**, identify gaps and advance a public policy agenda.
- **Activists** – to expand **civic engagement** to tackle surveillance, disinformation and shutdowns.

The next section of this report will outline the literature review that provided the conceptual framing for the ten country reports. Preliminary findings from the country reports are then presented on the range of technologies tools, tactics and techniques identified, before drawing some tentative conclusions and summarising the recommendations made by the report's authors.

 DOI: 10.19088/IDS.2021.005

# 2. Literature review

This section presents the literature review and conceptual framing used in commissioning the ten digital rights landscape country reports. The section summarises the literature on: (a) digital rights; (b) civic space and sustainable development; and (c) closing civic space. It concludes by identifying gaps in the existing literature and opportunities for further research.

**Human rights are the rights and freedoms that every person is entitled to.** The Universal Declaration of Human Rights bestows the same rights on every human irrespective of age, gender, ethnicity, sexuality, wealth, political or religious opinion or other status (UN 1948). These human rights include freedom of opinion and speech, political affiliation, privacy, and assembly. Everyone has the right to information, freedom of association, communication, and direct and indirect participation in political and public affairs (OHCHR 2020).

**Digital rights are those same rights in online spaces.** Given the increasing centrality of the internet as a space for information exchange and following the findings of the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression (UNHRC 2011), the UN declared that 'the same rights people have offline must also be protected online'. The UN General Assembly later recognised the 'unique and transformative nature of the internet, not only to enable individuals to exercise their right to freedom of opinion and expression, but also a range of other human rights, and to promote the development of society as a whole' (UNHRC 2018). The African Declaration on Internet Rights and Freedoms (African Declaration 2019) built upon these foundations to provide a detailed articulation of digital rights. The declaration includes a civil society section giving them the duty to 'advocate for Internet rights and freedoms; monitor Internet laws and regulations; and highlight abuses' (*ibid.*).

**There is broad agreement that use of digital technologies can enable sustainable development** (UNDP 2015; World Bank 2016; WSIS 2018); affect government transparency and accountability (OECD 2018; McGee *et al.* 2018); enhance civil society (Michelson 2006); and play a positive role in women's empowerment (Buskens and Webb 2009; Moolman, Primo and Shackleton 2011; Hafkin 2012; Buskens and Webb 2014). As a result, SDGs include specific targets for extending mobile and internet use (SDG 9c); expanding access to information and communication technologies (ICTs) (SDG 17.6 and 17.8); and women's empowerment (SDG 5b). There is extensive literature documenting the ways in which the use of digital technologies can support social mobilisation and collective action by connecting citizens,

 DOI: 10.19088/IDS.2021.005

creating new spaces for engagement between citizens and the state, and helping to empower citizens and strengthen their agency for engagement (McGee *et al.* 2018).

**However, the use of digital technologies can also constrain citizens' voices, undermine and obstruct accountability, and facilitate surveillance and repression** (*ibid.*). Any technology has more than one potential application. It is common for technologies to be appropriated for purposes other than those originally in the mind of their inventors. As Kranzberg's first law of technology notes, the technologies themselves are neither good nor bad, but nor are they ever neutral (Kranzberg 1986). The inherent 'interpretive flexibility' of technologies (Pinch and Bijker 1984) allows them to be used in 'good' or 'bad' ways, with the use of technologies often reflecting the politics and values of society and users (MacKensie and Wajcman 1985; Feenberg 1992).

**Affordances are a useful concept for analysing the use of technology to open and close civic space.** The concept of affordances concerns what 'action possibilities' a particular technology allows, invites or enables (Gibson 1977; Norman 1988). For example, the use of social media affords citizens the action possibility of publishing opinion and images instantly, at scale and internationally, enabling real-time reporting of police brutality or viral hashtag campaigns such as #BlackLivesMatter or #MeToo. However, social media also affords governments and corporations the action possibility of surveillance-profiling and disinformation micro-targeting in order to covertly manipulate citizens' beliefs and voting behaviour (O'Neil 2016; Benjamin 2019; Zuboff 2019; Sadowski 2020). Analysing the affordances of different technologies is advantageous in understanding their use in opening and closing civic space in ways that enhance or diminish digital rights.

**Africa has experienced a rapid – but uneven – expansion in the use of mobile and internet technologies.** This has produced digital dividends for some in the form of improved social and economic development (Buskens and Webb 2014; WSIS 2018). However, access to digital devices and connectivity is uneven, creating new exclusions, and digital divides. These divides exist both within and between countries (World Bank 2016). The use of digital technologies has been shown to reflect, reproduce, and amplify existing patterns of (dis)advantage (O'Neil 2016; Eubanks 2017; Hernandez and Roberts 2018). Technology access and the ability to make effective use of it, is uneven across intersecting divides of gender, class, and ethnicity (Eubanks 2017; Noble 2018; Benjamin 2019). A mobile gender gap exists across low- and middle-income countries: 300 million fewer women than men have access to mobile internet (GSMA 2020). The gap continues to grow between those who are able to regularly upgrade to the latest devices and fastest connections, and those who remain unconnected or digitally illiterate (Roberts and Hernandez 2019).

 DOI: 10.19088/IDS.2021.005

**Uneven digital access and digital literacy create hierarchies of digital citizenship.** Citizenship is often understood narrowly as the relationship of rights and responsibilities between an individual and the state. A broader and more inclusive understanding of citizenship focuses on the actions of a person or persons, whether formally documented citizens or not, in exercising, defending, or claiming rights. This agency-based rights-claiming conception of citizenship is the most appropriate in the context of digital rights. **Digital citizenship** is this same rights-claiming citizen agency but in online spaces (Isin and Ruppert 2015; Hintz, Dencik and Wahl-Jorgensen 2019). Due to uneven technology access, not all citizens are digital citizens; and not all digital citizens have equal access to the kind of digital devices, online spaces, or digital literacy necessary to exercise, defend, or expand digital rights.

**The UN is among those arguing that an open and vibrant civic space is essential to inclusive democracy and sustainable development** (UNDP 2015; World Bank 2016). To reflect this belief SDG 16 commits signatory governments to achieving 'inclusive, participatory, and representative decision-making at every level'; and SDG 17 requires building a partnership for development between civil society, governments, and the private sector (UNDP 2015). All ten countries included in this study are signatories to the SDGs. The UN High-Level Forum on Aid Effectiveness and the High-Level Panel on the 2030 Sustainable Development agenda both underscored the central role of civil society as partners in delivering the SDGs (UN 2013; ACT Alliance and CIDSE 2014; ICNL 2016).

**However, in many countries the civic space necessary for inclusive, participatory dialogue and policy deliberation is rapidly shrinking** (Dupuy, Ron and Prakash 2016; Hossain *et al.* 2018; CIPESA 2019; Freedom House 2019a). In 2020, over 90 per cent of African countries were experiencing significant restrictions to basic civic freedoms, with only 2 out of 54 countries categorised as having open[3] civic space (CIVICUS 2020). Mechanisms used to close civic space have included deregistering non-governmental organisations, regulations to cut off funding, violence and harassment, arbitrary arrest and disappearance of civil society actors (Dupuy *et al.* 2016; Hossain *et al.* 2018). Citizens who propose policy alternatives, publicly criticise the government or organise political opposition are at risk of arrest and violence (CIVICUS 2019). In terms of political rights and civil liberties, 2020 was the 14th consecutive year of global decline (Freedom House 2020). Trust in politicians and the democratic process is in decline globally (Bertsou 2019). Unless this democratic backsliding is reversed, the global challenge of achieving inclusive and sustainable development as defined in the SDGs is unattainable by 2030.

3 **CIVICUS Monitor** uses five categories of open, narrowed, obstructed, restricted and closed.

 DOI: 10.19088/IDS.2021.005

**During periods of *closing civic space* activists forced underground or into exile have often fought back by *opening online civic space*** from where their right to freedom of speech and assembly can be exercised and defended (Buyse 2018; Roberts 2019). The use of SMS text messages by Kenyan activists to create an online map of unfolding election violence in 2007 (Okolloh 2009; Roberts and Marchais 2018) and by Egyptian feminists to map sexual harassment in Cairo (Peuchaud 2014) are positive examples of using digital technologies to create online civic space. The opening of civic space online has been characterised by hashtag campaigns, viral memes, and civic technologies as mechanisms for digital rights advocacy (Nyabola 2018; Solomon 2018). Online civic space has been particularly valuable for repressed groups to discuss sensitive subjects; to project the voices of underrepresented groups, such as LGBTQI and ethnic minorities; and to propose policies that have been inadequately represented by establishment media and political parties (Tufekci 2017; Gurumurthy, Bharthur and Chami 2017; Hossain *et al.* 2019). However, online civic space is not open to everyone equally. For example, women, including female politicians, and LGBTQI groups often experience gender-based violence in online spaces (APC 2018; Faith and Fraser 2018; Vlahakis 2018).

**Repressive governments often deploy digital technologies to *close online civic space*.** In recent years, those with political and economic power have been able to expand their arsenal of digital technology tools and tactics to disrupt, drown out or shut down online civic space. This was exemplified by 'political marketing' consultancy Cambridge Analytica testing its covert voter manipulation methods in Kenya's 2013 election prior to their deployment in the UK's Brexit referendum and Donald Trump's 2016 presidential campaign victory (Nyabola 2018; Solomon 2018). In South Africa, another political marketing consultancy, Bell Pottinger, coordinated a network of trolls and bots[4] to fan the flames of racial division for political advantage (Fraser 2017). Political parties now routinely hire private companies – such as Cambridge Analytica and Bell Pottinger – to profile citizens using Facebook, mobile phone and other personal data (Zuboff 2018; Sadowski 2020) in order to micro-target voters with fake news and disinformation, via troll farms, cyborg networks, bot armies,[5] and other 'coordinated inauthentic behaviour' (Bradshaw and Howard 2017; Woolley and Howard 2017; Howard 2020).

**Internet surveillance and mobile intercept technologies are now regularly employed by African governments.** In addition to the social media surveillance discussed above, African governments are now buying mass surveillance technologies from the US or China to spy on citizens' email

4 Disinformation can be posted manually by people (called trolls) or automatically by programs (called bots).

5 Coordinated disinformation campaigns can be run by teams of trolls (working in troll 'farms'), by large numbers of automated bots (called 'bot-nets' or bot armies) and by integrated part-troll-part-bot 'cyborg networks'.

 DOI: 10.19088/IDS.2021.005

and internet communications (Feldstein 2019; Freedom House 2019). Some African governments are buying new mobile phone interception technologies (Marczak *et al.* 2020), and internet shutdown and disruption technologies (Access Now 2020). The number of intentional internet shutdowns in Africa rose from 21 in 2019 to 25 in 2020 (Taye 2020). In African elections over the next few years, incumbents and powerful challengers will continue to be able to hire troll farms and bot armies to disrupt debate, manufacture opinion and covertly manipulate voting behaviour (Baker and Blaagaard 2016; Bradshaw and Howard 2017; Woolley and Howard 2019). These covert measures damage democracy and diminish digital rights, making impossible the kind of inclusive and participatory governance outlined in the SDGs.

**Existing surveillance and disinformation literature is limited in detailing the dimensions and dynamics of the African experience.** From the first use of SMS in protest movements (Ekine 2010) to viral social media hashtag campaigns, researchers have documented African citizens' use of mobile phones and social media to open new online spaces (Nyamnjoh 2016; Tufekci 2017; Egbunike 2018). Members of the African Digital Rights Network have made important contributions to the growing literature on the use of digital technologies by citizens to open civic space (Gagliardone 2014; Nyabola 2018; Ojebode 2018; Bosch 2019; Karekwaivanane 2019a; Oosterom 2019; Roberts 2019; CIPESA 2019b, 2020). However, the closing of online civic space by African governments is relatively under-researched. The existing literature on digital surveillance and disinformation is predominantly focused on the global North. Relatively little is known about how these digital practices affect the 1.3 billion citizens of the 54 countries on the African continent. Addressing this gap is urgent given the critical importance of digital rights and open civic space to inclusive democracy and sustainable development. The research that does exist on Africa is primarily composed of single-technology, single-event, and single-country studies. **There is not yet any comparative African literature to identify trends, build theory, and guide policy and practice. Without clear definition of the detail, dimensions, and dynamics of the use of digital technologies to close civic space, it is impossible to design adequate remedies.**

Drawing on this literature review, the African Digital Rights Network resolved to make a preliminary contribution to addressing gaps in existing literature by producing a series of ten digital rights landscape country reports. Our intention was to conduct an initial scoping of which actors are using which digital technologies to both open and close civic space. The concepts of digital rights and literature on closing civic space were central to the

 DOI: 10.19088/IDS.2021.005

framing of the reports. Although the concepts of digital citizenship, gender inequalities, and digital affordances emerged from the literature review as a potentially useful lens, it was decided not to use them to frame the preliminary country reports, and to use them instead in the thematic papers planned in the next research phase.

Country report authors were required to preface their analysis of the digital rights landscape with three sections charting the most relevant political, civic space, and technology developments in each country's history between 2000 and 2020. This was in order to assess the extent to which contextual political events and technology developments affect openings and closings of civic space, and the ability of citizens to exercise their digital rights.

Before presenting the initial findings arising out of the ten digital rights landscape country reports, the next section briefly explains the methodological design and country sample.

 DOI: 10.19088/IDS.2021.005

# 3. Methodology

The African Digital Rights Network[6] was established in May 2020 using a Global Challenges Research Fund-UK Research and Innovation Digital Innovation for Development in Africa Networking Grant[7] to develop a network of activists, researchers, journalists, and policymakers working on digital rights in Africa. Its aim was to build new relationships that would stimulate novel research and innovation ideas that enhance citizens' ability to exercise, defend and expand their digital rights.

The network brought together 20 activists, analysts, and academics, some of whom had already published research on the use of digital activism to open civic space (Abraham 2014; Gagliardone 2014; Nyabola 2018; Ojebode 2018; Bosch 2019; Karekwaivanane 2019; Oosterom 2019; Roberts 2019), as well as internet shutdowns and disruption to close civic space (Taye 2019).

The initial focus was to document which actors were using which tools to open and close online civic space; and to identify gaps in evidence, awareness, and domestic capacity. The short-term goal was to inform the articulation of a multi-year research and innovation strategy to enhance digital rights in Africa. In the first six months, network members resolved to conduct an initial scoping of digital rights by producing country reports that provided a preliminary mapping and analysis of the drivers, actors, tools, and tactics being used in the ten countries both to open and close civic space. The medium-term objective was to build capacity for research and innovation that supported change in policy and practice. The longer-term aim was to open civic space and for citizens to be better able to exercise, defend and expand their digital rights.

The authors of ten digital rights landscape reports were asked to identify who was using which digital technologies, tools, tactics, or techniques to either open or close civic space in their country. In order to analyse the drivers of both openings and closings of civic space, authors were asked to preface their analysis of the current digital rights situation with a review of the key political, civic space, and technological developments that have shaped the digital rights landscape since the turn of the millennium. To enable cross-country comparison, each country report adopted this same structure and contained two tables: the first summarised key openings and closings of civic space between 2000 and 2020; while the second provided a timeline of the most relevant digital technology developments for the same period.

6 **African Digital Rights Network project page**, Institute of Development Studies website.
7 **GCRF Digital Innovation for Development in Africa**.

 DOI: 10.19088/IDS.2021.005

The ten-country sample was selected to be representative of the main geographical regions of the continent, as well as a range of levels of civic space openness, political and internet freedoms and economic development (Table 3.1). The sample was also pragmatically shaped by resource constraints, network contacts and positive responses to outreach.

## Table 3.1 Country selection

| | | Freedoms[8] | Civic space[9] | Internet freedom[10] | HDI[11] | Gini coefficient[12] | Internet access (%)[13] |
|---|---|---|---|---|---|---|---|
| **1** | **South Africa** | 79 | Narrowed | 70 | 0.709 | 63 | 56.2 |
| **2** | **Zambia** | 54 | Obstructed | 59 | 0.584 | 57 | 39.3 |
| **3** | **Kenya** | 48 | Obstructed | 67 | 0.601 | 41 | 87.2 |
| **4** | **Nigeria** | 47 | Obstructed | 60 | 0.539 | 35 | 61.2 |
| **5** | **Uganda** | 34 | Repressed | 56 | 0.544 | 43 | 40.5 |
| **6** | **Zimbabwe** | 29 | Repressed | 46 | 0.571 | 44 | 56.5 |
| **7** | **Ethiopia** | 24 | Repressed | 29 | 0.485 | 35 | 17.8 |
| **8** | **Egypt** | 21 | Closed | 26 | 0.707 | 32 | 48.1 |
| **9** | **Cameroon** | 18 | Repressed | n/a | 0.563 | 47 | 29.7 |
| **10** | **Sudan** | 12 | Repressed | 30 | 0.510 | 34 | 29.9 |

*Note:* HDI = Human Development Index

*Source:* Authors' own.

Rather than produce our own digital rights index, we chose instead to build on existing freedom and civic space scorecards by CIVICUS and Freedom House (see Table 3.1) and contribute country reports that provided a qualitative assessment of the dynamic nature of openings and closings and to document the wide range of digital tools, tactics and techniques being deployed to enhance and constrain digital rights. The intention was that this would enable textured findings that, when analysed, would shed light on the causes and solutions to the diminution of civic space and digital rights.

8 **Countries and Territories**, Freedom House.
9 **Monitor: Tracking Civic Space**, CIVICUS.
10 **Internet Freedom Scores**, Freedom House.
11 **Human Development Index**, Human Development Reports.
12 **Gini coefficient index**, World Bank.
13 **Internet World Stats: Usage and Population Statistics**.

 DOI: 10.19088/IDS.2021.005

The ten digital rights country landscape reports were commissioned from network members and external experts. The reports identified 65 examples of digital technologies being used to open civic space across Africa; and 115 examples of technologies, tactics and techniques used to close civic space. Several rounds of inductive coding were used to cluster these examples into ten categories of openings and 12 categories of closings, which are tabulated in the next section.

The country reports were prepared in the second half of 2020 during the coronavirus disease (Covid-19) pandemic. Covid-19 restrictions meant that all research activities had to be desk based and virtual. Research carried out was predominantly qualitative desk review of online secondary sources. The next phase of this research should incorporate primary data collection, including interviews with key informants to validate secondary data sources and deepen analysis in those areas identified as key during this initial scoping (e.g., surveillance, disinformation, and internet shutdowns). This qualitative analysis should be complemented with quantitative data analysis using software such as NodeXL to provide detailed analysis of the dimensions, principal actors and timelines of online hashtag and disinformation campaigns.

The next section presents some preliminary findings from the country reports and discusses their relevance to extending citizens' digital rights.

 DOI: 10.19088/IDS.2021.005

# 4. Findings and discussion

When this research was originally conceived, we imagined that our contribution might be to complement the **closing civic space** literature with data and analysis of **opening civic space** online. However, our findings about closing online civic space are at least as significant. Report authors identified almost twice as many examples of digital closings as digital openings.

**The ten country reports provide 65 examples of digital openings and 115 examples of digital closings.** We categorised the 65 examples of digital technology used to open civic space into ten main categories (Table 4.1). The 115 examples of technologies, tactics and techniques used to close civic space were coded into the 12 categories. The following sections present our findings from a preliminary analysis across the ten country reports and discuss their relevance for opening civic space and enhancing digital rights.

## Table 4.1 Digital openings

| | Digital openings of civic space – 65 examples presented in 10 categories | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | Increased – but uneven – access to mobile devices and internet | ZW | ZM | UG | SD | SA | NG | KE | ET | EG | CM |
| **2** | SMS activism | ZW | ZM | | | | | | | | |
| **3** | Social media activism | ZW | ZM | UG | SD | SA | NG | KE | ET | EG | CM |
| **4** | Civic tech activism | ZW | ZM | | | SA | NG | KE | ET | | CM |
| **5** | Diaspora amplifies message to apply international pressure | ZW | | UG | SD | | NG | KE | ET | | CM |
| **6** | Laws conferring new (digital) rights and entitlements | | ZM | UG | | SA | NG | KE | | EG | |
| **7** | Digital policies promoting access, rights, open data, etc. | | | | | SA | NG | KE | | | CM |
| **9** | Digital security (e.g. Signal, VPNs, encryption) | ZW | ZM | | SD | | | | | EG | CM |
| **8** | Strategic litigation to defend digital rights | | | | | SA | | KE | | | |
| **10** | IMSI sniffer app | ZW | | | | | | | | | |

*Note:* IMSI = International mobile subscriber identity; VPN = virtual private network

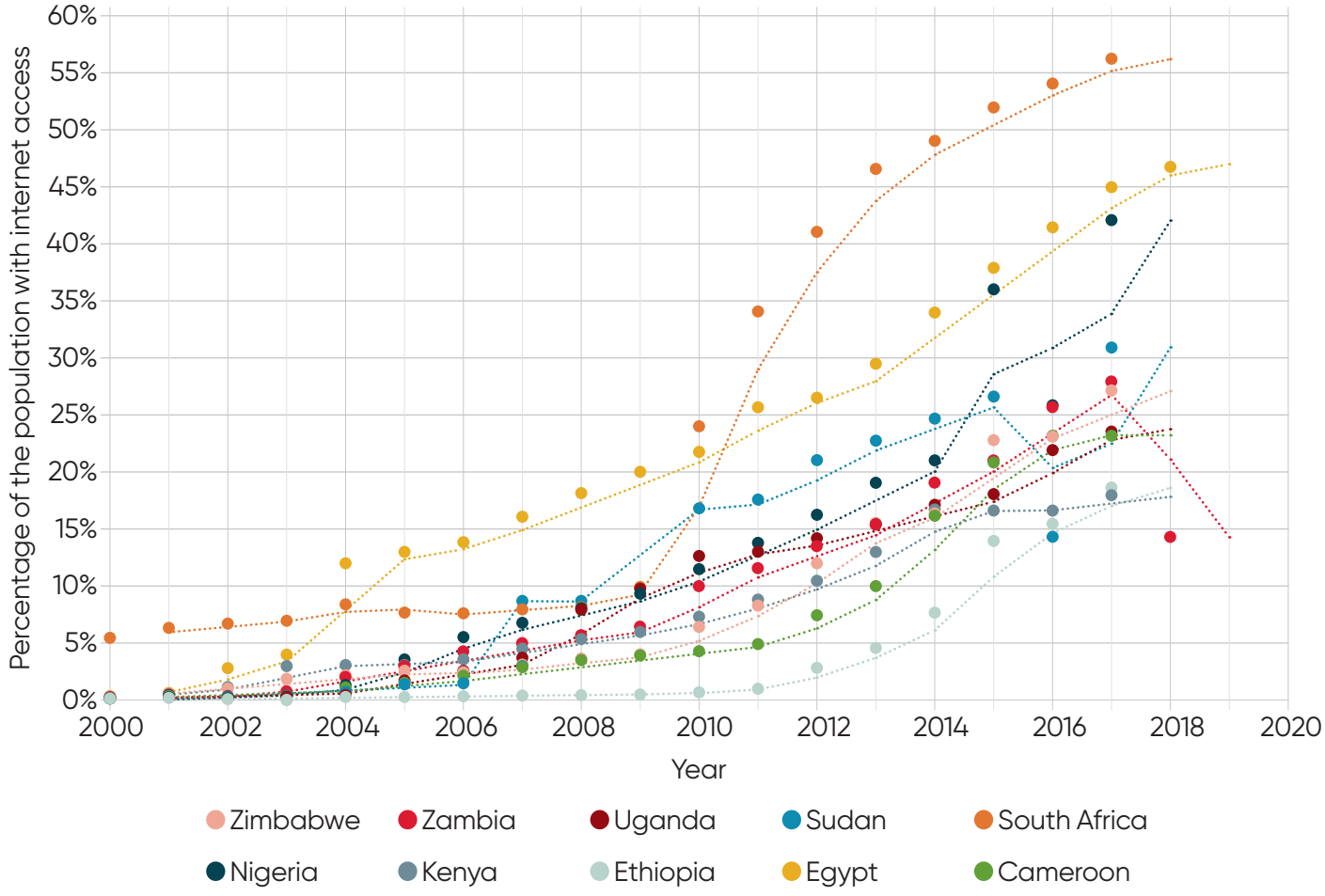
*Country key:* CM = Cameroon; EG = Egypt; ET = Ethiopia; KE = Kenya; NG = Nigeria; SA = South Africa; SD = Sudan; UG = Uganda; ZM = Zambia; ZW = Zimbabwe

*Source:* Authors' own.

 DOI: 10.19088/IDS.2021.005

**The rapid increase in mobile and internet access is a key driver of opening civic space online.** Although computers have long been used by activists, only a small percentage of the population in many countries had access to them. The relatively high levels of mobile phone ownership afforded new action possibilities for wider civic engagement. In all ten country reports the dramatic expansion of mobile phone use and internet access was highlighted as providing new means to instantly exchange information and to communicate interactively over long distances. These new affordances qualitatively increased the speed, scale and reach of citizen-led advocacy and civic engagement. However, as discussed below, access to digital devices and connectivity is uneven across gender and income, such that previously (under)privileged groups are often further (dis)advantaged.

## Figure 4.1 Growth in internet access




*Source:* Adapted from Internet World Stats[14]

14 **Internet World Stats: Usage and Population Statistics**.

 DOI: 10.19088/IDS.2021.005

**SMS activism was the first widespread digital tool used to create virtual civic space.** The Ethiopia country report (Gagliardone 2021, this collection) shows how the successful use of SMS text messages to issue 'calls to action' during the dramatic opening of civic space ahead of the 2005 election led the government to block and interrupt SMS services. In the country reports on Sudan and Uganda, the authors note that governments became so fearful of the power of SMS after the 2011 uprisings in Tunisia and Egypt that they temporarily blocked SMS in their countries (in this collection: Mohamed Ali 2021 and Nanfuka 2021).

The report by Karekwaivanane (2021, this collection) shows how sending bulk text messages became part of the repertoire of activists' methods in Zimbabwe and resulted in the government issuing a ban on all bulk SMS messaging in 2013. Around the same time, many African governments also started introducing mandatory SIM card registration, taking advantage of the surveillance affordances of mobile phones. Fifty of Africa's 54 countries had mandatory SIM card registration in place by 2019 (Privacy International 2019). Mobile phone SIM card registration removed from citizens the mobile affordance of anonymity, which preserved their right to privacy, and replaced it with the new action possibility for governments to surveil, geolocate, track and target citizens.

**Social media activism to open civic space online is the most evident tactic in the ten reports.** Although text messaging dominated in the first decade of the millennium, between 2010 and 2020 social media became the most used online civic space. The Zambia and Ethiopia country reports are among those that point to the key role played by independent citizen bloggers in opening online civic space (in this collection: Phiri and Zorro 2021 and Gagliardone 2021). The affordances of social media allowed 'unruly' citizen publication of opinion by individuals from outside establishment media, political parties, or civil society structures (Khanna *et al.* 2013).

However, by the second decade of the millennium corporate social media platforms such as Facebook, Twitter, and WhatsApp had in effect colonised online civic space. Citizens famously made use of Facebook and Twitter in the Egyptian revolution (Farahat 2021, this collection) and the platform quickly became central to digital citizenship across the continent. Some governments that perceive social media as more of a threat than an opportunity have sought to address this threat by blocking or limiting its use. The Zimbabwe government used massive price hikes to make social media unaffordable during periods of civic action, raising the cost by 500 per cent in 2016 and by 2,500 per cent in 2017 (Karekwaivanane 2021, this collection). The Ugandan government introduced a 'social media tax' (Nanfuka 2021, this collection). The majority of country reports (8 out of 10) document incidents in which those using social media to criticise the government are arrested or jailed.

 DOI: 10.19088/IDS.2021.005

**Civic tech activism became a popular way to open civic space in some African countries from around 2010 onwards.** The Nigeria country report (Oladapo and Ojebode 2021, this collection) shows how technology activism organisation BudgIT[15] used online space to monitor government budget implementation and hold extractive industries to account. The same report provides the example of activist organisation Enough is Enough Nigeria[16] promoting good governance and citizen engagement using the affordances of digital technologies for connective action (Bennett and Segerberg 2013). The South Africa country report (Bosch and Roberts 2021, this collection) documents the increase in civic tech organisations that afford possibilities for citizen campaigns, civic engagement and budget scrutiny, including Amandla.mobi,[17] GovChat[18] and Vulekamali.[19] Unlike SMS and social media activism, the country reports do not mention government efforts to close down the civic space opened by this form of activism. **Further research could usefully seek to understand whether incumbent governments see civic tech as a significant threat to their interests, whether there are examples of blocking or shutting down civic tech, and whether it is easier to contain and co-opt civic tech**.

**Diaspora engagement positively amplifies the international impact of online campaigns.** A clear theme emerging from the country reports was the importance of African diaspora engagement in amplifying domestic social media campaigns across the globe. The Cameroon country report (Ndongmo 2021, this collection) provides the example of #AnglophoneCrisis, which went viral internationally. Other hashtag campaigns mentioned in the country reports that were able to enlist the African diaspora to bring international pressure to bear on their governments were the Nigerian #BringBackOurGirls campaign, the Ugandan #FreeStellaNyanzi campaign, and the Ethiopian #FreeZone9Bloggers campaign (in this collection: Oladapo and Ojebode 2021, Nanfuka 2021, and Gagliardone 2021). It is worth noting that the ability for viral citizen-led campaigns to take place is enabled by the digital affordances of social media for instant, global, communication of calls to action, images, and video reportage. **This finding reinforces the need to build international networks of digital rights activists, journalists, and researchers to build public engagement and mobilise political pressure for policy change; and to facilitate South-to-South and international knowledge and experience exchanges**.

15 **BudgIT**.
16 **Enough is Enough Nigeria**.
17 **Amandla.mobi**.
18 **GovChat**.
19 **Vulekamali**.

 DOI: 10.19088/IDS.2021.005

**Digital security tools are effective but under-used.** A second important theme emerging from the reports was that secure digital practices are useful in opening civic space and extending digital rights. When the Sudanese government in 2018 shut down social media during pro-democracy protests, citizens used virtual private networks (VPNs) to stay online (Mohamed Ali 2021, this collection), but not everyone had the technical awareness to do so. The increase in surveillance and arrests for online speech creates a need for new tools, awareness, and skills to practice online safety and data safeguarding. The use of VPNs helps citizens to disguise their location and evade state censorship and blocking. Digital encryption allows activists and researchers to encode their emails, text and instant messages, and secure sensitive or personal data on their phones or other digital devices.

The uptake of the secure Signal messaging app among activists and journalists is one example of this trend. The Egypt country report notes that its use was considered significant enough for the government to block all use of the Signal app for a week in December 2016 (Farahat 2021, this collection). Too few African citizens, rights activists, and researchers know how to safely save, access, or send sensitive information using mobile phones, email, or apps (THRDC 2016). A significant amount of work has gone into producing digital security toolkits and training (Ganesh and Gutermuth 2014). However, levels of awareness and uptake remain low, and there is no existing knowledge infrastructure to efficiently share new surveillance and security resources. **Work to increase knowledge, make available, and enable effective use of digital security tools like VPNs, Signal and the Tor[20] internet browser should be built into project awareness-raising and capacity-building programmes.**

**Intersectional inequalities affect access to civic space, digital citizenship, and digital rights.** An emerging theme from the country reports that demands more focused attention in subsequent research phases is the complex ways in which gender and intersectional inequalities shape digital access, digital citizenship, and digital rights (Ganesh, Deutch and Schulte 2016). The country report on Cameroon (Ndongmo 2021, this collection) illustrates how LGBTQI citizens are restricted in their use of physical and online civic space. Similar closing of civic space occurred for citizens in Uganda and Nigeria (in this collection: Nanfuka 2021 and Oladapo and Ojebode 2021).

Civic space and digital rights are sometimes treated as universal categories, but as several country reports in this collection illustrate, women – especially low-income women, black women politicians, and LGBTQI citizens – do not enjoy equal access to digital tools or connectivity. They are subject to gender-based violence online, and this restricts their effective access and rights (APC

20 Unlike market-leading browsers from Google or Microsoft, the Tor browser disables tracking and cookies.

 DOI: 10.19088/IDS.2021.005

2018; Faith and Fraser 2018; Vlahakis 2018). It is important to be mindful that the use of all digital technologies generally excludes some entirely, and for others it creates hierarchies of access and ability (Roberts and Hernandez 2019). **In order to produce a more nuanced analysis, subsequent phases of this research should avoid binary conceptions of open/closed civic space and ask, 'Open to whom?' and 'Which civic space?' to produce more detailed and actionable analysis.**

## Table 4.3 Digital closings

| | Digital closings of civic space – 115 examples presented in 12 categories | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | Surveillance | ZW | ZM | UG | SD | SA | NG | KE | ET | EG | CM |
| **2** | Disinformation | ZW | ZM | | SD | SA | NG | KE | | EG | |
| **3** | Internet shutdowns | ZW | ZM | UG | SD | | NG | | ET | EG | CM |
| **4** | Laws and regulations | ZW | ZM | UG | SD | SA | NG | KE | ET | EG | CM |
| **5** | Arrests for online speech | ZW | ZM | UG | SD | | NG | KE | ET | EG | CM |
| **6** | Closing civic space to specific groups | ZW | | UG | | SA | NG | | ET | EG | CM |
| **7** | Mandatory mobile SIM card registration[21] | ZW | ZM | UG | SD | SA | NG | KE | ET | EG | CM |
| **8** | Price hikes, social media tax | ZW | ZM | UG | | | | | | | CM |
| **9** | Mandatory registration of bloggers | | ZM | UG | | | | | | | |
| **10** | Mandatory ID for internet cafe use | | | | | | | | | EG | |
| **11** | Bulk SMS ban | ZW | | | | | | | | | |
| **12** | Murder of digital election official | | | | | | | KE | | | |

*Country key:* CM = Cameroon; EG = Egypt; ET = Ethiopia; KE = Kenya; NG = Nigeria; SA = South Africa; SD = Sudan; UG = Uganda; ZM = Zambia; ZW = Zimbabwe

*Source:* Authors' own.

**Surveillance is the technique mentioned most often in country reports as closing civic space and diminishing digital rights**. The Kenya country report documents funding from the US and China to build mass surveillance infrastructure (Nyabola 2018). China and the US supply surveillance technologies to many African countries including Nigeria, South Africa,

21 Six of the country reports explicitly mention mandatory SIM card registration. We were able to establish that it is compulsory in all ten countries in this study, and in 50 of Africa's 54 countries overall (Privacy International 2019).

 DOI: 10.19088/IDS.2021.005

Sudan, Egypt, Cameroon, and Zambia. The Government of Uganda is among those which have procured mobile phone intercept technologies from Italian company Hacking Team (Nanfuka 2021, this collection), which also supplies the Sudanese government (Mohamed Ali 2021, this collection). While still in office President Robert Mugabe of Zimbabwe received a 'gift' of monitoring and surveillance technology from Iran that included mobile phone scanners, enabling his government to intercept citizens' private mobile communications and locations (Karekwaivanane 2021, this collection).

In addition to the above state surveillance technologies, the advent of 'surveillance capitalism' (Zuboff 2018) means that African governments are now able to buy surveillance as a commercial service from social media companies, intermediate data brokers, and political marketing consultancies such as Cambridge Analytica and Bell Pottinger. US corporations including Facebook, Twitter, YouTube, and WhatsApp have effectively privatised and monopolised online civic space. This enables those corporations to monitor and track millions of citizens in key marginal constituencies; ascertain their political preferences, 'likes' and trigger issues; predict their voting behaviour; and then sell their digital profiles as a commodity to powerful politicians for targeting and covert manipulation (Bradshaw and Howard 2017; Zuboff 2019; Sadowski 2020). **Minimal detailed research and analysis exists on surveillance drivers, actors, mechanisms, and appropriate responses in Africa. This is a critical area in which further research is urgently needed.**

**Surveillance involves an inherent power imbalance between the watcher and the watched.** Ways to redress the power imbalance include building public awareness about rights and surveillance practices and building the 'sousveillance' (Mann *et al.* 2003) capacity – or 'inverse surveillance' capacity – of those being watched to better understand the tools and techniques of the watchers and inform the design of effective legal and policy responses. **This inversion of surveillance can be used as a tactic to build the knowledge, agency and critical digital literacy of citizens and to inform policy changes that protect and extend digital rights.**

**Disinformation is increasingly common across Africa and a key feature of election campaigns.** Disinformation has long been part of political campaigning, but in the era of traditional mass media a single message was broadcast nationwide. Now, increased use of mobile phones and social media affords the possibility to precisely profile millions of citizens and to micro-target each one with highly tailored disinformation messaging, instantly, repeatedly and at relatively low cost. The country reports on Kenya and South Africa are among those that record the use of voter manipulation and political disinformation (in this collection: Nyabola 2021 and Bosch and Roberts 2021).

The affordances of algorithmic analysis and machine learning make this digital disinformation qualitatively and quantitatively distinct from pre-

 DOI: 10.19088/IDS.2021.005

digital mechanisms. Disinformation is not only used to covertly manipulate citizens' beliefs and voting behaviour, but also to manipulate public opinion on crucial policy issues such as vaccines, climate change, immigration, agriculture and education. The country reports on Sudan and Zimbabwe document disinformation being deployed around the Covid-19 pandemic (in this collection: Mohamed Ali 2021 and Karekwaivanane 2021). The country reports on Cameroon, Kenya and South Africa document the weaponisation of disinformation to enflame ethnic hatred for political gain (in this collection: Ndongmo 2021, Nyabola 2021, and Bosch and Roberts 2021).

Digital disinformation and the use of automated 'computational propaganda' is on the rise in a growing list of countries in Africa (Bradshaw and Howard 2019). There is good reason to expect elections and public policy debates in Africa to continue to be impacted by digital surveillance, profiling and micro-targeting of citizens with disinformation. Disinformation threatens all democracies, but the threat is arguably greatest in fragile democracies: those with weak legal and regulatory oversight, poor institutional protections and where levels of disinformation literacy are lowest. **The clear threat to African democracies, open civic space and digital rights presented by the increasing use of covert disinformation to manipulate citizens' beliefs and behaviour, coupled with significant gaps in our knowledge of the dimensions and dynamics of disinformation in African countries, mean that further research is urgently needed in this area.**

**Internet shutdowns are on the rise in African countries.** The Ugandan government began blocking individual websites as early as 2006 (Nanfuka 2021, this collection). Now, it is increasingly common for governments to shut down the entire internet or mobile phone system. The number of intentional internet shutdowns by governments in Africa rose to 25 in 2020, up from 21 in 2019, with Algeria, Ethiopia and Sudan the worst-affected countries in Africa (Taye 2020). However, digital disruptions short of nationwide blackouts – such as bandwidth throttling and blocking individual applications, locations, or users – are often not captured in this top-level data and require further research attention. The Sudan country report documents the government's blocking, controlling, jamming, and throttling of pro-democracy websites and private accounts (Mohamed Ali 2021, this collection). The Zambia country report documents the government's 2016 blocking of accountability websites such as Zambian Watchdog (Phiri and Zorro 2021, this collection). **Building domestic capacity to monitor and report on internet shutdowns and disruptions would help raise awareness, protect civic space, and defend digital rights.**

**Arrests for online speech feature in nine of the ten country reports.** The right to freedom of speech and freedoms of political opinion, affiliation and association are guaranteed in the Universal Declaration of Human Rights and many other international treaties and conventions to which all ten countries in this study

 DOI: 10.19088/IDS.2021.005

are signatories. However, as nine of the ten country reports show, criticising the president or government policies on social media can get you arrested in countries including Egypt, Ethiopia, and Nigeria (in this collection: Farahat 2021, Gagliardone 2021, and Oladapo and Ojebode 2021). The affordances of digital technologies to track the geolocation of a citizen who the state wants to arrest is becoming increasingly easy, as individuals leave digital traces whenever they use social media, use mobile money or a credit card, pass a facial recognition camera, or use their mobile phone (Privacy International 2020).

**When citizens open civic space online, governments regularly close it down.** A pattern emerges from the country reports of the contestation of civic space between citizens and government online. As citizens incorporate new and different digital tools into their repertoire for opening civic space, some governments develop additional tactics and techniques to counter them and close civic space. Citizens' use of SMS for activism has been followed by bans and mandatory registration; citizen bloggers have been arrested and jailed; social media has been privatised; feminist activists online have been attacked by misogynists; ethnic groups have been targeted; Facebook and Twitter have become sites of surveillance and disinformation; and during protests and elections, governments have intentionally shut down or disrupted online civic space (see Table 4.4).

## Table 4.4 Openings and responses

| Digital opening | Government responses | Example |
|---|---|---|
| SMS activism | Blocking accounts | Uganda, Ethiopia |
| | Banning bulk SMS | Zimbabwe |
| | Mandatory SIM registration | Zimbabwe, Uganda, Zambia, Cameroon, Nigeria |
| Political bloggers | Arresting bloggers | Egypt, Ethiopia, Nigeria, Kenya |
| Platform activism<br>Facebook, Twitter, etc. | Blocking access | Zimbabwe, Zambia, Sudan, Egypt, Nigeria |
| | Price hikes | Zimbabwe, Zambia |
| | Social media tax | Uganda |
| | Arrests for online speech | All countries except South Africa and Kenya |
| | Internet shutdowns | All countries except South Africa and Kenya |
| | Disinformation | Zimbabwe, Sudan, Zambia, South Africa |
| | Coordinating trolls, cyborgs, bots | Zimbabwe, South Africa, Sudan |
| Encrypted apps (Signal) | Blocking Signal app | Egypt |
| | Hacking encrypted messages | Sudan, Uganda, Ethiopia |

*Source:* Authors' own.

 DOI: 10.19088/IDS.2021.005

**Legislation was ranked as highly important in both opening and closing civic space.** A series of laws are highlighted in country reports that enhance digital rights by providing freedom of information, legal protections against spying and surveillance, or entitlements to internet access and use. The 2005 Access to Information Acts in Sudan and Uganda are examples of legislation to enable digital citizenship and extend digital rights (in this collection: Mohamed Ali 2021 and Nanfuka 2021).

Several country report sections draw attention to laws that significantly diminish digital rights by giving new powers to the state to surveil and intercept citizens' private communications or which criminalise political speech. The 2010 Cybersecurity Act in Cameroon specifically limits freedom of speech online (Ndongmo 2021, this collection) and the 2012 National Intelligence Service Act in Kenya gives the state new powers of citizen surveillance (Nyabola 2021, this collection). Similarly, the Zimbabwe country report uses the example of the Interception of Communications Act, which was introduced in 2006 in response to increasing use of digital platforms to criticise the government (Karekwaivanane 2021, this collection).

It is clear from reading the country reports that legislation is a potentially powerful mechanism for extending digital access, enabling digital citizenship, expanding civic space, and enhancing digital rights. This preliminary scoping study has only scraped the surface of this critically important issue. **This is an area that requires focused and in-depth attention to survey existing legal provisions, breaches, and gaps, and to identify where and why legal provisions translate into effective protections that expand civic space and digital rights.**

The ten country reports make a series of recommendations arising from their analysis of the digital rights landscape, as summarised in Table 4.5. Foremost among the recommendations is the urgent need to dramatically expand evidence, awareness, and capacity around the threats to democracy presented by surveillance, disinformation, and internet shutdowns. Other recommendations include extending the provision of fast and affordable internet to excluded groups, to review and improve legal protections, and raise awareness about available digital security tools.

 DOI: 10.19088/IDS.2021.005

# Table 4.5 Recommendations

| | Recommendation | Actors | Countries | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | Further research and research partnerships | Universities and research institutions | ZW | ZM | UG | SD | SA | NG | KE | ET | EG | CM |
| **2** | Capacity-building and strengthening programmes | Civil society | ZW | ZM | UG | | SA | | KE | ET | EG | |
| **3** | Access to fast and affordable internet | Governments | | | UG | SD | SA | | | | EG | CM |
| **4** | Disinformation awareness | Public and journalists | ZW | | | SD | SA | NG | | ET | EG | CM |
| **5** | Anti-surveillance awareness (e.g. VPNs, Tor, Signal) | Public and civil society | ZW | ZM | UG | SD | | | KE | | EG | CM |
| **6** | Strategic litigation to defend digital rights | Lawyers | ZW | | UG | | SA | | | | EG | |
| **7** | Advocacy for domestic digital rights law | Civil society | | | UG | SD | | NG | KE | | EG | |
| **8** | South–South networks and knowledge exchanges | CSOs | | ZM | | SD | | | KE | | | |
| **9** | Local language translation of digital rights materials | Civil society | | | | | SA | | KE | | | |

*Country key:* CM = Cameroon; EG = Egypt; ET = Ethiopia; KE = Kenya; NG = Nigeria; SA = South Africa; SD = Sudan; UG = Uganda; ZM = Zambia; ZW = Zimbabwe

*Source:* Authors' own.

**Building domestic capacity to monitor, analyse and develop solutions to closing civic space is fundamental to improving digital rights.** All the country reports identified gaps in knowledge, public awareness, and civil society capabilities. The reports' authors make a series of recommendations designed to mitigate and overcome the threat to democracy posed by growing digital authoritarianism. Local activists, journalists, researchers, and policymakers lack detailed knowledge of the dimensions of digital surveillance, disinformation, and disruption in their countries. The Zambia country report is one of several to recommend that civil society actors should be equipped with the necessary skills and technologies to enable the systematic monitoring of state and private actors' online disinformation

 DOI: 10.19088/IDS.2021.005

(Phiri and Zorro 2021, this collection). The Zimbabwe country report concludes that there is an urgent need to build domestic technical abilities to monitor, analyse and combat the increased use of surveillance and digital propaganda by pro-government actors (Karekwaivanane 2021, this collection). **Until local actors can accurately detail the dimensions and dynamics of the problem in their own countries, it is impossible for them to define and develop effective countermeasures to restore civic space and digital rights.**

**Digital citizenship, digital affordances and digital inequalities are potentially useful conceptual lenses** for the future study of civic space and digital rights. Analysing the findings from the ten digital rights landscape country reports has made clear the importance of contextual political, civic space, and technological developments to understand the digital rights landscape in a country. New laws and technical innovations need to be part of opening civic space online to expand digital rights. However, approaches that ignore the wider political dynamics and power imbalances will be insufficient and potentially counterproductive. The conceptual framing of digital citizenship has emerged as a potentially useful means to centre citizen agency and rights-claiming as phenomena that need to be expanded, rather than relying more narrowly on techno- or legal-centric perspectives. Throughout this exercise, the concept of affordances has proved to be a valuable lens for understanding and articulating the possibilities for action afforded by specific technologies for opening or closing civic space and digital rights. We acknowledge that to date we have paid insufficient attention to how different social groups experience unequal access to digital technologies and unequal civic space online in ways that constrain the scope of their digital citizenship and ability to exercise digital rights. In future research it will be important to ask, 'Open to whom?' and 'Open by how much?' in order to produce a more nuanced analysis of who is (dis)advantaged when civic space is opened or closed.

 DOI: 10.19088/IDS.2021.005

# 5. Conclusion

The digital rights landscape country reports set out to provide new evidence about the drivers, actors, tools and techniques being used to open and close civic space in ten African countries. We set out to understand more about how digital rights were being shaped by the wider political, civic space and technological landscape. We documented 180 examples that illustrate who is using which digital technologies, in which countries, to either open or close civic space, and with what implications for digital rights.

At the outset, we imagined that our contribution would mainly illustrate the range of creative ways that citizens have responded to closing civic space **offline** by opening civic space **online**. In fact, our contribution is as much about how powerful actors are now **closing** civic space online. We found nearly twice as many examples of the use of digital tactics to close civic space online as we found of the use of digital tactics to open civic space online. A pattern emerged of citizens using digital technologies to open civic space online and exercise their digital rights, and of governments using digital technologies to close civic space online and diminish digital rights.

Although digital technologies are potentially available to anyone, unequal power relationships explain unequal patterns of access and an overall decline in democratic space and digital rights. Some citizens gain access to digital technologies, online civic space, and a degree of digital citizenship. However, governments have access to pervasive digital surveillance, and the ability to deploy disinformation and covertly manipulate citizens' beliefs and behaviour; and they can choose to shut down the internet or imprison citizens for online speech. The country reports also provide examples of civic space being closed by powerful actors **other than governments**, including corporations and dominant gender or ethnic groups, which sometimes also use their power to disrupt democratic dialogue, dominate discourse, and diminish digital rights.

These findings resonate with Kranzberg's first rule that technologies themselves are neither good nor bad, but they are never neutral. Technologies such as social media have affordances that can be used to open civic space, close civic space, or both. How they are used in practice will generally reflect wider political dynamics. Unequal power relationships result in unequal access to technologies; unequal ability to open or close civic space; uneven digital citizenship capabilities and digital rights. The country reports make several key recommendations about how to increase the power of citizens to better exercise, defend and expand their digital rights.

 DOI: 10.19088/IDS.2021.005

All ten country reports identify gaps in existing evidence, awareness, and civil society capacity to independently monitor, analyse, and respond to activities that close civic space and diminish digital rights. A key recommendation overall is for further research by African researchers and activists to increase what is known about the dimensions and distinctive dynamics of emerging tactics in digital surveillance and disinformation.

Until local researchers, journalists, activists, and policymakers can accurately detail the dimensions and dynamics of problems in their own countries, it is impossible for them to define and develop effective countermeasures to restore civic space and digital rights. The necessary research should not be conducted in an ivory tower. An applied multi-actor, interdisciplinary research programme is required to build domestic capacity in each country to effectively monitor, analyse and overcome threats to democratic space and digital rights.

While further research, technical capacity and legal remedies are necessary elements of the solution, they are likely to prove insufficient in isolation from raised public awareness and citizen-led political movement for change. Any such movement requires an active alliance of multiple actors and initiatives. As indicated in section 1, the next steps therefore involve working with:

- **Researchers** – to produce new **evidence** about surveillance actors, tools, tactics and techniques.
- **Journalists** – to raise **public awareness** about the practices and consequences of surveillance.
- **Policymakers** – to map existing **legislation**, identify gaps and advance a public policy agenda.
- **Activists** – to expand **civic engagement** to tackle surveillance, disinformation and shutdowns.

 DOI: 10.19088/IDS.2021.005

# References

Abraham, K. (2014) 'Sex, Respect and Freedom from Shame: Zambian Women Create Space for Social Change Through Social Networking', in I. Buskens and A. Webb (eds), *Women and ICT in Africa and the Middle East*, London: Zed Books

ACT Alliance and CIDSE (2015) ***Space for Civil Society: How to Protect and Expand an Enabling Environment***, Switzerland and Brussels: Act Alliance and CIDSE (accessed 26 January 2021)

African Declaration (2019) ***African Declaration on Internet Rights and Freedoms*** (accessed 26 January 2021)

APC (2018) ***Annual Report 2018***, Manila: Association for Progressive Communications (accessed 26 January 2021)

APC (2006) ***APC Internet Rights Charter***, South Africa: Association for Progressive Communications (accessed 26 January 2021)

Assefa, A. and Zewde, B. (2008) *Civil Society at the Crossroads: Challenges and Prospects in Ethiopia*, Addis Ababa: Forum for Social Studies

Baker, M. and Blaagaard, B. (2016) *Citizen Media and Public Spaces*, London: Routledge

Benjamin, R. (2019) *Race After Technology: Abolitionist Tools for the New Jim Code*, New York: Polity Press

Bennett, W. and Segerberg, A. (2013) *The Logic of Connective Action*, Cambridge: Cambridge University Press

Bertsou, E. (2019) 'Rethinking Political Distrust', *European Political Science Review* 11.2: 213–30

Bosch, T. (2019) 'Social Media and Protest Movements in South Africa: #FeesMustFall and #ZumaMustFall', in M. Dwyer and T. Molony (eds), *Social Media and Politics in Africa*, London: Zed Books

Boyd, D. (2010) 'Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications', in Z. Papacharissi (ed.), *Networked Self: Identity, Community, and Culture*, Oxon and New York: Routledge

Bradshaw, S. and Howard, P. (2019) ***The Global Disinformation Order 2019: Global Inventory of Organised Social Media Manipulation***, Working Paper 2019.3, Oxford: Project on Computational Propaganda, University of Oxford (accessed 26 January 2021)

Bradshaw, S. and Howard, P. (2017) ***Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation***, Working Paper 2017.12, Oxford: Project on Computational Propaganda, University of Oxford (accessed 26 January 2021)

Brown, E. (2019) **'Online Fake News is Costing Us $78 billion Globally Each Year'**, ZDNet, 18 December (accessed 26 January 2021)

Buskens, I. and Webb, A. (eds) (2014) *Women and ICT in Africa and the Middle East*, London: Zed Books

Buskens, I. and Webb, A. (eds) (2009) *African Women and ICTs*, London: Zed Books

Buyse, A. (2018) 'Squeezing Civic Space: Restrictions on Civil Society Organizations and the Linkages with Human Rights', *International Journal of Human Rights* 22.8: 966–88

CIPESA (2019a) ***2019 State of Internet Freedom in Africa Report Launched: African Countries are Broadening Control Over the Internet***, Kampala: Collaboration on International ICT Policy in East and Southern Africa (accessed 26 January 2021)

CIPESA (2019b) ***The Shrinking Civic Space in East Africa***, Kampala: Collaboration on International ICT Policy in East and Southern Africa (accessed 26 January 2021)

CIPESA (2016) ***Analysis of Twitter During the 2016 Presidential Debates***, Kampala: Collaboration on International ICT Policy in East and Southern Africa (accessed 26 January 2021)

CIVICUS (2020) ***People Power Under Attack 2020***, Johannesburg: CIVICUS (accessed 26 January 2021)

CIVICUS (2019) ***State of Civil Society Report 2019***, Johannesburg: CIVICUS (accessed 26 January 2021)

 DOI: 10.19088/IDS.2021.005

Dahir, A. (2018) **'In a Continent Dominated by WhatsApp, Ethiopia Prefers Telegram'**, *Quartz*, 24 February (accessed 20 October 2019)

Dupuy, K.; Ron, J. and Prakash, A. (2016) 'Hands Off My Regime! Governments' Restrictions on Foreign Aid to Non-Governmental Organizations in Poor and Middle-Income Countries', *World Development* 84: 299–311 (accessed 10 February 2021)

Dupuy, K.; Ron, J. and Prakash, A. (2014) '**Who Survived? Ethiopia's Regulatory Crackdown on Foreign-Funded NGOs**', *Review of International Political Economy* 22.2: 419–59, DOI: 10.1080/09692290.2014.903854 (accessed 10 February 2021)

Egbunike, N. (2019) 'Social Media Propelled Ethnocentric Disinformation and Propaganda During the Nigerian Elections', *Global Voices*, 6 November

Egbunike, N. (2018) '**Hashtags: Social Media, Politics and Ethnicity in Nigeria**', *Literary Everything*, 12 November (accessed 26 January 2021)

EISA (2020) ***2021 African Election Calendar,*** Electoral Institute for Sustainable Democracy in Africa (accessed 26 January 2021)

Ekine, S. (ed.) (2010) *SMS Uprising: Mobile Activism in Africa*, Cape Town: Pambazuka Press

Eubanks, V. (2017) *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor*, New York: St Martin's Press

Faith, B. and Fraser, E. (2018) *Digital Harassment of Women Leaders: A Review of the Evidence*, VAWG Helpdesk Research Report 209, UK: Department for International Development

Feenberg, A. (1992) '**Subversive Rationalization: Technology, Power, and Democracy**', *Inquiry: An Interdisciplinary Journal of Philosophy* 35: 3–4: 301–22 (accessed 10 February 2021)

Feldstein, S. (2019) ***The Global Expansion of AI Surveillance***, Carnegie Endowment for International Peace (accessed 26 January 2021)

Figari, A.; Diehm, C. and Lawrence, R. (2019) ***Shrinking Civil Space: A Digital Perspective***, Berlin: Tactical Tech (accessed 26 January 2021)

Fraser, A. (2017) '**We Go Inside the Guptabot Fake News Network**', *Tech Central*, 4 September (accessed 26 January 2021)

Freedom House (2020) ***A Leaderless Struggle for Democracy*** (accessed 26 January 2021)

Freedom House (2019) ***The Spread of Anti-NGO Measures in Africa: Freedoms Under Threat*** (accessed 26 January 2021)

Freedom House (2018) ***The Rise of Digital Authoritarianism*** (accessed 26 January 2021)

Freyburg, T. and Garbe, L. (2018) '**Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa**', *International Journal of Communication* 12: 3896–3916 (accessed 26 January 2021)

Gagliardone, I. (2016) *The Politics of Technology in Africa: Communication, Development, and Nation-Building in Ethiopia*, Cambridge: Cambridge University Press

Gagliardone, I. (2014) 'New Media and the Developmental State in Ethiopia', *African Affairs* 113.451: 279–99

Ganesh, M.I. and Gutermuth, L. (2014) ***Case Study: Women's Rights Campaigning: Info-Activism Toolkit***, Tactical Technology Collective (accessed 26 January 2021)

Ganesh, M.I.; Deutch, J. and Schulte, J. (2016) ***Privacy, Anonymity, Visibility: Dilemmas in Tech Use by Marginalised Communities***, Brighton: Institute of Development Studies (accessed 26 January 2021)

Gaventa, J. (2005) *Reflections on the Uses of the Power Cube Approach for Analysing Spaces, Places and Dynamics of Civil Society Participation and Engagement*, CPF Evaluation Series 4: Mfp Breed Netwerk

Gibson, J. (1977) 'The Theory of Affordances', in R. Shaw and J. Bransford (eds), *Perceiving, Acting, and Knowing: Toward and Ecological Psychology*, London: Oxford University Press

GISWatch (2019) *Artificial Intelligence: Human Rights, Social Justice and Development*, Association for Progressive Communications

 DOI: 10.19088/IDS.2021.005

GISWatch (2014) ***Communications Surveillance in the Digital Age***, Association for Progressive Communications and Hivos (accessed 26 January 2021)

Global Witness (2016) ***On Dangerous Ground***, London: Global Witness (accessed 26 January 2021)

Greene, T. (2019) '**How a Ban on Political Ads is the Second Best Gift Twitter Ever Gave Trump**', TNW, 7 November (accessed 26 January 2021)

GSMA (2020) **The Mobile Gender Gap Report 2020**, London: GSMA (accessed 26 January 2021)

Gurumurthy, A.; Bharthur, D. and Chami, N. (2017) ***Voice or Chatter? Making ICTs Work for Transformative Engagement: Research Report Summary***, Brighton: Institute of Development Studies (accessed 26 January 2021)

Hafkin, N. (2012) 'Gender', in G. Sadowski (ed.), *Accelerating Development Using the Web: Empowering Poor and Marginalized Populations*, London: WebFoundation

Hernandez, K. and Roberts, T. (2018) ***Leaving No One Behind in a Digital World***, K4D Emerging Issues Report 10, Brighton: Institute of Development Studies (accessed 26 January 2021)

Hintz, A.; Dencik, L. and Wahl-Jorgensen, K. (2019) *Digital Citizenship in a Datafied Society*, Cambridge: Polity Press

Hossain, N.; Khurana, N.; Mohmand, S.; Nazneen, S.; Oosterom, M.; Roberts, T. *et al.* (2018) ***What Does Closing Civic Space Mean for Development?*** IDS Working Paper 515, Brighton: Institute of Development Studies (accessed 26 January 2021)

Hossain, N.; Khurana, N.; Nazneen, S.; Oosterom, M.; Schröder, P. and Shankland, A. (2019) *Development Needs Civil Society – The Implications of Civic Space for the SDGs*, Geneva: Act Alliance

Hossain, N.; Khurana, N.; Oosterom, M.; Roberts, T.; Santos, R. and Shankland, A. (2017) 'The Implications of Closing Civic Space for Development', report for DFID, unpublished

Howard, P. (2020) *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*, New Haven CT: Yale University Press

Ibrahim, K. (2020) *Monitored and Targeted: Sale of Surveillance Technology Puts Lives of MENA Activists at Risk*, IFEX

ICNL (2016) '**Survey of Trends Affecting Civic Space: 2015–16**', *Global Trends in NGO Law: A Quarterly Review of NGO Legal Trends around the World* 7.4 (accessed 10 February 2021)

Isin, E. and Ruppert, E. (2015) *Being Digital Citizens*, London: Rowman and Littlefield

Jones, K. (2019) ***Online Disinformation and Political Discourse: Applying a Human Rights Framework***, Research Paper, London: Chatham House, Royal Institute of International Affairs (accessed 10 February 2021)

Jorgensen, R. (2006) *Human Rights in the Global Information Society*, Cambridge MA: MIT Press

Karekwaivanane, G. (2019a) ' "Tapanduka Zvamuchese": Facebook, "Unruly Publics", and Zimbabwean Politics', *Journal of East African Studies* 13.1: 54–71

Karekwaivanane, G. (2019b) 'We Are Not Just Voters, We Are Citizens: Social Media, the #Thisflag Campaign and Insurgent Citizenship in Zimbabwe', in M. Dwyer and T. Molony (eds), *Social Media and Politics in Africa*, London: Zed Books

Khanna, A.; Mani, P.; Patterson, Z.; Pantazidou, M. and Shqera, M. (2013) ***The Changing Faces of Citizen Action: A Mapping Study through an 'Unruly' Lens***, IDS Working Paper 423, Brighton: Institute of Development Studies (accessed 26 January 2021)

Kode, D. (2018) '**Civic Space Restrictions in Africa: How Does Civil Society Respond?**', Conflict Trends 2018.1: 10–17 (accessed 26 January 2021)

Kranzberg, M. (1986) '**Technology and History: "Kranzberg's Laws"**', *Technology and Culture* 27.3: 544–60 (accessed 26 January 2021)

MacKensie, D. and Wajcman, J. (eds) (1985) *The Social Shaping of Technology*, Buckingham: Open University Press

Mann, S.; Nolan, J. and Wellman, B. (2003) 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments', *Surveillance and Society* 1.3: 331–55

 DOI: 10.19088/IDS.2021.005

Marczak, B.; Scott-Railton, J.; Rao, S.; Anstis, S. and Deibert, R. (2020) ***Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles***, The Citizen Lab (accessed 26 January 2021)

McGee, R.; Edwards, D.; Anderson, C.; Hudson, H. and Feruglio, F. (2018) ***Appropriating Technology for Accountability: Messages from Making All Voices Count***, Making All Voices Count, Research Report, Brighton: Institute of Development Studies (accessed 26 January 2021)

Michelson, E. (2006) '**Clicking Toward Development: Understanding the Role of ICTs for Civil Society**', *Journal of Technology Studies* 32.1: 53–63 (accessed 26 January 2021)

Moolman, J.; Primo, N. and Shackleton, S-J. (2011) '**Introduction: Taking a Byte of Technology: Women and ICTs**', *Agenda: Empowering Women for Gender Equity* 21.1: 4–14 (accessed 26 January 2021)

Mudhai, O.; Tettey, W. and Banda, F. (2009) *African Media and the Digital Public Sphere*, Hampshire: Palgrave MacMillan

Nanfuka, J. (2019) '**Social Media Tax Cuts Ugandan Internet Users by Five Million, Penetration Down From 47% to 35%**', 31 January, Kampala: Collaboration on International ICT Policy for East and Southern Africa (accessed 26 January 2021)

Noble, S. (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York: New York University Press

Norman, D. (1988) *The Design of Everyday Things*, New York: Basic Books

Nyabola, N. (2018) *Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya (African Arguments)*, London: Zed Books

Nyamnjoh, F. (2016) *#RhodesMustFall: Nibbling at Resilient Colonialism in South Africa*, Bamenda: Langaa RPCIG

O'Neil, C. (2016) *Weapons of Math Destruction*, London: Penguin Random House

OECD (2018) '**Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact**,' *OECD Digital Government Studies*, Paris: Organisation for Economic Co-operation and Development (accessed 26 January 2021)

OHCHR (2020) ***OHCHR and Equal Participation in Political and Public Affairs***, Office of the High Commissioner for Human Rights (accessed 26 January 2021)

Ojebode, A. and Oladapo, W. (2018) '***Using Social Media for Long-Haul Activism: Lessons from the BBOG Movement in Nigeria***', Briefing, Partnership for African Social Governance Research (accessed 26 January 2021)

Okolloh, O. (2009) 'Ushahidi or Testimony: Web 2.0 Tools for Crowdsourcing Crisis Information', *PLA Notes* 59: 65–70

Oosterom, M. (2019) '**The Implications of Closing Civic Space for Sustainable Development in Zimbabwe**', mimeo, IDS and ACT Alliance (accessed 26 January 2021)

PartnersGlobal; Roig, J.; Gomez Chow, L.; Barringer, D. and Vasquez-Yetter, R. (2017) ***The Importance of Ensuring an Enabling Environment for Civil Society as It Relates to the Sustainable Development Goals***, Report to the Working Group on Enabling and Protecting Civil Society of the Community of Democracies, Washington DC: Community of Democracies (accessed 26 January 2021)

Peuchaud, S. (2014) 'Social Media Activism and Egyptians' Use of Social Media to Combat Sexual Violence', *Health Promotion International* 29.suppl 1: i113–i120

Pinch, T. and Bijker, W. (1984) '**The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other**', *Social Studies of Science* 14.3: 399–441 (accessed 26 January 2021)

Privacy International (2019) '**Africa: SIM Card Registration Only Increases Monitoring and Exclusion**', *Privacy International*, 5 August (accessed 26 January 2021)

Roberts, T. (2019) ***Closing Civic Space and Inclusive Development in Ethiopia***, IDS Working Paper 527, Brighton: Institute of Development Studies (accessed 26 January 2021)

Roberts, T. and Hernandez, K. (2019) '**Digital Access is not Binary: The 5 'A's of Technology Access in the Philippines**', *Electronic Journal of Information Systems in Developing Countries* 85.4 (accessed 26 January 2021)

Roberts, T. and Marchais, G. (2018) ***Assessing the Role of Social Media and Digital Technology in Violence Reporting***, IDS Working Paper 492, Brighton: Institute of Development Studies (accessed 26 January 2021)

Sadowski, J. (2020) ***Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over the World***, Cambridge MA: MIT Press (accessed 26 January 2021)

Solomon, S. (2018) '**Cambridge Analytica Played Roles in Multiple African Elections**', *VOA News*, 22 March (accessed 26 January 2021)

Statista (2020) '**Number of Affected Users and Economic Cost of Internet Shutdowns Worldwide 2019**,' Statista, 25 January (accessed 26 January 2021)

Taye, B. (2020) ***Targeted, Cut Off and Left in the Dark: The #KeepItOn Report on Internet Shutdowns in 2019***, Access Now (accessed 26 January 2021)

Taye, B. (2018) ***The State of Internet Shutdowns Around the World: The 2018 #KeepItOn Report***, Access Now (accessed 26 January 2021)

THRDC (2016) ***Annual Report 2016***, Arusha: Tanzania Human Rights Defenders Coalition (accessed 26 January 2021)

Tufekci, Z. (2017) *Twitter and Tear Gas*, New Haven CT: Yale University Press

UN (2015) *Transforming Our World: The 2030 Agenda for Sustainable Development*, A/RES/70/1, New York: United Nations

UN (2013) ***A New Global Partnership: Eradicate Poverty and Transform Economies Through Sustainable Development: The Report of the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda***, New York: United Nations (accessed 26 January 2021)

UN (1948) ***Universal Declaration of Human Rights***, New York: United Nations (accessed 26 January 2021)

UNDP (2015) *The 2030 Agenda for Sustainable Development*, New York: United Nations Development Programme

UNHRC (2018) ***Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet***, Geneva: United Nations Human Rights Council (accessed 26 January 2021)

UNHRC (2011) ***Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression***, New York: United Nations Human Rights Council (accessed 26 January 2021)

Vlahakis, M. (2018) *Breaking the Silence: Ending Online Violence and Abuse Against Women's Rights Activists*, London: Womankind Worldwide

We Are Social (2019) *Digital 2019: Global Digital Overview*, Hootsuite

Woolley, S. and Howard, P. (2019) *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, Oxford: Oxford University Press

Woolley, S. and Howard, P. (2017) *Computational Propaganda*, Working Paper 2017.11, Oxford Internet Institute: Project on Computational Propaganda

World Bank (2016) ***World Development Report 2016: Digital Dividends***, Washington DC: World Bank (accessed 26 January 2021)

WSIS (2018) ***Leveraging ICTs to Build Information and Knowledge Societies for Achieving the Sustainable Development Goals (SDGs)***, World Summit on the Information Society (WSIS) Forum 2018 Outcome Document, Geneva: International Telecommunication Union (accessed 26 January 2021)

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London: Profile Books

 DOI: 10.19088/IDS.2021.005

# Zimbabwe Digital Rights Landscape Report

George Karekwaivanane and Natasha Msonza



This report is part of 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries'; the Introduction is also recommended reading.

©2021 George Karekwaivanane & Natasha Msonza ©Institute of Development Studies. DOI: 10.19088/IDS.2021.006

# 1. Introduction

Over the past two decades there has been a rapid adoption of mobile and internet technologies in Zimbabwe. This has empowered citizens but also expanded the repressive capacity of the state. This double-edged impact of technology on civic space and digital rights can only be fully understood in the context of the country's protracted political crisis and authoritarian state.

We begin by discussing the political developments in the country since the late 1990s that have provided the backdrop for the adoption and use of digital technology in the country. This is followed in section 3 by a discussion of the alternating openings and closings of civic space that emerged out of political contests. Section 4 examines the ways that digital media has been employed by citizens and the state in the prosecution of different sociopolitical agendas. Section 5 assesses the digital landscape in the country and offers recommendations for ways that the digital rights regime can be strengthened. In section 6 we offer some reflections on the impact of the Covid-19 pandemic on digital rights. Finally, we end with some concluding observations.

 DOI: 10.19088/IDS.2021.006

# 2. Political landscape

Since the early 2000s, Zimbabwe's politics has been characterised by an unresolved contest. On one side is the Zimbabwe African National Union–Patriotic Front (ZANU–PF), a liberation party that has been in power since independence in 1980, but which has proven unable to reform itself or the country, and is willing to violate the spirit and the letter of the law to hold on to power. On the other is the Movement for Democratic Change (MDC). The opposition party has managed to attract significant popular support, but has failed to mobilise citizens beyond its urban strongholds; and is unable to maintain sufficient unity within its ranks and to consistently act strategically. In the face of this unresolved battle, the country has found itself unable to break out of a socioeconomic crisis in which it has been trapped for the better part of two decades.

Antonio Gramsci (1971)'s concept of the 'interregnum' is a useful prism through which to understand Zimbabwe's political circumstances. 'The crisis', Gramsci argues, 'consists precisely in the fact that the old is dying and the new cannot be born; in this interregnum a great variety of morbid symptoms appear' (*ibid.*: 276). However, it would be incorrect to suggest that the past 20 years have been marked by an inexorable descent into an ever-deepening crisis. Instead, there has been an alternation between periods of opening and closing of civic space. However, it is arguably true that there has been a progressive drift away from open, inclusive democratic practices.

Between 2000 and 2008, ZANU–PF passed a series of repressive laws, interfered with the workings of the judiciary, manipulated elections and used violence and intimidation against opposition supporters and officials (Karekwaivanane 2017). It also deployed a discourse of exclusion, which divided society into 'patriots' who supported it and 'sell-outs' who supported the MDC (Tendi 2020: 53, 57). The ever-broadening category of sell-outs came to include civil society, private media and other organisations that sought to hold the government to account. Crucially, by discursively constructing these groups and individuals as sell-outs or traitors ZANU–PF rendered them legitimate objects of violence.

The political deadlock led to a deepening social and economic crisis marked by record-breaking inflation and a massive exodus of Zimbabweans into the diaspora. The crisis ultimately led to mediation efforts by the Southern African Development Community (SADC). Matters came to a head in mid-2008 when President Robert Mugabe mounted a violent campaign in the lead-up to the June run-off election, compelling the MDC's Morgan Tsvangirai to pull out of

 DOI: 10.19088/IDS.2021.006

the election. Although Mugabe declared himself the winner, he was faced with an acute crisis of legitimacy at home and abroad. He was thus forced to agree to a Government of National Unity (GNU) with the opposition.

The five-year term of the GNU (2009–13) was a period of relative political opening, designed to allow for the implementation of reforms and drafting of a new constitution, as detailed in the Global Political Agreement (Raftopoulos 2013). However, few political reforms were fully implemented. The signature achievement of the GNU was the adoption of a new constitution in 2013. However, since 'winning' the 2013 presidential and parliamentary elections ZANU–PF has been reluctant to bring the repressive laws on the statute book into line with the new Constitution. The thinking that informed ZANU–PF inertia is summed up in the statement by the then cabinet minister Prof. Jonathan Moyo that 'Zanu PF will never reform itself out of power' (Tshili 2016).

When ZANU–PF returned to sole power following the 2013 election, there was a significant loss in investor confidence. Much of the social and economic progress made under the GNU was reversed and Mugabe was drawn into bitter infighting within his party. In November 2017, Mugabe was deposed in a military coup and died in hospital less than two years later. The protagonists of the coup were anxious to mark a break with the past and styled their government 'the new dispensation' or 'the second republic'. However, as we show in the next section the repressive political strategies of the administrations of Mugabe and his successor Emmerson Mnangagwa have been very similar.

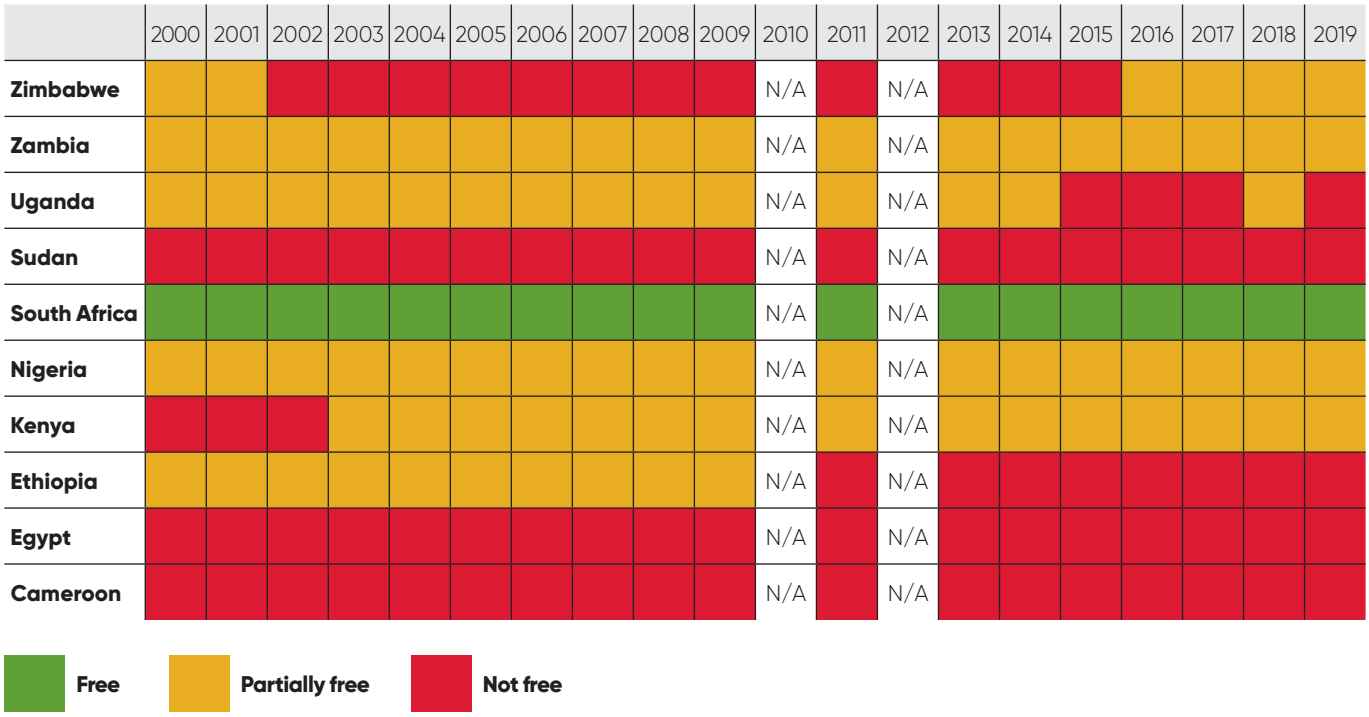
 DOI: 10.19088/IDS.2021.006

# 3. Civic space landscape

The political developments described in section 2 had important implications for the opening and closing of civic space in the country. It is arguably true that the more ZANU–PF has felt politically threatened, the more severe the attacks it has made on civic space. The period between 2000 and 2020 thus witnessed prolonged periods of rapidly shrinking civic space punctuated by windows of expanding civic space. Nevertheless, the predominant trend has been towards shrinking civic space.

Unsurprisingly, the key political indicators for the period show only very slight improvements between 2000 and 2019, if at all. For example, Zimbabwe's 2019 freedom ranking of 'partly free' was a return to the 2000 level after a prolonged period in the 'not free' ranking (see Figure 3.1). Recent political developments indicate that these very modest gains are not guaranteed to be permanent and that the trend might be moving in the opposite direction.

## Figure 3.1 Freedom House ranking for ADRN countries, 2000–19[1]




*Note:* ADRN – African Digital Rights Network.

*Source:* Adapted from Freedom House (2019)

1 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.006

The 1987 Unity Accord in effect removed any political threat to ZANU–PF from rival political parties.[2] This absence of serious political threats partly explains why the ruling party allowed an expansion of civic space throughout the 1990s. This period witnessed the emergence or growth of several organisations that went on to play an important role in civil society. These included the Zimbabwe Human Rights Association, Zimbabwe Lawyers for Human Rights (ZLHR), the National Constitutional Assembly and the Zimbabwe Human Rights NGO Forum (Masunungure 2014: 10).

The period 2000–08 was marked by a drastic closing of civic space as ZANU–PF sought to fend off the political challenge posed by the MDC. The security agencies, war veterans, and youth militia were used to intimidate, assault and, in some instances, kill the ruling party's political opponents (Karekwaivanane 2017: 220). The law was also used to criminalise political dissent. A lot of the violence and intimidation centred on the elections that were held in 2000, 2002, 2005 and 2008.

Civil society organisations (CSOs) made significant efforts to challenge the government's repression. The earlier generation of CSOs were joined by a host of new ones such as Zimbabwe Peace Project, Zimbabwe Electoral Support Network, the Crisis in Zimbabwe Coalition and Women of Zimbabwe Arise (Masunungure 2014: 10). The excessive nature of the violence ultimately backfired as it undermined the legitimacy of Mugabe's government and forced SADC to intervene. It was this intervention that led to the establishment in 2008 of the power-sharing GNU.

Between 2008 and 2013 the power-sharing arrangement resulted in a significant expansion of civic space. The countrywide constitutional consultation process, flawed as it was, helped to create the space for wide-ranging grassroots-level political debate (Sachikonye 2013). The process resulted in a progressive constitution with a justiciable bill of rights, although few concrete steps were taken to implement transitional justice measures.

The GNU came to an abrupt end in 2013 when a hastily organised election returned ZANU–PF to power with a two-thirds majority in Parliament. With ZANU–PF in full control of the state, the years leading up to 2017 saw a progressive weakening in the capacity of civil society and opposition political organisations. The weakness in these institutions led to a proliferation of citizen-led protests. The Occupy Africa Unity Square campaign began in 2014 and the #ThisFlag, #Tajamuka, #BeatThePot and #ThisGown campaigns of 2016 followed in quick succession (Karekwaivanane and Mare 2019). What is significant about this period was the growing use of social

2 The 1987 Unity Accord led to a merger between ZANU-PF and the main opposition party, Zimbabwe African People's Union (PF–ZAPU). The accord ended the government-directed violence against PF–ZAPU members and leaders.

 DOI: 10.19088/IDS.2021.006

media by citizens to mobilise and coordinate social and political action. However, these campaigns were frequently met with firm state repression that was reminiscent of the period between 2000 and 2008.

Ironically, the military coup of 2017 ushered in a short period of widening civic space between the November 2017 coup and the July 2018 elections. The new dispensation allowed a measure of freedom of association and expression in order to convince potential investors that they were reform minded. However, this superficial commitment to greater freedoms was already fraying in the weeks leading up to the July 2018 elections.

Amidst heightened anxiety and suspicion over vote counting and announcement of the election results, the government ordered the army on to the streets of the capital Harare to suppress growing protests. The crackdown left six civilians dead and dozens more seriously injured (Motlanthe Commission of Inquiry 2018). Fuel price protests in January 2019 were met with another military crackdown, during which more citizens were killed, and an internet shutdown was imposed (Amnesty International 2019). Abductions of prominent voices of dissent such as journalists, union leaders, comedians and opposition officials became more commonplace (OHCHR 2020). This trend of closing civic space continued in 2020.

## Table 3.1 Civic space timeline

| Year | Shift | Implication |
|---|---|---|
| **1997–99** | Emergence of a civil society coalition under the National Constitutional Assembly. | Opening of civic space and formation of the Movement for Democratic Change (MDC). |
| **2000–08** | All-out effort by the Zimbabwe African National Union-Patriotic Front (ZANU–PF) to hold on to power. | Rapidly shrinking civic space and targeting of civil society and opposition activists. |
| **2008–13** | Government of National Unity. | Expansion of civic space and adoption of new Constitution. |
| **2013–late-2017** | ZANU–PF's shock defeat of opposition MDC. | Renewed shrinking of civic space and repression of citizen-led protest campaigns. |
| **November 2017–July 2018** | Following a military coup, a new government led by Emmerson Mnangagwa takes office. | Broadening civic space and increased freedom of speech, assembly and association. |
| **August 2018–present** | Post-election killings usher in a return to overt repression. | Closing of civic space, and carrot-and-stick approach towards opposition politicians, civil society activists and unionists. |

*Source:* Authors' own.

 DOI: 10.19088/IDS.2021.006

# 4. Technology landscape

Over the past 20 years, there has been a significant expansion in the uptake of the internet and mobile phones in Zimbabwe. Between 2000 and 2019 the mobile penetration rate rose from 2.3 per cent to 90.6 per cent of the total population (POTRAZ 2019). From 2009 to 2019 the internet penetration level rose from 5.1 per cent to 60.6 per cent of the total population (*ibid.*). However, the high cost of data means that subscribers often cannot afford regular access to the internet. In addition, there remains a significant disparity in internet access among citizens. Increased internet and mobile penetration has been accompanied by a rise in the use of social media platforms such as WhatsApp, Facebook and Twitter. WhatsApp is the most widely used, followed by Facebook, which was estimated to have 994,000 subscribers in Zimbabwe at the end of 2019 (Internet World Stats 2020).

Due to its widespread availability, digital technology has played an important role in the opening and closing of civic space. On the one hand, citizens have used digital technologies in increasingly innovative ways to expand and take full advantage of civic space. On the other, the government has employed digital technologies to control and conduct surveillance on its citizens. In this section we highlight the main steps taken by the government and citizens, respectively.

The legal basis for repressing digital rights in Zimbabwe rests on laws such as the 2003 Access to Information and Protection of Privacy Act (AIPPA). AIPPA has been used by the government to inhibit media freedom (Article 19 and MISA-Zimbabwe 2004). The Interception of Communications Act (ICA) of 2007 was introduced at a time when Zimbabweans were increasingly using digital platforms to criticise the government. The legislation empowered the government to set up the Interception of Communications Monitoring Centre, which enabled it to place its critics under intrusive surveillance in the name of national security (The President and the Parliament of Zimbabwe 2007). Section 9 of the act requires telecommunications service providers to provide the state with 'real time and full time monitoring facilities for the interception of communications' and failure to comply is punishable by a fine or a jail term of up to three years (*ibid:* 7).

During the 2013 election campaign, the government banned the use of bulk SMS (text messaging) (Batambuze III 2013) on the grounds that it was trying to ensure that telecommunications operators respected 'the constitutional right of customers to personal privacy' and to protect customers from 'unsolicited Bulk SMS' (POTRAZ 2013). However, bulk SMS messages were a powerful means for activists and non-governmental organisations in Zimbabwe to reach wide audiences with civic education information. The

 DOI: 10.19088/IDS.2021.006

ban thus curtailed access to information, especially for those who could not afford smartphones and mobile data.

In 2013, the government claimed that the introduction of mandatory SIM card registration was in line with the global trend and was intended to 'safeguard national security' and control crime (POTRAZ 2013). However, it effectively expanded state surveillance capabilities while reducing citizens' privacy and freedoms.

This capability has on occasion been used to instil fear in citizens. For example, on the day of the July 2016 stay-away co-ordinated by the #ThisFlag campaign,[3] the government, through the Post and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), issued a veiled threat through a public notice in the press (Gambanga 2016). The notice stipulated that people who were sharing 'abusive and subversive materials' would be 'disconnected… arrested and dealt with accordingly in the national interest'. The public notice further warned that: 'All SIM cards in Zimbabwe are registered in the name of the user. Perpetrators can easily be identified' (*ibid.*).

The government has also used pricing of data to close down online opposition. On 4 August 2016, during a period of sustained online campaigning and a nationwide stay-away campaign, the government increased the cost of mobile data by 500 per cent (Htxt 2016; Muzulu 2017). This timing stoked speculation that the price hikes were a deliberate move by the government to quash social activism and online organising. Public uproar at the price rises led to a policy reversal five days later, but the tactic was deployed again in 2017; this time prices were hiked by 2,500 per cent in January (Muzulu 2017). Many Zimbabweans were temporarily forced to go offline and forfeit their freedom of expression, demonstrating the increasing centrality of mobile data access to digital rights.

Price hikes were not the only tactic in President Mugabe's arsenal for closing civic space. In 2015, he received a 'gift' of monitoring and surveillance technology from Iran including international mobile subscriber identity (IMSI) catchers that make it possible to intercept mobile phone traffic, as well as track the location data of mobile phone users (Bulawayo24 2015). This gave the government new capabilities to target government critics or perceived enemies of the state. A study by cybersecurity researchers used an IMSI catcher sniffer app to detect IMSI catchers 'on the cell phone towers of the government-owned cell phone provider NetOne' (Gwagwa and Hove n.d.). According to media reports about the alleged bugging of the mobile phones of opposition officials, the government is using such technology to conduct surveillance on Zimbabwean citizens (Ndlela 2020).

3 A stay-away is a form of protest in which citizens stay away from their places of work for a set period of time. The goal is to bring the economy to a standstill while avoiding violent confrontations with the authorities.

 DOI: 10.19088/IDS.2021.006

In addition to installing IMSI catchers, the government has also extended its surveillance capabilities through the installation of a large-scale facial recognition programme, as part of a 2018 'strategic' public-private partnership backed by the Chinese Belt and Road Initiative (Quartz Africa 2018). This partnership is an example of the way that the Chinese information control model is being diffused via the digital silk road (Weber 2019). For its part, the government intends to use the facial recognition system for law enforcement purposes. Cloudwalk Technology, the Chinese company providing the facial recognition equipment, will receive a stock of photographs that will be used to 'train the racial bias out of its facial recognition systems' (Quartz Africa 2018).

In addition, data collected by researchers at the Carnegie Endowment for International Peace show that artificial intelligence surveillance technology from two other Chinese firms, Huawei and Hikvision, is currently being used in Zimbabwe (Feldstein 2019). This has stoked fears that the adoption of this technology signals a broader adoption of China's information control model, and that the facial recognition programme may represent a step towards the pervasive and panoptic surveillance measures used in Chinese cities (Weber 2019).

This progressive increase in state surveillance capabilities may be linked to a rise in arrests of individuals for their online activities. Since July 2014, ZLHR has assisted at least 200 people who have been arrested for posts that they have made on social media sites (CIPESA 2020). These include former editor of the state-owned *Sunday Mail* newspaper Edmund Kudzayi (Laiton 2014) and prominent journalist Hopewell Chin'ono, who was arrested in a round-up of government critics ahead of the anti-corruption protests planned for 31 July 2020 (New Zimbabwe 2020). These arrests have had a chilling effect on citizens, causing government critics to use pseudonyms to engage in online discussions of politics, or self-censor to avoid arrest (Mokwetsi 2014).

Social media has become an important space partly due to aggressive policing of street protests. The opening of online civic space is a response to the repressive closing of physical civic space – the two are intimately connected. The opening of online civic space has produced a number of influential hashtag campaigns in Zimbabwe that have produced street demonstrations. The #ThisFlag campaign of 2016 was triggered by a social media video in which Pastor Evan Mawarire bemoaned the protracted socioeconomic and political crises confronting the country (Karekwaivanane and Mare 2019). Unemployed university graduates took advantage of the momentum by initiating the #ThisGown campaign. #ShutDownZimbabwe also started through online cyber-activism, but culminated in nationwide street protests in January 2019, which turned violent and led to the destruction of property and loss of lives.

 DOI: 10.19088/IDS.2021.006

Ahead of elections in July 2018, the president issued a 'call to arms'[4] to his supporters to '*rakasha*' (thrash) his opponents online. This led to an upsurge in new social media accounts amplifying ruling party propaganda and derailing critical political conversations. This has been described locally as the '*Varakashi*' phenomenon,[5] which has played out as online mobs of individual trolls and 'sock puppet' accounts who actively close online civic space by harassing opposition voices and coordinating disinformation campaigns.

The *Varakashi* illustrate the regime's shift to appropriating the same technology tools and platforms used by its opponents. Our research has shown that during the 2018 election season, pro-government trolls succeeded in intimidating opposition voices and shutting down civic space. Activists became aware that everything political that they posted was being closely monitored, sometimes culminating in threats of violence in their offline lives. Varakashi continued to play a role in Zimbabwe's politically polarised landscape in 2020, aggressively targeting opposition party members and activists who try to speak out about ongoing human rights violations.

At the time of writing, the most recent influential hashtag campaign has been #ZimbabweanLivesMatter, which rose to prominence in August 2020. The campaign has kept open civic space and hopes of democratic reform, as other forms of civic protest are being suppressed through harassment, intimidation and arrests of citizens (Karombo and Brown 2020). Our research has found that the level of global attention to the #ZimbabweanLivesMatter campaign has clearly unsettled the government, as there has been a spike in the number of individuals arrested for their online activities.

Overall, there is a discernible pattern of hashtags emerging in times of significant sociopolitical turmoil. The hashtags open civic space online and tend to draw large followings. They have woken up a lot of Zimbabwe to the concept of cyber-activism and campaigning as an alternative form of protest. Concerns about surveillance have also led to greater awareness about the need for security, resulting in the adoption of messaging apps that are deemed to be more secure, such as Telegram and Signal.

The first countrywide internet shutdown happened in January 2019, following massive protests against a 150 per cent fuel price hike and the struggle for economic justice. The shutdown was in effect for six days, during which time the armed forces unleashed a wave of terror, killing over a dozen people (Ndlovu 2019). Through his Twitter and Facebook accounts,[6] President Mnangagwa justified the shutdown, saying that 'social networks [were] being

4 **Alex T Magaisa tweet, 13 April 2018**.

5 '*Varakashi*' refers to the group of pro-government voices on Twitter who actively defend the government and troll its opponents.

6 **President Mnangagwa Facebook post, January 2019**.

 DOI: 10.19088/IDS.2021.006

used to plan and incite disorder and to spread misinformation leading to violence' (Chaparadza 2019).

In response, many Zimbabweans began downloading virtual private network software in order to circumvent the shutdown. The Zimbabwe chapter of the Media Institute of Southern Africa (MISA) successfully challenged the shutdown in the High Court on a legal technicality (Dzirutwe 2019). However, given that the constitutionality of the shutdown was not decided on, the government can implement a shutdown again so long as it uses the right procedure to do so.

## Table 4.1 Technology timeline

| Year | Shift | Implication |
|---|---|---|
| **2001–02** | Legislation to restrict digital rights. | Freedom of expression reduced by Broadcasting Services Act (2001) and Access to Information and Protection of Privacy Act (AIPPA) (2002). |
| **2013** | Bulk SMS ban. | Closed means for civic information, especially voter education. |
| **2014** | Mandatory SIM card registration. | Reduced right to privacy and increased state capacity for digital surveillance. |
| **2015** | State surveillance tools procured. | International mobile subscriber identity catchers, GPS trackers, vehicle trackers and mobile phone bugging of opposition politicians and civic activists for their online activities. |
| **2016** | Emergence of hashtag campaigns. | Opening of new online civic space. |
| | 500% price increase for mobile data. | Introduction of strategy to limit access and stifle freedom of expression. |
| **2017** | Cybersecurity and Data Protection Bill. | Multiple problematic provisions that can be used to shrink freedom of expression. |
| **2018** | Facial recognition technology. | Zimbabwe–China relationship over problematic Cloudwalk Technology (in terms of privacy rights). |
| | *Varakashi* – pro-government trolls. | Coordinated misinformation used to close civic space online. |
| **2019** | Internet shutdown for six days in January. | Zimbabwe's first total internet shutdown closes off online civic space and entirely removes digital rights. |
| **2020** | Hashtag protests. | #ZimbabweanLivesMatter, #ZanuPFMustGo. |

*Source:* Authors' own.

 DOI: 10.19088/IDS.2021.006

# 5. Digital rights landscape

What is clear from the previous section is that although Zimbabwean citizens have been making use of digital technologies to open civic space and express their digital rights, significant challenges persist. The laws and policies implemented by the state – such as the provisions that allow for the interception of communications or the collection of user data – and bans on specific technologies all stand in the way of achieving internet freedom and the full enjoyment of digital rights.

Although smartphones have provided citizens with many powerful tools to voice their concerns, the government's growing arsenal is quite substantial. The asymmetry is very apparent and building the capacity of civil society is urgent if the government is to be held accountable and citizens are to be able to express and defend their digital rights. Efforts have to be targeted at two connected levels: (a) building up technical capacities; and (b) building up awareness.

Due to the political struggles of the past two decades, the language of rights has become very common in the Zimbabwean public sphere. However, debates have rarely extended to issues of digital rights. This is despite the fact that as digital technologies become embedded in people's lives 'offline' and 'online' rights are becoming increasingly interdependent. Valuable documents that set out important principles for digital rights such as the African Declaration on Internet Rights and Freedoms, which was produced by a transnational coalition of CSOs (including MISA-Zimbabwe) are rarely, if ever, invoked (African Declaration on Internet Rights and Freedoms 2020).

The strong legal capacity in Zimbabwean civil society provides a foundation to build on in defending digital rights, but much more needs to be done to build the capacity of lawyers to engage with issues such as privacy and personal data protection. There is also an urgent need to push for greater checks and balances, as well as transparency in the way that laws relating to the interception of communications are implemented.

Aside from the legal capacity there is need for greater information and communications technology (ICT) capacity in order for CSOs to be able to monitor and detect issues such as the use of intrusive surveillance technologies and bring these to the attention of legal experts and advocacy groups. This should also extend to raising the capacity of civic organisations to protect their data and communications in the face of an authoritarian state that is intensifying surveillance. The combined efforts of ICT experts and legal experts can produce strong grounds for legal challenges to the constitutionality of repressive legislation.

 DOI: 10.19088/IDS.2021.006

Given the prevailing socioeconomic hardships, many Zimbabweans are focused on meeting their basic needs rather than digital rights. Issues such as SIM card registration, facial recognition and online disinformation are not given the attention they deserve. At the same time, there is limited realisation that the continued suppression of civic space and curtailment of digital rights leaves Zimbabweans limited in their ability to contest political corruption, fuel and food prices, or abuse of civil liberties and political freedom.

Organisations such as the Digital Society of Africa (DSA) have in some instances tracked activity around bandwidth throttling and network interference when they have occurred in Zimbabwe. However, this is not the primary work of the organisation and such activities are intermittent. Although these efforts have unearthed revealing behaviours, patterns and trends, they have been discontinued on grounds of lack of capacity. Ultimately, there is a need to develop public awareness, civic capacity and technical abilities to undertake systematic monitoring, tracking, analysis and public education on digital rights developments. Such local capacity needs to be complemented with transnational partnerships.

Much more needs to be done to increase public awareness of the actions of the state, corporate organisations and, indeed, other citizens that affect people's digital rights. To a degree, many of the legal and technological strategies employed by the government to suppress digital rights are neither widely publicised nor understood. It is also not uncommon for draconian legislation to be passed without meaningful public consultation. Much more needs to be done to promote public awareness of the key principles of internet freedom and digital rights. The study of efforts to promote human rights across the continent has shown that the most sustainable and successful efforts have to be centred on and driven by citizens (Englund 2005; Neocosmos 2006).

 DOI: 10.19088/IDS.2021.006

# 6. Digital rights in times of Covid-19

The coronavirus (Covid-19) pandemic has tended to accentuate existing social and political dynamics in Zimbabwe. In keeping with the aphorism 'never let a good crisis go to waste', the government has tried to use the pandemic in multiple ways to aid its own agenda. It has expanded the powers of the police and passed regulations that enable them to arrest individuals who are found to be acting in ways that are deemed to promote the spread of the virus.

These laws have been used to suppress civic expressions of dissent. There has also been a proliferation of conspiracy theories around Covid-19 on social media and, in some instances, these have been disseminated to serve political purposes. For example, Deputy Minister of Defence Victor Matemadanda sought to discourage citizens from participating in anticorruption protests planned for 31 July 2020 by arguing that foreign agents were planning on infecting the participants with coronavirus.[7] It is difficult to determine what impact such Covid-19 disinformation has had. However, what it does indicate is an effort to weaponise Covid-19-related disinformation.

In 2020, the economic situation worsened under lockdown conditions and this has intensified the focus on corrupt activities of the political elite. The restrictions on movement have forced protest activities to move online. For example, citizen activists started a protest online using two campaigns. One aimed to have massive numbers of people unfollow the president on Twitter, on the basis that: 'Dictatorships thrive on public validation. Unfollowing is a great form of resistance against his corrupt rule… it is public rejection which he can't rig!' (Mashininga 2020). Another hashtag campaign during lockdown was #July31st, used concurrently with #ZanuPFMustGo, challenging Zimbabweans to go out on to the streets in protest against government ineptitude. Ruling party supporters attempted to hijack #ZanuPFMustGo by creating the counter-hashtag: #ZanuPFMustGoOn. Because Twitter sometimes auto-completes popular hashtags, some less observant Twitter users accidentally ended up tacking on the wrong hashtag.

7 **Dewa Mavhinga tweet, 1 August 2020**.

 DOI: 10.19088/IDS.2021.006

# 7. Conclusion

The preceding sections have illustrated that over the past two decades digital technology has been increasingly enlisted in the struggles that are animating Zimbabwean politics. In all of this it has functioned as a double-edged sword, empowering citizens on the one hand and reinforcing state power on the other. We have also underscored the asymmetric nature of these struggles due to the vast resources the state has at its disposal to counter any empowering aspects of digital technologies.

If digital media are to play a greater role in expanding civic space and ending the interregnum that Zimbabwe finds itself trapped in, two steps need to be taken.

First, there is a critical need for civil society's capacity to be strengthened in order to deal with three important areas: (a) monitoring, (b) lobbying policymakers and (c) building public awareness. Zimbabwean civil society is very weak in the area of digital rights and there is an urgent need to build up technical abilities to monitor developments in the digital sphere, from the adoption of cutting-edge surveillance technology to the implementation of different forms of computational propaganda. This ICT capacity has to be coupled with the legal capacity to evaluate legislation and formulate policy alternatives. Building public awareness is a crucial part of any digital rights strategy.

Second, local and transnational partnerships have to be central to any strategy to build a stronger digital rights regime in Zimbabwe. There is ample scope for building synergistic partnerships between organisations that have decades of experience on human rights work, such as ZLHR, and those working in the area of digital security, such as the DSA. Partnerships between organisations across the continent can foster important opportunities for knowledge exchange.

 DOI: 10.19088/IDS.2021.006

# References

African Declaration on Internet Rights and Freedoms (2020) ***African Declaration on Internet Rights and Freedoms*** (accessed 1 September 2020)

Amnesty International (2019) ***'Open for Business Closed for Dissent': Crackdown in Zimbabwe During the National Stay-away 14–16 January 2019***, 8 February (accessed 20 October 2020)

Article 19 and MISA-Zimbabwe (2004) ***Access to Information and Protection of Privacy Act: Two Years On*** (accessed 20 October 2020)

Batambuze III, E. (2013) **'Bulk Text Messaging Service Banned in Zimbabwe'**, *PC Tech Magazine*, 29 July (accessed 1 September 2020)

Bulawayo24 (2015) **'Iran Gives Mugabe Spy Technology'**, 26 January (accessed 1 September 2020)

Chaparadza, A. (2019) **'President Mnangagwa Justifies Internet Shut Down, Although "He Deeply Believes In Freedom Of Speech And Expression"'**, *TechZim*, 26 January (accessed 20 October 2020)

CIPESA (2020) ***State of Internet Freedom in Zimbabwe 2019: Mapping Trends in Government Internet Controls, 1999-2019,*** Kampala: Collaboration on International ICT Policy for East and Southern Africa (accessed 1 September 2020)

Dzirutwe, M. (2019) **'Zimbabwe Court says Internet Shutdown Illegal as More Civilians Detained'**, *Reuters*, 21 January (accessed 20 October 2020)

Englund, H. (2005) *Prisoners of Freedom: Human Rights and the African Poor*, Berkley CA: University of California Press

Feldstein, S. (2019) ***The Global Expansion of AI Surveillance***, Working Paper, Washington DC: Carnegie Endowment for International Peace (accessed 20 October 2020)

Freedom House (2020) ***Country and Territory Ratings and Statuses 1973–2020*** (accessed 1 September 2020)

Freedom House (2019) ***Freedom in the World*** (accessed 4 December 2020)

Gambanga, N. (2016) **'Here's the Zimbabwean Government's Warning Against Social Media Abuse'**, *TechZim*, 6 July (accessed 1 September 2020)

Gramsci, A. (1971) *Selections from the Prison Notebooks*, ed. and trans. by Quintin Hoare and Geoffrey Nowell-Smith (1992), London: Lawrence & Wishart

Gwagwa, A. and Hove, K. (n.d.) ***Use of IMSI Catchers in Zimbabwe's Domestic Law Enforcement*** (accessed 1 September 2020)

Htxt, L.S. (2016) **'Zimbabwe Data Prices Hiked up by up to 500% to Curb Social Media Activism and Dissent'**, *Mail & Guardian*, 5 August (accessed 1 September 2020)

Internet World Stats (2020) ***Internet User Statistics for Africa*** (accessed 1 September 2020)

Karekwaivanane, G. (2017) *The Struggle over State Power in Zimbabwe: Law and Politics since 1950*, Cambridge: Cambridge University Press

Karekwaivanane, G. and Mare, A. (2019) ' "We Are Not Just Voters, We Are Citizens", Social Media, the #ThisFlag Campaign and Insurgent Citizenship in Zimbabwe', in T. Molony and M. Dwyer (eds), *Social Media and Politics in Africa: Democracy, Security and Surveillance*, London: Zed Books

Karombo, T. and Brown, R.L. (2020) **'When a Crackdown Prevented Protests a Hashtag Gave Them a Voice'**, *The Christian Science Monitor*, 17 August (accessed 7 September 2020)

Laiton, C. (2014) **'Sunday Mail Editor "is Baba Jukwa" '**, *The Standard*, 22 June (accessed 20 October 2020)

Mashininga, K. (2020) **'Unfollow the Leader: The Twitter Campaign Against Zimbabwe's President'**, *Mail & Guardian*, 8 July (accessed 20 October 2020)

Masunungure, E.V. (2014) *The Changing Role of Civil Society in Zimbabwe's Democratic Processes: 2014 and Beyond*, Working Paper, Bonn and Berlin: Friedrich Ebert Stiftung

 DOI: 10.19088/IDS.2021.006

Mokwetsi, J. (2014) **'Zimbabwe: Cyber Freedom – Have we Started to Censor Ourselves?'**, *The Standard*, 13 July (accessed 20 October 2020)

Motlanthe Commission of Inquiry (2018) ***Report of the Commission of Enquiry into the 1 August 2018 Post-Election Violence***, Harare: Commission of Enquiry into the 1 August 2018 Post-Election Violence (accessed 20 October 2020)

Muzulu, P. (2017) **'Uproar over Data Tariff Rise'**, *Newsday*, 12 January (accessed 20 October 2020)

Ndlela, D. (2020) **'Shutting Down the Citizens: Forget Your Privacy You are Under Surveillance'**, *The Standard*, 26 January (accessed 1 September 2020)

Ndlovu, M. (2019) **'First Total Internet Shutdown in Zimbabwe'**, *Bulawayo24*, 15 January (accessed 1 September 2020)

Neocosmos, M. (2006) **'Can a Human Rights Culture Enable Emancipation? Clearing some Theoretical Ground for the Renewal of a Critical Sociology'**, *South African Review of Sociology* 37.2: 356–79, DOI: 10.1080/21528586.2006.10419163 (accessed 20 October 2020)

New Zimbabwe (2020) **'Journalist Hopewell Chin'ono home raided by cops, Ngarivhume arrested'** (accessed 1 September 2020)

OHCHR (2020) ***Zimbabwe: UN Experts Demand an Immediate End to Abductions and Torture***, Geneva: United Nations Office of the High Commissioner for Human Rights (accessed 1 September 2020)

POTRAZ (2019) *Annual Postal and Telecommunications Sector Performance Report 2019*, Harare: Post and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)

POTRAZ (2013) ***Circular on Bulk SMS***, Harare: POTRAZ (accessed 1 September 2020)

Quartz Africa (2018) **'China is Exporting Facial Recognition Software to Africa, Expanding its Vast Database'**, 25 May (accessed 1 September 2020)

Raftopoulos, B. (ed.) (2013) *The Hard Road to Reform: The Politics of Zimbabwe's Global Political Agreement*, Harare: Weaver Press

Sachikonye, L.M. (2013) 'Continuity or Reform in Zimbabwean Politics? An Overview of the 2013 Referendum', *Journal of African Elections* 12.1: 178–85

Tendi, B.-M. (2020) **'The Motivations and Dynamics of Zimbabwe's 2017 Military Coup'**, *African Affairs* 119.474: 39–67, DOI: 10.1093/afraf/adz024 (accessed 20 October 2020)

The President and the Parliament of Zimbabwe (2007) ***Interception of Communications Act [Chapter 11:20] Act 6/2007***, Harare: The Parliament of Zimbabwe (accessed 20 October 2020)

Tshili, N. (2016) **'Zanu-PF will never Reform itself out of Power, Prof Moyo Declares'**, *The Chronicle*, 6 September (accessed 20 October 2020)

Weber, V. (2019) *The Worldwide Web of Chinese and Russian Information Controls*, Working Paper Series 11, Oxford: Oxford Centre for Technology of Global Affairs, University of Oxford

# Zambia Digital Rights Landscape Report

Sam Phiri and Zorro



This report is part of 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries'; the Introduction is also recommended reading.

© 2021 Sam Phiri and Zorro © Institute of Development Studies. DOI: 10.19088/IDS.2021.007

# 1. Introduction

This report offers an overview of the digital rights situation in Zambia. The purpose is to scope the rights landscape in Zambia; and to document the political, civic, and technological areas. The report is dependent on desk reviews of existing documents about what is taking place in the country. The overall objectives of this study are to: promote an understanding of the civic and digital rights situation in the country; identify local Zambian capabilities and existing gaps; reflect upon the digital technologies used by government and civil society; and, finally, to recommend areas for further research, civic activism, and policy change.

Generally, it is observed that Zambia's civic space has, over the years, narrowed through a combination of factors. These factors include government political and legal actions on one side, and the rather weak civil society base on the other. Ultimately, though, in promoting a better understanding of the digital rights situation in Zambia, this report seeks to ensure that citizens continue advocating for the expansion of local civic spaces. At the same time, scholars are expected to back up this 'pushback movement' with the requisite empirical research into this critical area of social practice. By so doing, civil society, scholars, and policymakers, jointly or separately, will hopefully build new platforms and bases, to promote policy change and new policy directions.

For our purposes, we define civic space as 'the set of conditions that determine the extent to which all members of society, both as individuals and in informal or organised groups, are able to freely, effectively and without discrimination exercise their basic civil rights' (Malena 2015: 14) and delimit the notion of digital rights to human rights during the era of the internet. These are basically civil rights that relate to the right of online privacy, freedom of expression and freedom of online association (Hutt 2020).

Thus, the report takes a bird's eye view of the political situation over the past 20 years, closely examines the status of Zambian civic space and scrutinises the technologies used. It concludes that the fortunes of the country's digital rights situation could depend on: the emergence of more vibrant civic activism; the building of a culture of respect for human rights; creation of more open civic spaces; and ensuring greater civic participation in policy formulation and implementation.

 DOI: 10.19088/IDS.2021.007

# 2. Political landscape

Zambia, with a population of 18 million people, has been an independent state since October 1964. In a period of 56 years, it has undergone three major political phases. These are the eras of multiparty democracy, one-party rule and then a return to multiparty democracy in 1990. Since then, Zambia has enjoyed a relatively free and peaceful political environment, albeit with a lot of economic and other social problems.

However, throughout these periods, what has remained constant is the powerful position occupied by the executive wing of government over all other sectors such as parliament, the judiciary, the media, and civil society formations. What Zambia has had since 1964 has been an authoritative patrimonial and almost imperial presidency that is ably reinforced by a governing party and looms large across all sections of society.

This is despite Zambia having had three different constitutions and two additional major constitutional amendments in 1964, 1969, 1973, 1991 and 1996, respectively (ZIS 1991; Chinyere and Hamauswa 2016). However, the basics of the winner-takes-all one-party rule paradigm have remained unchanged. This static situation has generally impacted upon Zambia's human rights ethos and resulted in a weak participative culture in civic activities by its citizens.

Besides, from the initial years of Zambia's independence, its first president, Kenneth Kaunda, established an oppressive and ubiquitous eavesdropping state security apparatus, which spied on citizens and bugged communication lines, such as telephones (Sardanis 2014: 89). This 'System' as it is colloquially called, was supported by an entrenched pyramidal political party structure. This was the supreme governing body of the country that since independence in 1964 had continued to vest itself with more and more powers (*ibid.*: 89). This entrenched a tradition of social control that has largely continued and is now impacting on human rights and digital citizenship.

However, after the changes of 1990–91, when the country returned to multiparty democracy, there were promising signs that the socio-political dominance of governing political parties as described above was to take a back seat and that spaces for media and civil society would open up. This hope did not last long. By 2011, such positive political reforms had dwindled. Systemically and then, quickly, they were reversed when new President Michael Sata came into office.

Sata, who cut his political teeth during the one-party era, was sent to the Soviet Union by the Kaunda government to study as a 'commissar' in

 DOI: 10.19088/IDS.2021.007

political party organisation (Scott 2019: 54). After becoming president, he subsequently reasserted the supremacy of his governing political party, the Patriotic Front (PF), placed the PF's chief executive officer on the government payroll, and ensured that government ministers genuflected to the PF. Social policy, too, was generated from the corridors of the party offices, as was the case before 1991. Whereas in the immediate aftermath of the 1991 changes, the governing party was distanced from the government, Sata reasserted the supremacy of the PF as the overlord 'ruling' party, thereby placing state functionaries into submissive roles to those of PF party officials (Zambia Reports 2012a). The reversal was almost complete.

Further, Sata ensured that the Public Order Act (POA) – an old, repressive colonial law, enacted in 1955, and, originally meant to subdue anti-colonial protests – was used to the maximum, to reduce dissent, paralyse civil society activism and mollify opposition elements. In fact, within six months of being in office, Sata said that the POA, which when in opposition he had considered reprehensible, was in fact a good law for maintaining social order (Zambia Reports 2012b; Zambian Watchdog 2012).

These reversals were strongly opposed by civil society organisations (CSOs) including the Zambia Episcopal Conference (ZEC), representing the Catholic Church; the Law Association of Zambia (LAZ) for the legal fraternity; and the Council of Churches in Zambia, on behalf of Protestant Christians. Summing up the feelings of the times, ZEC said: 'looking at what is happening… it would seem to us that the ideals of a politically plural society have not been fully understood and appreciated by those who aspire for political leadership in our successive governments'. The ZEC called on political leaders to 'prudently exercise the power that the Zambian people have entrusted in them' (Zambia Reports 2013).

Since then, there has been a closing-in of political spaces for actors with alternative views such as the CSOs. Old laws have been harshly enforced. New ones have been put in place. Hopes for a more open society have been largely dashed. Among the laws and regulations in Zambia that now specifically oversee digital citizenship, or govern digital rights are those listed below.[1]

## 2.1 Information and Technologies Act of 2009

A unique feature of this law is that it takes 'supremacy' where there is inconsistency between it and any other law with regard to the regulation of information and communication technologies (ICTs). Also, it empowers the regulatory authority, the Zambia Information and Communications Technologies Authority (ZICTA), which it created, to be responsible for radio

1 All the cited laws are available on the **Zambian National Assembly website**.

 DOI: 10.19088/IDS.2021.007

frequency transmissions. This has a direct effect on the broadcasting sector in Zambia. For instance, in August 2020 the Independent Broadcasting Authority (IBA), the broadcasting regulatory authority that works in tandem with ZICTA, claimed that all online broadcasting should be licensed because according to the IBA, the law states that:

> Any person wishing to operate or provide broadcasting service in Zambia, regardless of whether the broadcasting service is conveyed through radio frequency spectrum or any electronic communication networks such as the Internet, is required to obtain a broadcasting license from the IBA. Operating without a broadcasting license amounts to an offence.
>
> (News Diggers 2020)

The IBA was responding to a Zambia-based online television station, Spring TV, which had incorrectly reported the suicide of a fired government minister. General Education Minister David Mabumba had been dropped from the cabinet for producing and distributing pornography on the internet, but he was alive (The Mast 2020; The Zambian Observer 2020).

## 2.2 Electronic Communication and Transaction Act of 2009

This law allows for the 'lawful' interception of communications; for service providers to install interception devices/software in their infrastructure; for the minister to instruct service providers to disclose 'alleged illegal activities' of suspects, and for the establishment of a government-controlled Central Monitoring and Coordination Centre, which, on behalf of the state, aggregates all communications interceptions. Further, there is an absence of data protection and privacy laws to safeguard the interests of digital citizens in Zambia. Whereas, in brief, this law ostensibly forbids service providers from monitoring user activities, nonetheless the minister can order that they install devices for real-time monitoring of suspects and disclose suspects' activities to the authorities. Moreover, there are no safeguards for data collected by telecoms companies, traffic police, insurance companies, and even hospitals since the emergence of diseases such as HIV/AIDS and the coronavirus disease (Covid-19).

## 2.3 Statutory Instrument No. 65 of 2011

This sub-legislation provides for the registration of all SIM cards used in Zambia. Owners are expected to give personal details regarding their residences and particulars of national registration cards (NRCs). All Zambians are compelled to be registered and are expected to carry their NRC with them at all times from the age of 16 years.

 DOI: 10.19088/IDS.2021.007

## 2.4 Non-Governmental Organisations Act No. 16 of 2009

This law requires that all non-governmental organisations (NGOs), including those engaged in digital rights work, whether local or international, be registered with the Registrar of Societies. It is also a requirement that NGOs should on an annual basis submit their activity reports to the government department responsible for NGOs, the Ministry of Social Welfare. The inflows and outflows of the finances of NGOs are also closely monitored by the government. This means that any organisation that is working in the civic sphere, whether on aspects of human or digital rights or not, is closely monitored by the government. Such oversight has been considered 'highly restrictive' (CIVICUS 2017) by some observers. Moreover, the mere presence of the demand that all CSOs should be registered by a government agency presupposes the absence of privacy for civic activists. The good thing, though, is that this act is under revision, with some limited consultation with the NGO sector.

## 2.5 Preservation of Public Security Act (PPSA) of 1960

This law has been used to control public gatherings; ban publications considered to be 'prejudicial to public security'; and regulate assemblies, including those of political parties and CSOs. The law also authorises the president to do anything 'as appear[s] to him to be strictly required by the exigencies of the situation in Zambia'. This law was used in 1996 to ban the online issue of *The Post* newspaper, including its hard-copy edition. On many occasions, it has been used to stop unauthorised public gatherings, arrest protesters, and violently disperse public gatherings, including those of NGOs and opposition political parties, actions which in some instances have led to deaths (*ibid.*).

Clearly, Zambia has witnessed the government exercising greater control over its people. Also, the country has observed that the state was getting as much information as possible about people's private lives and activities (MTN 2020). Then, too, the domestic civic space has been substantially narrowed especially for human rights activists, lesbian, gay, bisexual, transgender, intersex and queer (LGBTIQ) people, bloggers, academic researchers and all others who are on the margins of, or outside, government thinking.

The next section focuses on how this political and legal context has shaped the civic space in Zambia.

 DOI: 10.19088/IDS.2021.007

# 3. Civic space landscape

Since its independence from Great Britain in 1964, Zambia has enjoyed a diverse and active civil society, which includes labour unions, community-based human rights activists, development organisations, and church groups. Additionally, the country has maintained peace and stability since the change in 1990–91 to multiparty politics, marking a break from 19 years of one-party rule, which had been established in 1972.

As a result, the *Freedom in the World* report of 2019 scores Zambia as partly free with a total of 54 points on a scale of 1 to 100 (Freedom House 2019a). According to the report, Zambia scores 22 out of 40 for political rights and 32 out of 60 for civil liberties.

## Figure 3.1 Freedom House ranking for ADRN countries, 2000–19[2]

| | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Zimbabwe** | | | | | | | | | | | N/A | | N/A | | | | | | | |
| **Zambia** | | | | | | | | | | | N/A | | N/A | | | | | | | |
| **Uganda** | | | | | | | | | | | N/A | | N/A | | | | | | | |
| **Sudan** | | | | | | | | | | | N/A | | N/A | | | | | | | |
| **South Africa** | | | | | | | | | | | N/A | | N/A | | | | | | | |
| **Nigeria** | | | | | | | | | | | N/A | | N/A | | | | | | | |
| **Kenya** | | | | | | | | | | | N/A | | N/A | | | | | | | |
| **Ethiopia** | | | | | | | | | | | N/A | | N/A | | | | | | | |
| **Egypt** | | | | | | | | | | | N/A | | N/A | | | | | | | |
| **Cameroon** | | | | | | | | | | | N/A | | N/A | | | | | | | |

**Free** **Partially free** **Not free**

*Note:* ADRN – African Digital Rights Network.

*Source:* Adapted from Freedom House (2019b)

2 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.007

Further, a 2017 overview of Zambia by CIVICUS states that civil society's challenges include limited capacity for networking and high dependency on external resources. However, other broader societal challenges include political polarisation, lack of judicial independence, and practices such as torture and unlawful killings by the police force (CIVICUS 2017).

Therefore, a current source of concern for the operations of civil society is the introduction of legislation to control civic and public space. One example of this is the Non-Governmental Organisations Act No. 16 of 2009, referred to above, that provides for the coordination and regulation of NGOs; and establishment of the Non-Governmental Organisations' Registration Board (NGO Board) and the Zambia Congress of Non-Governmental Organisations, for the ostensible reason of enhancing transparency and accountability in the activities of the NGO sector (PMRC 2016).

The act was introduced in spite of CSOs' efforts at self-regulation. Earlier in 1999, CSOs had instead created a voluntary code of conduct for self-regulation in response to government plans to regulate them. The voluntary code was meant to strengthen CSOs' capacity to work independently and to negotiate with government.

According to Leah Mitaba, the director of the Zambia Council for Social Development, the NGO Act contravenes the constitution and places Zambia in a bad light globally and among its people who, since the return to the multiparty system, have wished to ensure that Zambia thrives through an active citizenry that holds its government to account (Chakwe 2020).

The NGO Act contains provisions that make it susceptible to abuse and offers the state the opportunity of constraining the freedoms of NGOs. Key points requiring review in the legislation are: the definition of what NGOs are; excessive ministerial authority; severity of penalties; imbalanced representation on the NGO Board; and the absence of an appeals process (PMRC 2016).

Other pieces of legislation that at the time of writing were yet to be brought before parliament by the government, albeit with notably low public engagement, include: The E-Government Bill; Data Protection Bill; E-Transactions and E-Commerce Bill; and the Cyber Security and Cyber Crime Bill.

For Mitaba, civil society needs to engage the state to ensure that any such proposed legislation complies with Zambia's international and continental obligations, as well as best practices, and that they offer an enabling environment for civil society operations.

Table 3.1 offers a perspective on the implications of the above-mentioned laws and political actions for civic space in Zambia.

 DOI: 10.19088/IDS.2021.007

# Table 3.1 Civic space timeline

| Year | Shift | Implication |
|---|---|---|
| **1999** | CSOs create voluntary code of conduct | Strengthens CSOs' capacity to work independently and to negotiate with government |
| **2000–present** | Increased inter-party violence during elections | Narrowing of space for political activity as citizens are generally fearful of partaking in political activities, including elections |
| **2004** | Government publishes contentious NGO Bill | Plans to give government control over CSOs financing, registration and other activities |
| **2009** | NGO Act becomes law | Reduced operational freedom and effectiveness of NGOs |
| **2011–present** | Abuse of Public Order Act | Obstruction of public policy debate, freedom of expression and freedom of association |
| **2011** | Forced registration of SIM cards | Makes it easier for government to check and follow citizens' communication |
| **2013** | Secret service ordered to tap phone conversations and emails of all people in Zambia | Fear among the public of talking openly and freely |
| **2013** | Online websites forcibly shut down | Free flow of information and free exchange of views curtailed |
| **2016** | *The Post* newspaper closed by government | Civic space narrowed |
| **2018–present** | Introduction of well-funded social media accounts by state functionaries | Promotion of fake news, disinformation, misinformation and the drowning out of alternative voices |
| **2018** | Introduction of tariffs on internet phone calls | High cost of communication reduces the amount of communication taking place in society |
| **2018** | CSOs form own Council of Non-Governmental Organisations in Zambia to strengthen the independence from government of NGOs | Pushback by CSOs against government control |
| **2019** | Independent television station Prime TV closed | Media freedom curtailed |
| **2019** | Government introduces tax on online streaming platform Netflix with the purpose of sharing profits | High costs bar entry and access into this new form of social communication |
| **2019** | Cabinet approves Access to Information Bill, which has been on ice since 2002 | Hopes for a more open government raised – but as of 25 January 2021 the Bill had not gone before parliament, once again dashing hope and optimism |
| **2019** | Introduction of constitutional amendments to strengthen the presidency and weaken the judiciary and parliament | Public debate around this constitutional amendment (Bill No.10 of 2019) splits the country as a substantial number of CSOs and the public are against the intended changes |
| **2020** | Arrests of social media 'bloggers' | Public disengagement from free expression on matters of public policy; increased levels of fear generally among the public |

*Source:* Authors' own.

 DOI: 10.19088/IDS.2021.007

As can be seen from Table 3.1, the introduction of the internet and social media has substantially increased interactions in digital spaces. This dynamism, however, has also attracted government attention. Further, although observers expected greater civic activism and dialogues within the available digital spaces, especially where the enduring and pervasive restrictions on physical space had not yet taken root, this hope remains under threat.

Section 4 therefore looks closely at how CSOs have responded to these challenges through the use of ICTs.

 DOI: 10.19088/IDS.2021.007

# 4. Technology landscape

According to ZICTA, since 2000 there has been a consistent increase in the number of households in Zambia that have access to the internet. It is estimated that 32 per cent of households in urban areas and just under 7 per cent in rural areas access the internet on a regular basis (ZICTA 2020: 32). Further, according to IWS (2020), in the first quarter of 2020 internet penetration within the Zambian population had reached 54 per cent, which is an almost 50 per cent growth within 20 years. On the other hand, the Paradigm Initiative (2020) states that in 2019 Zambia's internet penetration stood at 59 per cent, accounting for over 10 million users, most of whom access the internet using mobile devices. Moreover, out of a population of 18 million people, about 2.25 million are on Facebook (IWS 2020).

This digital presence and interactivity have given rise to a desire for expanded digital rights. As said above, digital rights are universal human rights in digital spaces. They include, but are not limited to, the right to privacy, freedom from violence, freedom of political opinion, freedom of expression and freedom of association (IDS 2020).

In this vein, several organisations are engaged in digital rights work in Zambia. Some of these are the Paradigm Initiative for Africa, which is supporting dialogues on digital rights in Zambia and the Southern African region; the Internet Governance Forum, an open and inclusive space for dialogue on internet governance issues of relevance to people in Zambia; the Internet Society Zambia Chapter (ISOCzm), a platform committed to fostering internet access; the Zambian Bloggers Network, an autonomous space for bloggers, internet content developers and journalists; and MISA Zambia (Media Institute for Southern Africa Zambia), a membership-driven organisation for independent Zambian media institutions and practitioners.

Notable among these is the Paradigm Initiative, which is an international organisation that was initiated from Nigeria and has offices in Abuja, Accra in Ghana, Douala in Cameroon, Nairobi in Kenya, and the Zambian capital Lusaka. It is a continental operation that advocates for digital rights in order to improve the lives of the youth (Paradigm Initiative 2020). The Lusaka office looks after digital rights interests in Southern Africa, especially Zambia, Malawi, and Zimbabwe. Broadly, its objectives are to empower CSOs to defend and advocate for digital rights; train media to report on, follow trends in and analyse digital rights issues; and to articulate an Africa-wide digital rights strategy around its four main action pillars:

 DOI: 10.19088/IDS.2021.007

- Internet shutdowns
- Social media
- Public policy
- Existing threats and opportunities.

This is a youthful centre of activism and among the most interesting organisations working on digital rights in Zambia. The other organisations referred to above are doing similar things, but approach issues differently.

Along with several other CSOs, they constitute a public response to emerging rights abuses in the country. For example, when it was learnt that tough secrecy bills were in the offing, journalists, CSOs, media and bloggers launched the hashtag #OpenSpaceZM, fearing that the new laws could have 'rights repressing clauses' (Paradigm Initiative 2020), and called for more openness and fuller public participation in the development of these laws.

Earlier, in 2016, prior to the general election CSOs came together and formed the Zambia Elections Information Centre (ZEIC) whose objective was to offer timely and credible information about the elections; be a platform for e-participation; offer weekly reports on the progress of the campaigns; and run a popular hashtag campaign, #TakeZambiaBack (this campaign was quite successful; in one week alone, in June 2016, ZEIC noted that there were 254,000 impressions).

Since then, there have been other CSO-based hashtag campaigns such as #YellowCard, #Bill10, #42X42, #Zambia and #HandsOffOurConstitution. These have dealt with corruption in government, and government attempts to meddle with the national constitution. In Table 4.1, we briefly examine the impact of state responses on civic digital activism.

## Table 4.1 Technology crackdown

| | | |
|---|---|---|
| **2016–present** | Shutdowns of internet and communication services in certain regions of the country that are strongholds of opposition parties | The regularity of these unexplained events suggests that this could have been a ploy to curtail the flow of political information and freedom of choice in affected areas |
| **2019** | Government establishes the 'Cybersecurity Crack Squad' aimed at tackling cybercrime on digital platforms | The squad consists of all the top security agencies, including the intelligence services – its formation spreads fear and has a chilling effect on freedom of expression |
| **2019** | A teacher is jailed for two years for defaming the president on his social media account | Chilling effect on public policy debates |
| **2020** | Former Law Association of Zambia president Lawrence Kasonde is arrested for 'insulting' President Lungu in a self-recorded viral video posted in a WhatsApp group where Kasonde displays a voter's card before unleashing insults on Lungu and his government | The government has the technological capability to locate sources of anti-state viral videos even on secure private platforms – this has a chilling effect on freedom of expression |

*Sources:* ZNBC (2020); News Diggers (2019); Zambia Today (2020).

 DOI: 10.19088/IDS.2021.007

The incidents listed in Table 4.1 lead us into discussing in some detail the existing technology landscape in Zambia today. Moreover, as indicated in section 2, in 1996 the government took down the online edition of *The Post* and banned the paper under the PPSA of 1960, initially passed in 1955. This law was adapted from an earlier British, law which has since been scrapped from the British statute books.

Nonetheless, in 2013 President Sata authorised the secret service to tap the phone calls and emails of 'anyone living in Zambia' (Zambian Watchdog 2013). In the same year, the government blocked four websites: Zambian Watchdog, Zambia Reports, Barotse Post and Radio Barotse. In March 2020, a 15-year-old nicknamed 'Zoom' was arrested for defaming President Lungu in his Facebook posts. The juvenile faces five years in prison if convicted.

The above actions have raised concern both locally and internationally. For instance, international organisations such as the Carnegie Endowment for International Peace have speculated that by 2013 the Zambia government had the means, through deep packet inspection (DPI) software, to internally monitor internet activity within its territory. The DPI technologies are used for 'online filtering and surveillance' (Weber 2020) of citizens' communication.

Besides that, the Zambian government reportedly, has facial recognition and artificial intelligence technologies that enable it to monitor citizens' activities beyond the internet. This ability was made possible by equipment imported from China and other countries, installed by companies such as Huawei, Hikvion, and ZTE (Carnegie 2020). According to Freedom House (2019a), Zambia is among 45 countries that use Israeli spyware, Pegasus, to spy on its citizens. Further, the extensive interconnectedness between Zambia and China reveals that Zambia is positioned at the core of China's technological sphere of influence ('techno-sphere') in Africa. In order to control its domestic population, the Zambian government has relied on censorship and surveillance gear supplied by Huawei and ZTE (Carnegie 2020).

It is claimed that Huawei employees allegedly aid the Zambian government to intercept digital communications of journalists and opposition groups (OONI 2016; Stratfor 2019; Citizen Lab 2020). Moreover, Huawei has also implemented a US$210m Lusaka smart city programme, which has increased the government's physical surveillance capabilities. This initiative has augmented the government's power to police its citizens, track those with dissenting views and compare their faces with records in the national data centre. In the near future, it will help build mobile broadband connectivity infrastructure that will reach rural villages, a platform where government programmes will be promoted (Bloomberg 2019). In addition, the media landscape of the country has been influenced by Chinese soft diplomacy, which has seen Zambian journalists attending various training programmes in China.

 DOI: 10.19088/IDS.2021.007

In terms of the uses and abuses of this power, there are already some indications of this. For example, in 2014 a 'fake account', Edgar Lungu for 2016, appeared in cyberspace touting and promoting Lungu, then officially only a 'junior' minister, for the presidency. Observers suspected that this was part of an emerging trend of what some later called the 'misinformation, disinformation, and impersonation of politicians and high profile individuals using fake social media accounts' (Paradigm Initiative 2020). Whether or not this particular account qualifies to be described as such, is unproven. Nonetheless, Lungu disassociated himself from the account; but two years later he was elected president.

Of note is that when the newly elected President Sata announced his initial cabinet on 29 September 2011, Lungu was officially named as deputy vice president in the office of Vice President Guy Scott (Bloomberg 2011). This appointment raised eyebrows because Scott, a Zambian of Scottish origins, could not in any circumstances constitutionally succeed the incumbent president because of his foreign roots. The concept of a 'deputy vice presidency' was quietly shelved from public discussions, as such a post did not exist in the national constitution, but may in fact have continued to exist, out of the public gaze.

Although Lungu was not officially deputy vice president, events before and in the aftermath of the death in office of President Sata may indicate otherwise. Whereas just before Sata's death, Lungu was anointed as chief executive officer of the ruling PF party, he was also named as minister of justice, defence, and home affairs concurrently. At the time of Sata's death, Lungu had 'no fewer than five high ranking titles' (Mukwita 2017: 111).

Of this transition period, Scott writes that after Sata's death, a power struggle ensued, adding that:

> there were significant breaches of the law and the constitution… the actions of some people influenced what happened then and what continues to happen. However, I am bound by the State Security Act, and I cannot give a partial account as it would be rather lopsided… a full account exists, and it will be made available at some time in the distant future.
>
> (Scott 2019: 239)

However, during the presidential election of August 2016, Zambian technology blog TechTrends reported several internet connectivity interruptions (Techzim 2016). No one really knows what caused these internet outages, but Lungu won the election by a slim margin of 100,530 votes of the 3,621,224 valid votes cast (ECZ 2020). The quick emergence of Lungu as Sata's successor, combined with digital interruptions that had not previously been

 DOI: 10.19088/IDS.2021.007

experienced, and the ever-growing Chinese presence in Zambian economic, digital and financial affairs, and ever since, in a country reportedly positioned at the core of China's techno-sphere (Carnegie 2020), are matters that are open to conjecture.

Table 4.2 illustrates public events that have had an impact on civic activism in Zambia since 2003.

## Table 4.2 Technology timeline

| Date | Shift | Response | Implications |
|---|---|---|---|
| **2003–present** | Government initiates constitutional review process | Outrage among CSOs against a less inclusive review process | Civic space slightly widens as CSOs push back |
| **2010–14** | Government insists on proceeding with the review process without CSOs | Red Card Campaign for a people-driven constitution | CSOs resist government pressure to close civic space |
| **2015** | Presidential by-election | CSOs jointly monitor 2015 presidential by-election campaigns | Civic activism expands |
| **2016** | General election and referendum to amend constitution | New constitution in place; CSOs monitor 2016 general election and referendum | CSOs reassert themselves and civic activism strengthens |
| **2018** | Financial Intelligence Centre (FIC) created by government | Revelations of deep corruption in the purchase of 42 fire engines for US$42m | Civic space expands through use of various platforms including Twitter, Facebook, SMS, WhatsApp, blogs, websites, hashtags and community-based radio |
| **2019** | FIC reveals more corrupt practices in government | Yellow Card Campaign results in some government ministers being fired | Civic activism increases |
| **2020** | Youth for accountability movement emerges | Youths launch campaign for jobs and government accountability, and against corruption | Emergence of youth activism within civic space and use of digital technologies |
| | Government tables constitutional amendment bill in parliament | Anti-constitutional amendments campaigns arise among CSOs, clergy and youth | Further struggle between the state and CSOs for control of civic space |

*Source:* Authors' own.

 DOI: 10.19088/IDS.2021.007

# 5. Technology assessment

Clearly, going by what has been discussed above, there are evidently digital technological competences in Zambia on the part of both the state and civil society. However, what is still unclear is the available capability in terms of CSOs' and individuals' abilities to monitor and analyse the effectiveness of their own digital-level campaigns, including hashtags. It is also unclear to the authors to what extent CSOs are able to monitor the secretive activities of the state and those of other powerful politicians.

However, what also emerges is that the Zambian government has the capacity to censor content on the internet, as was done between July 2013 and April 2014 when four online media outlets – Zambian Watchdog, Zambia Reports, Barotse Post and Radio Barotse – were blocked for critical coverage of the government (OONI 2016). According to a study conducted by the Centre for Intellectual Property and Information Technology Law (CIPIT) at Strathmore University in Kenya and the Open Observatory of Network Interference (OONI), DPI filtering tactics were used to block the Zambian Watchdog website. Moreover, during the CIPIT and OONI's 12-day test, it was found that at least ten different websites were 'consistently inaccessible' in Zambia immediately after the 2016 polls. These included dating sites for LGBTQI people; the website of the Organisation for American States, which promotes human rights in the Americas, and the World Economic Forum's website. Others were photo-sharing site Pinterest; and that of the World Zionist Organization, which campaigns for a Jewish homeland in Palestine (OONI 2016).

It is further argued that the Zambian government in 2019, arrested a group of bloggers who ran an opposition news site with the aid of a specialised cyber-surveillance unit located in ZICTA. The unit worked with the police to pinpoint the bloggers' locations and track their phones (Citizen Lab 2020).

Thus, as Zambia approaches the day of the general election in August 2021, there may be an upswing in state and other actors' actions in terms of disruption of online debates, cyber-surveillance of citizens online activities, blocking of critical websites and blogs, disinformation, misinformation or indeed influence-peddling exerted through fake news and other tricks. CSO activism will also substantially increase as CSOs lock horns with the government over control of civic spaces.

For now, it is perhaps important to reflect upon the impact that the emergence of the global Covid-19 pandemic has had on the human and digital rights landscape in Zambia. In doing so below, we reflect on some past health incidents, and how the state responded. The state's past responses echo current reactions in Zambia.

 DOI: 10.19088/IDS.2021.007

# 6. Digital rights landscape in times of Covid-19

Looking back, we are able to see that draconian force, closing civic space, and the circumvention of digital rights have not only been the mainstay of government reactions to the Covid-19 pandemic and other health emergencies, but that such state responses are nothing new in Zambia. They have happened many times before. The government has acted rashly in cholera outbreaks, during almost every other rainy season, and throughout other health emergencies. For instance, in 2018 the army was sent into one of Lusaka's high-density suburbs, Kanyama, to end protests after the forced closure of a market when cholera broke out in the area (Reuters 2018).

The rains fall in Zambia from the end of October to March the following year. During several such occasions, the army has been sent into the streets of the main towns, either to clean up the dirty parts or to enforce order, without the necessity of supportive legislation, or without the necessity of a declaration of a state of emergency. The same practice has been witnessed during the Covid-19 outbreak. A presidential statement is deemed adequate for such tough measures, which include the closure of civic spaces and the violation of human rights, although civil society groups have often objected to such expressions of state overreach.

The brutality exercised by the military during these clean-up activities – such as beating up people in all manner of ways, enforcing unregulated curfews in poorer and densely populated townships, and so on – openly violates human rights and limits civic spaces for citizens. Markets are closed, vendors who may have previously resisted local councils' directives to move off the streets are beaten or locked up, and/or forcibly chased out of business centres (districts) without being offered alternative trading places. As a result, their rights and sources of livelihood are blocked. Protests by civic actors are ignored by the government, as if the nation were under a state of emergency.

A good example of events that have impelled human rights violations happened in the early part of 2020. Unknown assailants attacked citizens in their residences at night with an unspecified gas. The public response came through vigilante mobs that killed suspects randomly across the country. This nationwide strife resulted in the government deploying troops to quell unrest (Bloomberg 2020). A few alleged masterminds were arrested but have yet to be brought before the courts. A few suspected perpetrators were released without charge.

 DOI: 10.19088/IDS.2021.007

Earlier, in 2017 and other previous years, cholera outbreaks were used as an excuse to curtail citizens' rights. Often, the army is sent into the streets to beat and torture vendors and other street sellers under the guise of cleaning up the cities (AFP 2017). Likewise, in 2017 a state of emergency was declared after a series of mysterious fires gutted markets in Lusaka and Copperbelt Province. The sources of those fires have not been identified. The same year, opposition leader Hakainde Hichilema was arrested and charged with treason for refusing to give way to a presidential motorcade. Before that, in 2016, there erupted sudden, but yet to be explained xenophobic violence against Rwandese residents in Zambia. All these incidents led to the evocation of emergency powers by the government. The government is seemingly not sparing when abusing these powers at the slightest excuse in a manner that has been referred to as a 'suspension of human rights approach', which in such circumstances is detrimental to democracy (Kayumba-Kalunga 2020).

In the case of the Covid-19 outbreak, Zambia may have witnessed what University of Zambia scholar Felicity Kayumba-Kalunga describes as 'executive disorder', as the government went about in an illegal, disorderly, and illegitimate fashion when faced with the new pandemic (*ibid.*). To critics, the state's response was not only a 'suspension of human rights approach', which included suspending freedom of association, but its actions were unconstitutional and unaccountable, especially with respect to the fundamental rights of citizens (*ibid.*).

The Covid-19 background is that Zambia recorded its first cases in March 2020 and since then the disease has spread to almost all parts of the country. By August 2020, there were more than 11,082 reported cases, which included 280 deaths, making it a 2.5 per cent death rate (Kasonde 2020). The government's response to the pandemic, which the state has referred to as the 'new normal', has been nothing short of draconian.

Without declaring the pandemic a national emergency, as required by law, the government proceeded to issue Statutory Instruments Numbers 21 and 22 of 2020, under the Public Health Act, which were followed by several presidential directives that were not backed by any written law.

Critics such as Lawrence Kasonde, a former LAZ president, and now heading civic organisation the Chapter One Foundation, have labelled the government's response to Covid-19 as being governed by political expediency and disrespect for human rights.

According to Kasonde, the most prominent victim of Covid-19 in Zambia has been the popular, privately owned Prime Television station, which on 9 April 2020 was shut down for refusing to broadcast advertisements and programmes on Covid-19 for free. The official reason for the closure was that the television station's licence had expired a month before.

 DOI: 10.19088/IDS.2021.007

Also, in June when a group of youths protested over unemployment and the lack of opportunities in an economy that was expected to shrink by 4.5 per cent in 2020, armed troops were sent into the Lusaka streets to stop the protest. However, the innovative youths went into the bush, about 150km east of the capital city, to stream their protest online, on various social media platforms, with an audience estimated at about 300,000 (*ibid.*).

Further, under the ostensible excuse of the spread of the pandemic, the government has used the Public Order Act to restrict public gatherings such as weddings and church meetings; and to curtail peaceful assemblies and freedom of association and expression. The law requires that gatherings of more than five people must be authorised by either the Ministry of Health or local government authorities.

However, in practice the above-mentioned laws and regulations have been applied selectively. They have not been used to stop political campaigns and other ruling party gatherings in preparation for the general election set for August 2021.

Nevertheless, in summary, this is what has happened since March 2020 when the first Covid-19 cases were detected in Zambia:

- Immediate and indefinite closure of all learning institutions throughout Zambia;
- Restriction of public gatherings, including funerals and religious services to not more than 50 people;
- Immediate closure of all social places, including bars and gyms, and reducing restaurants to takeaway facilities only;
- Lockdown of Kafue and Nakonde towns and restrictions on the movement of the people in and outside those two towns. Kafue is a small riverside town with about 50,000 people, while Nakonde and its environs, bordering Tanzania, host about 70,000 people. These measures directly affected more than 120,000 people in one swoop;
- Thereafter, the president in August 2020 decreed the mandatory wearing of face masks in all public places. Thus, the police were 'empowered' to stop public conveyance systems at any time and arrest people not wearing masks, fining them equivalent to US$40; or take them to court to face up to six months in prison. These measures were quickly abandoned when the state, under pressure from the LAZ, realised that there was no specific law backing them. However, shops and supermarkets have continued denying entry to people without face masks.

 DOI: 10.19088/IDS.2021.007

All these state actions are a demonstration of the narrowing of civic space under the pretext of the fear of the spread of Covid-19. In the meantime, the ruling PF party has taken advantage of these measures to print and widely distribute PF message-embroidered campaign masks in preparation for the 2021 general election. No opposition political party regalia, or masks, have been allowed on the streets by militarised PF political cadres (Lusaka Times 2020).

To enforce presidential directives, accompanied by government officials such as Lusaka Province minister Bowman Lusambo and Lusaka Mayor Miles Sampa, the police have raided, often at night, many privately owned premises including hair salons, restaurants, bars, Chinese factories and so on, closing them down, or whipping and beating up people found there, or in the vicinity. The have also stopped buses and harassed passengers. This has been done without any legal backing at all (Zambian Eye 2020).

However, there has been a degree of easing of some of these measures in recent weeks. For example, suspected public state beatings have eased, and the lockdowns in Kafue and Nakonde were lifted after a few days: schools and other learning institutions have partially reopened, but bars, stadiums, gyms and other such places remain closed. In the main, though, the measures remain in place.

 DOI: 10.19088/IDS.2021.007

# 7. Discussion, conclusions and recommendations

From the above, what we see is a government that has taken advantage of a combination of factors to entrench itself and to narrow civic space. These factors pre-existed or have freshly presented themselves to the state.

Such factors include old pre-colonial laws that are still on the statute book; and the existence of a weakened civil society movement, a movement enfeebled by laws such as the NGO Act, the Public Order Act and all the subsidiary statutory instruments that have been enacted since the arrival of Covid-19.

On the other side, there has been evident concern with the growing activism of civil society groups, especially youths and the clergy, as discussed above. This activism, seemingly, has pushed back the boundaries of civic space in Zambia. An expanded civic space necessitates a sapped state. The problem is in maintaining a reasonable balance to the satisfaction of the two competing sides.

Instead, what has been observed has been that the state, which is the stronger of the two forces, has pushed hardest and almost deformed the breathing space for CSOs by fiat and through other actions or instruments. Moreover, the state has tampered with the digital rights of its people in several ways, including surveillance, arrests and the banning of publications.

With the arrival of Covid-19, as was seen during cholera outbreaks, and other emergencies such as xenophobic attacks on Rwandan refugees, the destruction of town market centres, or unexplained vigilante mob violence, the pandemic has provided a new platform for the state to further justify its actions against civic actors.

As argued above, civic space and human rights are intertwined, between themselves and with digital rights. These three parts essentially cannot be prised apart. When one of them is under attack – when the state closes civic spaces, violates human rights and suppresses digital citizenship – the others suffer. It is therefore imperative that ways are found to sustain the viability of the three factors and interested CSOs against alleged state assaults.

As shown above, through the discussions of digital space and other related events surrounding civic activism, the figures seem to suggest that the number of digital citizens in Zambia has exponentially increased. These are people with the knowledge and skills to effectively use digital technologies to communicate with others, define their social spaces, and to confidently

 DOI: 10.19088/IDS.2021.007

participate in social affairs, competently, while creating digital content and using technologies (DTHub 2020).

From the foregoing, it is recommended that a number of things be done by NGOs, civil society groups, international actors, the government and other interested parties in responsibly responding to emergent situations. These actions include that:

- Zambian CSOs/NGOs should be linked to similarly inclined social movements across the continent and in Africa, as the ADRN is trying to do;
- African research institutes, higher-learning institutions and other similarly inclined organisations should embark on further research into the socio-political dynamics that are taking place in Zambia;
- Zambian CSOs should be equipped with the skills and technologies necessary for the systematic monitoring of state and other powerful elements' activities; and
- The ADRN should work towards redefining the manifestations or characteristics and meanings of digital citizenship and digital politics in Zambia today.

 DOI: 10.19088/IDS.2021.007

# References

AFP (2017) **'Zambia Deploys Army to Battle Cholera After 41 Deaths'**, 30 December (accessed 30 November 2020)

Bloomberg (2020) **'Zambia Deploys Army to Quell Riots After Criminal Attacks'**, 13 February (accessed 28 November 2020)

Bloomberg (2019) **'China's Digital Silk Road is Looking More Like an Iron Curtain'**, 10 January (accessed 16 August 2020)

Bloomberg (2011) **'Zambia's Cabinet Appointed by President Michael Sata'**, 29 September (accessed 16 August 2020)

Carnegie (2020) ***AI Global Surveillance (AIGS) Index Report*** (accessed 16 August 2020)

Chakwe, M. (2020) **'Current NGO Bill Contravenes Constitution – ZCSD'**, *The Mast Online*, 4 July (accessed 16 August 2020)

Chinyere, R. and Hamauswa, S. (2016) 'A Critique of the Constitutional History of Zambia', in R. Mukwena and F. Sumaili (eds), *Zambia at Fifty Years*, Kabwe: Partridge Publishing

Citizen Lab (2020) **'Running in Circles Uncovering the Clients of Cyberespionage Firm Circles'**, 1 December (accessed 2 December 2020)

CIVICUS (2017) **'Zambia Overview'**, Monitor Tracking Civic Space (accessed 3 July 2020)

DTHub (2020) ***Digital Citizenship*** (accessed 3 July 2020)

ECZ (2020) ***2016 Presidential Election***, Electoral Commission of Zambia (accessed 3 July 2020)

Freedom House (2019a) ***Freedom in the World*** (accessed 4 December 2020)

Freedom House (2019b) **'Zambia'**, *Freedom in the World* (accessed 28 August 2020)

Hutt (2020) **'What Are Your Digital Rights?'**, 13 November (accessed 28 August 2020)

IDS (2020) ***African Digital Rights Network***, Brighton: Institute of Development Studies (IDS) (accessed 24 August 2020)

IWS (2020) ***Internet Users Statistics for Africa***, Internet World Stats (IWS) (accessed 5 July 2020)

Kasonde, L. (2020) **'Covid-19, Human Rights and Zambia's "New Normal"'**, *Daily Maverick*, 21 August (accessed 23 August 2020)

Kayumba-Kalunga, F. (2020) ***Executive Disorder, Constitutionalism and COVID-19 in Zambia***, African Network of Constitutional Lawyers, 2 May (accessed 3 July 2020)

Lusaka Times (2020) **'Zambia : Presidential Empowerment Initiative Fund distributes PF regalia for to tailors for the Face mask Initiative Project'**, 16 May (accessed 25 January 2021)

Malena, C. (2015) ***Improving the Measurement of Civic Space***, London: Transparency and Accountability Initiative (accessed 28 August 2020)

MTN (2020) ***SIM Registration*** (accessed 8 January 2021)

Mukwita, A. (2017) *Against All Odds*, Partridge Publishing

News Diggers (2020) **'IBA Says It Has Powers to Regulate Online Broadcasting'**, 8 August (accessed 16 August 2020)

News Diggers (2019) **'Govt Forms "Special Joint Cyber Crime Crack Squad"'**, 4 February (accessed 26 November 2020)

OONI (2016) **'Zambia: Internet Censorship During the 2016 General Elections?'**, *Open Observatory of Network Interference*, 11 October (accessed 05 July 2020)

Paradigm Initiative (2020) ***Paradigm Initiative*** (accessed 5 July 2020)

PMRC (2016) ***PMRC Policy Analysis of the Non-Governmental Organisations' Act No.16 of 2009***, Lusaka: Policy Monitoring and Research Centre (accessed 24 August 2020)

 DOI: 10.19088/IDS.2021.007

Reuters (2018) **'Zambian Army Part of Cholera Controls'**, *Defenceweb*, 15 January (accessed 28 November 2020)

Sardanis, A. (2014) *Zambia: The First Fifty Years*, London: I.B. Taurus

Scott, G. (2019) *Adventures in Zambian Politics: A Story in Black and White*, London: Lynne Rienner

Stratfor (2019) **'Huawei May Be Helping Governments in Africa Boost Their Power to Spy'**, 2 September (accessed 26 November 2020)

Techzim (2016) **'Zambian Government Suspected of Causing Internet Shutdown Following Outage in Opposition Strongholds'**, 18 August (accessed 25 January 2021)

The Mast (2020) **'Lungu Fires Mabumba'**, 29 July (accessed 25 November 2020)

The Zambian Observer (2020) **'David Mabumba Has Sued Spring TV for Broadcasting that He Has Committed Suicide'**, 30 July (accessed 25 November 2020)

Weber, V. (2020) ***The Worldwide Web of Chinese and Russian Information Controls***, Open Technology Fund (accessed 16 August 2020)

Zambia Reports (2013) **'Zambia: The Catholic's Pastoral Letter'**, 28 January (accessed 3 July 2020)

Zambia Reports (2012a) **'Sata Clarifies Protocol, Elevating PF Secretary General to #2'**, 24 April (accessed 25 November 2020)

Zambia Reports (2012b) **'President Sata's U-turn on Public Order Act'**, 10 October (accessed 25 November 2020)

Zambia Today (2020) **'Southern Province in Internet Network Shut Down'** (accessed 26 November 2020)

Zambian Eye (2020) **'Lusambo Violates Article 15 of the Bill of Rights by Beating People – CiSCA'**, 23 April (accessed 30 November 2020)

Zambian Watchdog (2015) **'PF Resolves to Beat Opposition Supporters in Markets'** (accessed 11 February 2021)

Zambian Watchdog (2013) **'Sata Signs Order for OP to Tap Phones, Emails'**, March (accessed 26 November 2020)

Zambian Watchdog (2012) **'I Now Love the Public Order Act, Won't Repeal It – Sata'**, 6 October (accessed 25 November 2020)

ZCSD (2020) 'Zodiac Civic Space Monitoring Report May – 2020', unpublished report, Zambia Council for Social Development

ZICTA (2020) *2018 National Survey on Access and Usage of Information and Communication Technologies by Households and Individuals*, Lusaka: Zambia Information and Communications Technology Authority

ZIS (1991) 'Zambia in Brief', Lusaka: Zambia Information Services

ZNBC (2020) **'Kitwe Man Nabbed for Defaming President Lungu'**, Zambia National Broadcasting Corporation, 24 November (accessed 8 January 2021)

# Uganda Digital Rights Landscape Report

Juliet Nanfuka



This report is part of 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries'; the Introduction is also recommended reading.

© 2021 Juliet Nanfuka © Institute of Development Studies. DOI: 10.19088/IDS.2021.008

# 1. Introduction

Over the past two decades, the civic landscape in Africa has gone through a plethora of changes that have shaped its impact, influence and perceptions in ways both positive and negative. These have run parallel to increased awareness about human rights, as well as the growth in availability of and reliance on information and communication technology (ICT).

The aim of this report is to improve understanding of the political and technological landscapes as they have shaped openings and closings of civic space in Uganda and how these have affected citizens' digital rights. The report will describe the main contours of the dynamic political, civic and technological landscapes. It will then conclude with recommendations for practice, policy and further research that the author believes is necessary in order to enable citizens and civil society organisations to more effectively open civic space and exercise, defend and expand digital rights.

In the following sections, the evolution of the relationship between civic space, its related actors and digital rights is presented.

 DOI: 10.19088/IDS.2021.008

# 2. Political landscape

As of 2019, Uganda was ranked 99th (of 165 countries) by the Economist Intelligence Unit on its democracy index. It also describes the country as a hybrid regime due to its authoritarian tendencies, despite democratic rules in place. Since the civil war of the 1980s, the country has not experienced particularly extreme political volatility, even though political tensions have been present for an extended period of time.

Since 1986, the National Resistance Movement (NRM) has been the ruling party under the leadership of President Yoweri Museveni. In recent years, various amendments have been made to the Constitution that have enabled Museveni's protracted stay in office.

In 2005, the Parliament of Uganda voted to lift presidential term limits (Lacey 2005) through an amendment of the Constitution. This move allowed Museveni to seek a third term in the elections of 2006; the same year also marked the first elections under a multiparty system (Makara *et al.* 2005). Taking a similar stance, in 2019 the Constitutional Court upheld an amendment that would allow Museveni (at the time 73 years old) to seek another term in office, including the freedom to contest the presidency indefinitely after the 2021 elections and past the age of 75 (Al Jazeera 2018). The 1995 Constitution prohibited anyone younger than 35 or older than 75 from serving as president.

These actions have been used by a number of opposition actors and pressure groups against the president and the ruling party, arguing that the state is autocratic, monopolistic and authoritarian. Further to this, they have continuously alleged that the first presidential election held in 1996 was rigged (Nalumansi 2016).

Among the main political parties in the country are the Forum for Democratic Change (FDC), which grew out of the NRM and is the largest opposition party, through which Dr Kizza Besigye has challenged for the presidency on four separate occasions since 2001. With no success at any of the elections, Dr Besigye has raised accusations of rigging by the president – on two occasions (in 2001 and 2006), taking the matter to the Supreme Court. On both occasions, there was a unanimous ruling that acknowledged there had been widespread rigging but that it had not been enough to warrant the reversal of the final result. Dr Besigye will not stand in the 2021 presidential race (Draku 2020).

Other long-term key opposition parties include the Democratic Party, the Uganda People's Congress and a more recent entrant, as of 2019, the Alliance for National Transformation, which was launched by a former FDC leader,

 DOI: 10.19088/IDS.2021.008

General Mugisha Muntu. Meanwhile, the National Unity Platform, a pressure group led by Member of Parliament (MP) Robert Kyaluganyi Ssentamu (also known as 'Bobi Wine'), has gained momentum in response to Museveni's plans to extend his 31-year term (Bariyo 2017) and has been particularly critical of the ruling party and its leaders.

Various laws have been introduced that have enabled the curtailing of critical voices, and the work of civic actors and the media, in addition to also affecting key rights such as access to information and freedom of expression. These laws have been introduced despite the 1995 Constitution, which states in Article 29(1)(a) that 'every person shall have the right to freedom of expression and speech which includes freedom of the press and other media' (ILO 1995).

Over the years, more laws and regulations have been introduced that largely protect the political interests of the ruling party and the president more than those of citizens. Coupled with an increased use of technology to underpin these developments, concerns over data protection, surveillance, digital inclusion and self-censorship have come to shape the political relationship between citizens, civic actors, the media and the state.

The International Center for Not-for-Profit Law (ICNL) notes that the legal framework for civil society in Uganda is generally supportive of civil society organisations, but only insofar as their sphere of activity is politically and socially acceptable to the government (ICNL 2020).

 DOI: 10.19088/IDS.2021.008

# 3. Civic space landscape

## 3.1 The early years: 2000–10

Aided by the 1995 Constitution, during this decade, civic space and actors were establishing themselves, seeking out niche areas of focus, often in the traditional human rights sphere. Among the highlights of these early years was the introduction of the Access to Information Act, 2005. However, its potential to support civic space has largely remained underutilised. Nonetheless, the act was used successfully by journalists in 2015 when a chief magistrate's court ruled in their favour against the National Forestry Authority, which had denied them access to information related to a World Bank grant (Mugagura 2015).

The first multiparty elections in 2006 marked the emergence of civil society with an interest in 'mobilising and facilitating citizen participation in political, economic and social processes aimed at promoting transparency and accountability in governance' (Mugisha, Kiranda and Mbate 2019). While civil society had often worked on issues of social concern, increasingly they were beginning to challenge state actions and inaction – often critically.

It was during this period after the 2006 elections that civil society organisations evolved to include rights-based and political issues in their work. Growing concerns over state actions contributed to rising civic concern and public outcry, which started emerging during the mid-2000s. Among these was the 2007 civic reaction against the state sale of part of the Mabira Forest to a private entity to expand its cane plantation (Kavuma 2011). In the years that followed, restrictions increased on assemblies led by political opposition members (United States Department of State 2008) – including of Dr Besigye, whose spate of repeated arrests by the state started during this period.

## 3.2 A wave of new laws: 2010–20

On 11 July 2010, Somalia-based militant Islamist group Al-Shabaab claimed responsibility for bomb attacks during the screening of the FIFA World Cup final at two separate venues in the capital Kampala. This resulted in more restrictive measures being written into law; for example, the Regulation of Interception of Communications Act, which served to reinforce the Anti-Terrorism Act of 2002, which had been introduced following the terrorist attacks in the United States on 11 September 2001.

 DOI: 10.19088/IDS.2021.008

In 2011, the second presidential election was held, which granted Museveni another term following a highly contested win. However, during this time more open public protest took place, aided by online platforms, such as the Walk to Work campaign against rising food and fuel prices. These public protests also resulted in the arrests of campaigners and members of opposition parties (Namiti 2011).

This saw the introduction of the bill for the Public Order Management Act (POMA) in Parliament in 2011. The bill was signed into law two years later on 2 October 2013. POMA sought to 'provide for the regulation of public meetings; to provide for the duties and responsibilities of the police, organisers and participants in relation to public meetings; to prescribe measures for safeguarding public order; and for related matters' (ULII 2013: 5). The act in effect also handed the police the power to regulate public meetings, including the power to prevent the holding of meetings and stop meetings already in progress.

Since its introduction, POMA has been used on numerous occasions against civil society, the media and members of the opposition. The lesbian, gay, bisexual, transgender and intersex (LGBTI) community has largely remained unable to organise publicly, while opposition actors have also faced restrictions. It is interesting to note that ahead of the 2021 elections, on 26 March 2020, the Constitutional Court annulled POMA and also declared all acts done under the law null and void. The court ruled that the law was inconsistent with the country's Constitution (Chapter Four 2020).

However, the Covid-19 pandemic has provided the excuse for the state to limit assemblies and public gatherings (Macdonald and Owor 2020) initiated by the opposition, despite the ruling party attracting large crowds at its own campaigns (Kizza 2020). This has raised concerns over the extent to which civic space will be utilised – or restricted – in the lead up to the 2021 elections.

Political issues were among those highlighted in a 2012 report by Human Rights Watch. It noted that evidence-based research and civil society organisations with an advocacy focus on controversial issues in the Uganda context – such as transparency in the oil sector; compensation and reparations for land acquisitions and sales; political and legal reform; and protection of human rights, including the rights of LGBTI people – had experienced decreasing room to manoeuvre (HRW 2012).

Meanwhile, religion, education, tribal affiliations, proximity to wealth and even gender have also had an influence on civic space and how civic actors are politically perceived and positioned in mainstream narratives online and offline. These differences have even been used in political power plays, such

as during the 2014 controversy around the Anti-Homosexuality Bill where religion was used against civic actors advocating against the bill, but was also used as the political moral high ground, which worked in favour of those seeking political seats in the 2016 elections (Amnesty International 2014).

The topic of corruption is one that civil society and the media have treated with particular scrutiny over the years due to the vast amounts of aid funding the country receives, but with limited transparency and accountability over its use – regardless of the presence of the Access to Information Act.

In 2012, international donors withheld aid following allegations of embezzlement of donor funds amounting to US$12.7m by the Office of the Prime Minister (Al Jazeera 2012). This act saw the government unable to pay the salaries of public service workers such as police and teachers. In response to rampant corruption, civil society organised the Black Monday Movement (BMM) – due to the movement leaders encouraging the wearing of black clothes on Mondays (Mujuni 2013). This served as one of the key early campaigns by civil society that started gaining traction in online spaces. It aimed to work against the theft of public money by government (Uganda National NGO Forum 2013).

In the months that followed the establishment of BMM, the movement's efforts were thwarted by police including through unwarranted arrests for 'inciting violence' (HRNJ – Uganda 2013; IFEX 2013). Actions such as those taken against BMM by the state served to influence other civic actors in the long run. The charge of 'inciting violence' is one that has remained in common use, including against political activists such as social justice activist Dr Stella Nyanzi and Bobi Wine, as well as journalists and civil society activists (HRW 2014).

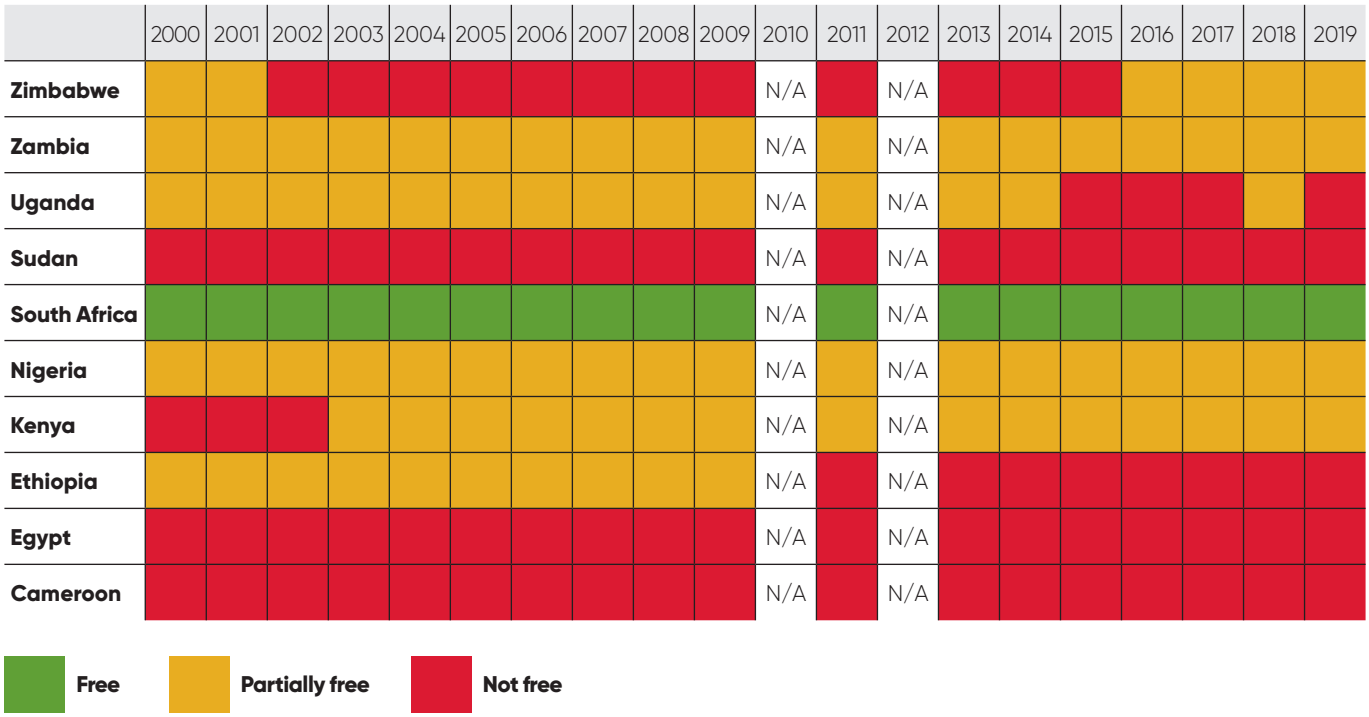
In 2013, the Non-Governmental Organisations Registration (Amendment) Bill was introduced, which sought to amend the NGO Act. The bill aimed to limit the work and activities of NGOs and called for changes in the processes for registering with authorities. It also appeared to be a deliberate move by the government towards the control of NGO and civic activities (Article19 2015).

According to Amnesty International, by 2014 some organisations had stopped working, scaled back on activities or significantly changed their work on 'sensitive' content areas due to continued targeting by the authorities. Meanwhile, self-censorship due to fear of closure also became a key issue among human rights organisations (Amnesty International 2014).

It was around this time that Uganda's position in Freedom House's (2019) Freedom Index began to descend from 'partially free' to 'not free' (see Figure 3.1).

 DOI: 10.19088/IDS.2021.008

## Figure 3.1 Freedom House ranking for ADRN countries, 2000–19[1]




*Note:* ADRN – African Digital Rights Network.

*Source:* Adapted from Freedom House (2019)

As such, these actions appeared to be increasingly shrinking civic space at a time when there was increasing public interest in political affairs, service delivery and state transparency, coupled with rising internet penetration and growing numbers of citizen journalists.

In 2014, several controversial laws were introduced that had implications for both civic and online spaces. Among these was the Anti-Pornography Act of 2014. The law fuelled a negative narrative against women, in particular, and went on to be used against women who fell victim to revenge pornography and had their nude images published or shared online without their consent (African Feminism 2020). The law also provided for the establishment of a Pornography Control Committee. In 2017, a nine-member committee was announced, accompanied with a budget of $516,000 per year (Gitta 2017) illustrating the state's commitment towards the work of the committee.

Upon the introduction of the Anti-Homosexuality Bill, a Minority Report arguing that the bill was discriminatory and that homosexuality was prohibited under existing laws was presented by opposing parliamentarians

1 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.008

(Parliament of the Republic of Uganda 2012). However, although President Museveni expressed concern about the Anti-Homosexuality Bill, it was signed into law on 24 February 2014 and gazetted on 10 March 2014 (New Vision 2014). This led to a petition being filed by civil society on the constitutionality of the act. A few months later, in August 2014, the act was declared null and void by the Constitutional Court, on the grounds that there was no quorum in court when it was passed (FIDH 2014).

However, the increased national narrative around anti-homosexuality laws fuelled further stigmatisation of the LGBTI community and exposed civic actors in the space to even further homophobic backlash. Organisations working on sexual minority rights, in addition to general civic organisations, became the targets of office break-ins. Unknown parties reportedly took computing equipment and other electronic devices. Police responded with limited investigations and the prevalence of these raids continue to pose a threat to the privacy of information held by civic organisations (CIPESA 2019).

Uganda passed the controversial Non-Governmental Organisation Bill in 2016, which sought to govern the activities of civil society. This marked a new era of concerns, especially for entities dealing with contentious issues such as sexual rights, abortion advocacy, politics, transparency and land grabbing (Paulat 2015).

In 2017, the might of civic actors and social media users in Uganda came into the spotlight through the #FreeStellaNyanzi campaign, which also gained international following. It sought the release of Dr Stella Nyanzi, who had protested against poor service delivery by the state (Kelly *et al.* 2017). Dr Nyanzi was detained in April 2017 and charged with 'cyber harassment' for her use of Facebook to criticise the president and his wife Janet Museveni for their poor service delivery (Al Jazeera 2017).

The Ugandan feminists' voice online has also grown despite the continued pushback against it through trolling and cyber harassment (CIPESA 2020). In 2018, the state attempted to frustrate efforts by women who wanted to march in protest against the threat of continued violence against women. A march eventually took place in July 2018 (Sadurni 2018).

Some hope, and indeed protection for civic space and its actors, emerged in 2020 with the Human Rights Defenders Protection Bill. In July, a motion was passed for MP Komakech Lyandro to go ahead with the development of the bill (Kivumbi 2020).

 DOI: 10.19088/IDS.2021.008

# Table 3.1 Civic space timeline

| Year | Shift | Implication |
|---|---|---|
| **2002** | Anti-Terrorism Act. | Exposes civic actors and the media to interception and intrusion on an undefined basis. |
| **2005** | Access to Information Act. | Civic actors and media can request state information more freely. |
| **2006** | President Museveni, leading the NRM, wins first multiparty elections. | Draws more civic actors into political discourse, and promotes public political discourse and participation. |
| **2007** | Civil society saves Mabira Forest. | Civil society advocates against state-enabled deforestation and wins. |
| **2009** | National Information Technology Authority Act. | The authority guides data collection and the policies shaping it. |
| **2010** | Regulation of Interception of Communications Act enacted, reinforcing Anti-Terrorism Act of 2002. | Communications of civic actors, critics of the state, opposition, etc. can now be more easily intercepted and surveiled. |
| **2011** | Public Order Management Act (POMA) introduced in Parliament in 2011 (signed into law two years later, on 2 October 2013). | POMA presents direct state control of civic space including over rights of association and assembly. |
| **2012** | Black Monday Movement (BMM) aims to work against government theft of public money. | BMM is one of the key early civil society campaigns that starts gaining traction in online spaces. |
| **2012** | State interest in purchasing digital communications interception equipment. | Likely targets of interception include state critics, civic actors, journalists and opposition members. |
| **2013** | Non-Governmental Organisations Registration (Amendment) Bill. | Potential to restrict the work of civic actors. |
| **2014** | Data Protection and Privacy Bill is drafted; Anti-Homosexuality Bill 2014 is assented to, but a few months later the Constitutional Court rules it invalid due to lack of quorum. | One of the few bills released for public commentary; civic actors point out gaps in the proposed law that expose individuals and organisations working on LGBTI issues to both state and non-state initiated violence. |
| **2016** | Non-Governmental Organisation Bill. | Affront to civic actors, especially those dealing with contentious issues such as sexual rights, abortion advocacy, politics, transparency and land grabbing. |
| **2017** | #FreeStellaNyanzi. | Amasses local and international following on social justice concerns. |
| **2020** | Constitutional Court annuls POMA and declares all acts done under the law null and void; announcement that Human Rights Defenders Protection Bill is to be developed. | Potential respite for the civic space and actors. |

*Source:* Author's own.

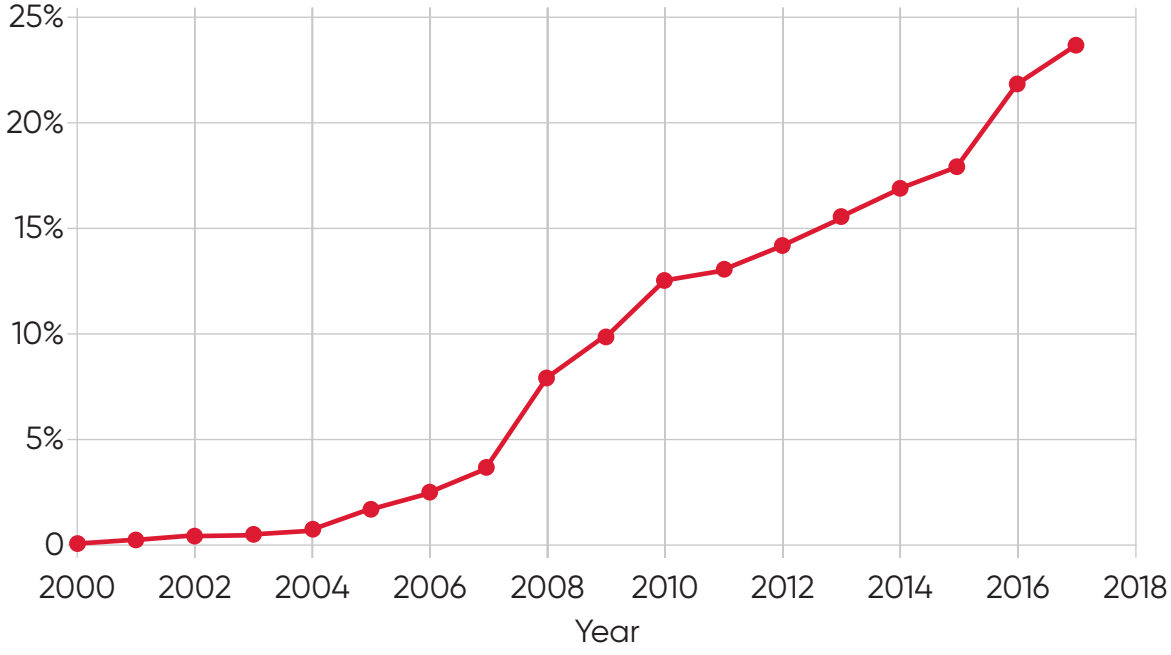
 DOI: 10.19088/IDS.2021.008

# 4. Technology landscape

## 4.1 The early days

At the turn of the century, Uganda had an internet penetration of 0.2 per cent, showing its infancy at the time. There were limited national frameworks directly pertaining to internet infrastructure, regulations and use. However, usage was steadily growing and by 2005, internet penetration stood at 1.5 per cent. More media houses had started generating online content and so had independent individuals and entities, some of whom were very critical of the state. The government regulatory body, the Uganda Communications Commission (UCC), had been established in 1995 and in early 2003 set up the Rural Communications Development Fund, which sought to develop communications infrastructure beyond the country's urban centres and enable last-mile access. Internet penetration has increased substantially since the early days; at the end of June 2020, internet penetration stood at 46 internet connections for every 100 Ugandans, according to the Uganda Communications Commission (UCC 2020).

### Figure 4.1 Percentage of the population with internet access in Uganda




*Source:* Based on data from ITU (2020)

 DOI: 10.19088/IDS.2021.008

## 4.2 The dawn of digital restrictions

In 2006, the government ordered internet service providers (ISPs) to block access to a website that published anti-government stories, radiokatwe.com. It accused the website of publishing 'malicious and false information against the ruling party NRM and its presidential candidate' (CPJ 2006). This happened in the same year that the first multiparty elections were held in Uganda.

The practice of blocking or closing media houses would become a common form of censorship, often in the guise of maintaining public order or preventing incitement of violence. Often, it served to drown out criticism of the state. In 2009, the state closed (the now defunct) Broadcasting Council of four radio stations, which were accused of fanning ethnic tensions (Eastern Africa Journalists Association 2009). These actions contributed to self-censorship by journalists and ordinary citizens alike on digital platforms.

In response to the 2010 Al-Shabaab bombings in Kampala, and in the support of the 'national security' argument often cited by the state, in 2011 the Computer Misuse Act, the Electronic Signatures Act and the Electronic Transactions Act were signed into law with no process of public consultation. These have been used against civil society actors, as well as critics of the state.

In 2011, the second presidential election was held. During that year, the regulations accompanying the Access to Information Act of 2005 were introduced. However, despite this progressive law, the 1964 Official Secrets Act continued to be cited as the basis for not disclosing information that should be in the public domain, including through open access platforms (e.g. www.askyourgov.ug). Thus, the work of civil society has continued to be undermined due to limited access to information, despite the presence of this law aimed at promoting transparency and accountability of state organs (Kyogabirwe 2017).

Some early social media campaigns were tightly linked to shrinking civic space and social justice concerns, such as the 2011 #WalkToWork protest and campaign (Oola 2011), which were in response to rising fuel and food prices. Meanwhile, the state also recognised the engaging nature of social media. ISPs temporarily blocked access to Facebook and Twitter for 24 hours following the #WalkToWork protests. Earlier in the year, the state had issued a directive to telecoms companies to block and regulate text messages that could 'instigate hatred, violence and unrest' during the presidential election period (Echwalu 2011). However, this was also seen as a move to stifle communications.

In 2012, the #AskThePM hashtag campaign aimed to provide a platform for the then prime minister, Amama Mbabazi, to engage with Twitter users more immediately and directly. This campaign tried to address the public image of the Office of the Prime Minister, which had been accused of embezzling US$12.7m with disastrous consequences for public service delivery and infrastructure.

Meanwhile, in July 2012, according to a ministerial policy statement the Office of the

 DOI: 10.19088/IDS.2021.008

President was looking for funds to purchase equipment that would enable interception of communications (Kiggundu 2012). The government's interest in intercepting communications raised concern among civil society actors and the media.

In 2013, the Uganda Communications Act was introduced. It enabled the communications regulator to 'monitor, inspect, license, supervise, control, and regulate communications services' and to 'monitor, and enforce compliance relating to content' (Freedom House 2016). By 2013, the state announced that it would monitor social media users, 'who are bent to cause a security threat to the nation' (CIPESA 2013), reigniting language used upon the introduction of the 2002 Anti-Terrorism Act and the Regulation of Interception of Communications Act of 2010. Both acts had elevated the surveillance powers of the state, reinforcing a culture of self-censorship online and raising surveillance concerns among civil society. The 2014 call for public commentary on the Data Protection and Privacy Bill did little to alleviate surveillance concerns.

In 2013, two newspaper outlets were closed following allegations of the distribution of a letter detailing an alleged assassination plot of officials opposed to the president. This led to a widespread campaign for press freedom (Natabaalo 2013). The hashtags #MonitorSiege and #RedPepperSiege were used to generate awareness and to challenge the state's actions. The media houses were re-opened after 11 days.

In 2015, amendments were made to the Anti-Terrorism Act of 2002 to align the law with international requirements by providing for aspects of terror financing and money laundering. Police were consequently granted the power to conduct surveillance of online transactions with the aim of establishing the sources of funding of terrorism activities. In the same year, the crackdown on commentators who relied on social media had already begun, with voices critical of the ruling party and independent media being curtailed. This was often in the guise of promoting public order and unity, as well as preventing the spread of false information, but damaged open dialogue on elections, including by hampering free speech. Among these was the arrest of state critic Robert Shaka on allegations of being behind the pseudonym Tom Voltaire Okwalinga; and, under Section 25 of the Computer Misuse Act, on charges of using computers and other electronic devices to issue 'offensive communication' (NITA 2011). There is no evidence to suggest that Shaka was responsible.

Mass surveillance concerns were also heightened in 2015, following reports that Uganda had procured Remote Control System (RCS), a product developed by the Hacking Team (an Italian company that sells intrusion and surveillance technology), which enables access to major operating systems and mobile platforms (Frenkel 2015).

In February 2016, the country held elections that in the lead-up had seen civic actors and opposition members face arrest and intimidation. These elections were the first time that social media platforms were aggressively used for campaigning

 DOI: 10.19088/IDS.2021.008

in the country. Amama Mbabazi took to YouTube to officially announce his intention to contest the presidential election. Not long after, Museveni released a video alleging Mbabazi aides were linked to sectarian content shared on WhatsApp (Aine 2015). Shortly thereafter, the authorities announced that a cybercrime unit had been established and its head appointed (Anena 2015). This alludes to the immediate measures often taken by the state in response to the use of new avenues for communication, especially by opposition or critical voices.

During the 2016 elections, Uganda hosted its first ever live televised presidential debates and provided an opportunity for citizens to scrutinise candidates' manifestos, including through the #UGDebates16 hashtag (interspersed with various other hashtags). However, on election day (18 February) social media and mobile money transactions in the country were shut down following a directive from the communications regulator to ISPs to disable all social media and mobile money services due to a 'threat to public order and safety' (CIPESA 2016). In May, a day before President Museveni was inaugurated for another five-year term, access to social media platforms including WhatsApp, Facebook and Twitter was again blocked (Nanfuka 2016).

In May 2018, the government passed the Excise Duty Amendment Act, which introduced an excise duty tax of 200 Ugandan shillings (US$0.05) per user per day for use of services such as WhatsApp, LinkedIn, Facebook and Twitter. This became commonly known as the 'social media tax'. The tax slashed the number of internet users in the country by five million within three months of its introduction (*ibid.*). In the same year, the state-run UCC called for all 'online data communication service providers, including online publishers, online news platforms, online radio and television operators' to apply and obtain authorisation from the commission (UCC 2018). This raised surveillance and censorship concerns across a broad spectrum of online users including bloggers, civic actors and media houses. In 2020, an October deadline was published.

With the introduction of more blatant mass surveillance, such as through CCTV cameras under Chinese telecoms company Huawei's 'Smart City' programme across Kampala, the potential for its misuse remains high (Woodhams 2020). In 2019, Huawei also was named in a *Wall Street Journal* exposé, which reported that staff in the Huawei Uganda office had helped police hack into the encrypted communications of an opposition figure and thus aided the security officers in foiling public mobilisation plans (Mwesigwa 2019).

Since then, online campaigns in support of social justice activist Dr Stella Nyanzi have gained global attention. Further campaigns in support of Bobi Wine also gained traction, with the #FreeStellaNyanzi and #FreeBobiWine often supporting each other. The campaign #SocialMediaTax (and related campaigns) also served to voice public discontent with the introduction of taxes on social media and mobile money transactions, and calls for their reversal. The state continues to disapprove of civic protest both online and offline.

 DOI: 10.19088/IDS.2021.008

# Table 4.1 Technology timeline

| Year | Shift | Implication |
|---|---|---|
| **2003** | Rural Communications Development Fund. | Aims to address last-mile connectivity. |
| **2006** | ISPs block access to radiokatwe.com. | Online censorship. |
| **2009** | State closes Broadcasting Council of four radio stations accused of fanning ethnic tensions. | Contributes to self-censorship online. |
| **2009** | National Information Technology Authority – Uganda is initiated. | Aims to coordinate and regulate information technology services in Uganda. |
| **2010** | Al-Shabaab bombings. | Sparks hasty release of cyber-related laws. |
| **2011** | Computer Misuse Act, Electronic Signatures Act and Electronic Transactions Act signed into law. | No process of public consultation; state granted excessive powers. |
| **2011** | SMS texts are regulated/blocked; ISPs temporarily block access to Facebook and Twitter for 24 hours. | Fears of an 'Arab Spring' are prevalent, leading to blocking of communications. |
| **2012** | Mandatory registration of SIM cards. | Concerns over data privacy and surveillance are heightened due to the amount of data citizens have to part with. |
| **2013** | Police shut down media houses for publishing/broadcasting a classified internal government letter, which allegedly contains the succession plans of the presidency. | The hashtags #MonitorSiege and #RedPepperSiege are used to create awareness and challenge the state's actions; media houses re-open after 11 days. |
| **2013** | Security minister announces that the government will start monitoring social media. | Promotes self-censorship among media, internet users and civic actors. |
| **2013** | Uganda Communications Act. | Threatens digital rights as it grants the state more power, with limited oversight mechanisms. |
| **2014** | Data Protection and Privacy Bill drafted. | Civic actors point out gaps in the bill. |
| **2015** | State procures Remote Control System. | Allows access to major systems and mobile networks. |
| **2018** | Social media tax introduced through Excise Duty Amendment Act. | Reduces online engagement, forcing some users offline. |
| **2018** | Online content regulations. | Potential for direct censorship. |
| **2019** | CCTV cameras installed across Kampala. | Raises concerns over monitoring and selective use of data. |
| **2020** | Deadline for registration as an online content producer. | Potential direct censorship, self-censorship and surveillance. |

*Source:* Author's own.

 DOI: 10.19088/IDS.2021.008

# 5. Conclusion

Uganda's civic and digital rights landscape has been shaped by a mixed bag of dynamics over the years. This has been due to the rushed release of laws; the surge in numbers of civic actors; a constantly evolving technological landscape, alongside the prioritisation of political interests over civic needs; and the abuse of state power.

Regressive laws have threatened the civic space, often being used selectively at critical times, such as in the lead-up to elections. Their presence remains a potential threat to the expansion of the work of civic actors. More recent shifts, such as the annulment of POMA and announcement of the development of the Human Rights Defenders Protection Bill, bring some hope of the easing of restrictions on civic space. Despite this positive step, the full potential for digital rights and online civic engagement to be realised remains weighed down by restrictions, which fuel self-censorship, impact affordability and enhance the perception of surveillance.

This report has demonstrated the potential that civic actors have to advance civic space and mobilise for digital rights. However, there remains a reactive nature as opposed to a proactive nature to this mobilisation, requiring more cohesion between the different actors (e.g. in the fields of tech, legal, policy and human rights). Often, gaps have been exploited to isolate groups (e.g. the LGBTI community) from more cohesive actions.

Civic space has adapted over the years, in line with state actions and laws. However, this has not kept civic actors safe from various forms of suppression tactics such as trumped-up charges, arrests, harassment, blocking of websites and intimidation aimed at stifling their work. Ultimately, the closing and opening of civic space is not uniform and does not affect everyone equally. Where some spaces are closed or more threatened (e.g. media and some civic actors, such as LGBTI groups), others remain less affected (e.g. the academic and research space may be less affected due to its proximity to mass public discourse and actions online and offline).

 DOI: 10.19088/IDS.2021.008

# 6. Recommendations

More state surveillance capacities call for more digital security and digital resilience skills and capacities for civic actors.

The shift towards more online interaction and engagement has created more opportunities for many retrogressive laws to be used. Thus, there is a need to more collectively organise civic actors on problematic clauses through an assortment of measures; for example, strategic litigation, online campaigns and evidence-based advocacy.

Given more sinister methods of information manipulation, such as online content regulation and social media taxation, it is fundamental to measure what narratives are lost when these avenues are used and the impact on digital rights.

Civic actors need to be more proactive in their measures to promote digital rights and protect civic space; for example, by working towards legislation that promotes digital inclusion and affordability in order for the government to comply with international human rights laws and norms.

 DOI: 10.19088/IDS.2021.008

# References

African Feminism (2020) ***Countering Nonconsensual Sharing of Intimate Images: How far do Uganda's Laws Go?***, CIPESA, 18 July (accessed 6 December)

Aine, K. (2015) **'Museveni Orders WhatsApp Audio Probe'**, *ChimpReports*, 30 May (accessed 20 October 2020)

Al Jazeera (2018) **'Uganda Enacts Law Ending Presidential Age Limits'**, 2 January (accessed 20 October 2020)

Al Jazeera (2017) **'Academic Stella Nyanzi Charged with "Cyber Harassment"'**, 10 April (accessed 7 December 2020)

Al Jazeera (2012) **'UK Suspends Uganda Aid over Corruption'**, 17 November (accessed 20 October 2020)

Amnesty International (2014) ***Rule by Law, Discriminatory Legislation and Legitimized Abuses in Uganda***, London: Amnesty International (accessed 20 October 2020)

Anena, H. (2015) **'Social Media Crime Crackdown. There's More to this Story'**, *African Centre for Media Excellence*, 22 June (accessed 19 August 2020)

Article19 (2015) ***NGO Bill would Restrict Civic Space*** (accessed 28 July 2020)

Bariyo, N. (2017) **'Ugandan President's Plan to Extend Rule Triggers Turmoil'**, *The Wall Street Journal*, 28 September (accessed 8 August 2020)

Chapter Four Uganda (2020) ***POMA: Uganda Court Annuls Public Order Law*** (accessed 15 August 2020)

CIPESA (2020) ***In Search of Safe Spaces Online: A Research Summary***, Collaboration on International ICT Policy for East and Southern Africa (accessed 10 August 2020)

CIPESA (2019) ***State of Internet Freedom in Africa 2018: Privacy and Personal Data Protection and Privacy: Challenges and Trends in Uganda*** (accessed 15 August 2020)

CIPESA (2016) **'Ugandans Turn to Proxies, VPNs in the Face of Social Media Shutdown'**, 18 February (accessed 24 September 2020)

CIPESA (2013) **'Uganda's Assurances on Social Media Monitoring Ring Hollow'**, 10 June (accessed 10 August 2020)

CPJ (2006) **'Critical Web Site Still Blocked on Eve of Presidential Election'**, *Committee to Protect Journalists*, 22 February (accessed 20 October 2020)

Draku, F. (2020) **'Besigye out of 2021 Election Race'**, *Daily Monitor*, 12 August (accessed 12 August 2020)

Eastern Africa Journalists Association (2009) **'Four Radio Stations Closed in Uganda'**, *Human Rights House Foundation*, 11 September (accessed 23 July 2020)

Echwalu, E. (2011) **'Ugandan Media Censored Over Walk to Work Protests'**, *Committee to Protect Journalists*, 19 April (accessed 8 December 2020)

FIDH (2014) **'Uganda: The Anti-Homosexuality Act Declared Illegal an Important First Step but Rights Protection must be Guaranteed'**, *International Federation for Human Rights* (FIDH), 6 August (accessed 23 September 2020)

Freedom House (2019) ***Freedom in the World*** (accessed 4 December 2020)

Freedom House (2016) ***Uganda: Freedom on the Net 2016*** (accessed 8 December 2020)

Frenkel, S. (2015) **'These Two Companies are Helping Governments Spy on Their Citizens'**, *BuzzFeed News*, 24 August (accessed 7 August 2020)

Gitta, A. (2017) **'Uganda: Government Introduces Pornography Control Committee'**, *DW.com* (accessed 10 August 2020)

HRNJ – Uganda (2013) **'Civil Society Anti-Corruption Activists Arrested by Ugandan Police'**, 7 January, *Human Rights Network for Journalists* – Uganda (accessed 14 August 2020)

 DOI: 10.19088/IDS.2021.008

HRW (2014) ***World Report 2014: Uganda***, New York NY: Human Rights Watch (HRW) (accessed 7 September 2020)

HRW (2012) ***Curtailing Criticism: Intimidation and Obstruction of Civil Society in Uganda*** (accessed 20 August 2020)

ICNL (2020) **'Uganda'**, *Civic Freedom Monitor*, International Center for Not-for-Profit Law (accessed 14 August 2020)

IFEX (2013) **'Ugandan Anti-corruption Activists Arrested, Charged with Inciting Violence'**, 26 June (accessed 16 August 2020)

ILO (1995) ***Constitution of the Republic of Uganda, 1995***, International Labour Organization (accessed 8 August 2020)

ITU (2020) ***Internet Access Statistics***, International Telecommunication Union (accessed 4 December 2020)

Kavuma, R. (2011) **'Plan to Sacrifice Forest for Sugar Puts Economy before Ecosphere in Uganda'**, *The Guardian*, 22 August (accessed 6 October 2020)

Kelly, S. *et al.* (2017) ***Freedom on the Net 2017***, Freedom House (accessed 8 August 2020)

Kiggundu, E. (2012) **'Phone Tapping: Uganda Govt Seeks 200bn'**, *The Observer*, 13 July (accessed 7 December 2020)

Kivumbi, K. (2020) **'In the Works: Ugandan Human Rights Defenders Protection Bill'**, *RightsAfrica.com*, 3 September (accessed 3 September 2020)

Kizza, J. (2020) **'As It Happened: NRM Primary Elections 2020'**, *New Vision*, 28 July (accessed 3 September 2020)

Kyogabirwe, L. (2017) ***Access to Public Information in Uganda: Rhetoric or Reality?***, CIPESA, 13 October (accessed 20 July 2020)

Lacey, M. (2005) **'Uganda: Parliament Eliminates Term Limits'**, *New York Times*, 13 July (accessed 8 August 2020)

Macdonald, A. and Owor, A. (2020) ***Food Distribution and Corona-Politics in Uganda: The View from Kampala***, LSE blogs, 15 June (accessed 20 October 2020)

Makara, S.; Rakner, L. and Rwengabo, S. (2005) ***Administering Uganda's 2006 Multiparty Elections: The Role of the Electoral Commission***, Working Paper 2008: 5, Bergen: Christensen Michelsen Institute (accessed 8 August 2020)

Mugagura, R. (2015) **'Journalist Wins Landmark Access to Information Case'**, *African Centre for Media Excellence*, 17 February (accessed 6 October 2020)

Mugisha, M.; Kiranda, Y. and Mbate, M. (2019) **'Civil Society in Uganda: Broadening Understanding of Uganda's Civil Society Ecosystem and Identifying Pathways for Effective Engagement with Civil Society in the Development Process'**, *Reality Check 11*, Kampala: Konrad Adenauer Stiftung – Centre for Development Alternatives

Mujuni, R. (2013) **'Black Monday Movement at One Year'**, *Uganda Radio Network*, 2 December (accessed 24 September 2020)

Mwesigwa, D. (2019) **'Africa in the Crosshairs of New Disinformation and Surveillance Schemes That Undermine Democracy'**, *CIPESA*, 9 December (accessed 7 October 2020)

Nalumansi, R. (2016) **'Ugandans Find a Reason to Vote in Their Rigged Elections'**, *Open Society Foundations*, 27 July (accessed 8 August 2020)

Namiti, M. (2011) **'Uganda Walk-to-Work Protests Kick Up Dust'**, *Al Jazeera*, 28 April (accessed 28 August 2020)

Nanfuka, J. (2019) **'Social Media Tax Cuts Ugandan Internet Users by Five Million, Penetration Down From 47% to 35%'**, *CIPESA*, 31 January (accessed 26 September 2020)

Nanfuka, J. (2016) **'Uganda Again Blocks Social Media to Stifle Anti-Museveni Protests'**, *CIPESA*, 12 May (accessed 25 September 2020)

 DOI: 10.19088/IDS.2021.008

Natabaalo, G. (2013) **'Ugandan police shut down papers over "plot"'**, *Al Jazeera*, 26 May (accessed 8 December 2020)

New Vision (2014) **'Museveni Responds to Obama on Anti-Gay Bill'**, 21 February (accessed 14 August 2020)

NITA (2011) *Computer Misuse Act*, Kampala: National Information Technology Authority – Uganda

Oola, S. (2011) **'Uganda: Understanding the Walk to Work Protest'**, *Peace Insight*, 13 May (accessed 20 October 2020)

Parliament of the Republic of Uganda (2012) *Minority Report by Members of the Sectoral Committee on Legal and Parliamentary Affairs on the Anti-Homosexuality Bill*, 2009, Kampala: Parliament of the Republic of Uganda

Paulat, L. (2015) **'Ugandan Parliament Passes Controversial NGO Bill'**, VOA, 15 December (accessed 9 August 2020)

Sadurni, S. (2018) **'Women Activists Take to the Streets of Kampala to Demand more Police Action'**, *The World*, PRX, 3 August (accessed 13 September 2020)

UCC (2020) ***Market Performance Report 2Q20 (April–June 2020)***, Kampala: Uganda Communications Commission (UCC) (accessed 7 December 2020)

UCC (2018) ***Registration of Online Data Communication and Broadcast Service Providers***, Kampala: UCC (accessed 29 August 2020)

Uganda National NGO Forum (2013) **'The Black Monday Movement as Participatory Democracy with Self-Direction'**, 24 July (accessed 29 July 2020)

ULII (2013) ***Public Order Management Act, 2013***, Uganda Legal Information Institute (ULII) (accessed 28 August 2020)

United States Department of State (2008) ***2008 Country Reports on Human Rights Practices – Uganda***, Washington DC: Bureau of Democracy, Human Rights and Labor, United States Department of State (accessed 7 October 2020)

Woodhams, S. (2020) **'Huawei Says its Surveillance Tech will Keep African Cities Safe but Activists Worry it'll be Misused'**, *Quartz Africa,* 20 March (accessed 25 September 2020)

 DOI: 10.19088/IDS.2021.008

# Sudan Digital Rights Landscape Report

Abrar Mohamed Ali



This report is part of 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries'; the Introduction is also recommended reading.

© 2021 Abrar Mohamed Ali © Institute of Development Studies. DOI: 10.19088/IDS.2021.009

# 1. Introduction

The purpose of this report is to understand how the political and technological landscapes in Sudan have contributed to openings and closings of civic space that have impinged on citizens' ability to exercise, defend and expand their digital rights. Internet access in Sudan is improving, and digital technologies are increasingly crucial to the enjoyment of rights and livelihood improvements. However, the government has at times taken aggressive measures to limit internet freedom and close civic space.

The term 'digital rights' refers to an individual's ability to access, use and create digital media freely to exercise human rights, including the right to privacy, data protection and freedom of expression (Human Rights Council 2016). The term 'civic space' refers to the space that people use to communicate with each other freely in a specific political and social context. Civic space provides people with an environment in which they can openly share their interests and concerns, and influence and shape policymaking. Closing civic space can shrink social connections and communications, and deprive individuals of their basic digital rights (CIVICUS 2016).

Section 2 of this report discusses the political landscape in Sudan, and how the digital rights of the Sudanese people are affected by political and technological issues. It addresses the ruling party that has played a part in opening and closing civic space from 2000 to 2020. Section 3 discusses the civic space landscape in Sudan, which includes a timeline of the past 20 years, plotting key points of political contestation and change as they have affected the closing and opening of civic space. Section 4 is a timeline of the past 20 years that describes key events in the use of digital technologies to open and close civic space. Section 5 describes the digital rights landscape, which is an analysis of the previous section. Section 6 is the conclusion, which includes the findings of the report and also makes recommendations to improve digital rights in Sudan.

 DOI: 10.19088/IDS.2021.009

# 2. Political landscape

Many political parties have ruled over Sudan. Omar al-Bashir led Sudan from 1989 to 2019, the country's seventh president. Al-Bashir came to power in 1989 when he became brigadier general of the Sudanese Army. He led a military coup that was negotiated with rebels in the south of the country and overthrew the democratically elected government of Sadiq al-Mahdi. In 1992, al-Bashir founded the dominant National Congress Party. Southern and northern Sudan had been at war for more than two decades.

From 2005, Sudan was governed according to the Comprehensive Peace Agreement, which ended the conflict. According to the agreement, there would be an autonomous government for southern Sudan,[1] which would manage its own political and legislative issues. The secession of South Sudan played a critical role in inducing numerous economic shocks. The most critical and direct effect was the loss of oil-producing regions, which accounts for about 50 per cent of the Government of Sudan's revenue and some 95 per cent of its exports, which considerably affected the country's economic growth. These factors led to price inflation and have triggered sporadic protests since September 2013.

Al-Bashir was accused of crimes including what United States (US) Secretary of State Colin Powell described as genocide (US Department of State 2004), and war crimes in Sudan's Darfur region. In 2008, the International Criminal Court issued a warrant for his arrest. In 2010, another arrest warrant was issued on three separate counts of genocide. Thousands of people lost their lives during the Darfur conflict that occurred in February 2013 as the government's Rapid Support Forces (RSF) moved against the Sudanese Liberation Movement and the Justice and Equality Movement.[2] After that incident, although the Government of Sudan took action against those accused of being involved in the conflict and arrested many people, they restricted citizens from putting human rights-related issues on the internet.

From December 2018 onwards, there were massive protests against al-Bashir all over the country. On 11 April 2019, the al-Bashir government was convicted by the Sudanese military of corruption and replaced by the Transitional Military Council (TMC). From 3 June 2019 to 9 July 2019 the internet was shut down amid a violent military crackdown that on 3 June led to the deaths of 100, with 700 injured and 70 rape victims (Taye 2019).

1 Southern Sudan refers to the south of the country before the independence of South Sudan in 2011.
2 The Sudanese Liberation Movement is a rebel group that has been active in Darfur since 2002. The opposition Justice and Equality Movement has been active in Sudan since 2000.

 DOI: 10.19088/IDS.2021.009

The blackout was listed as a near-total restriction on information flow both in and out of Sudan for most of the population in the country. Activists such as the Sudanese Professionals Association, a trade union, said that the ruling military council deliberately enforced a blackout in an attempt to violently roll back meagre gains by protesters who had assisted in ousting al-Bashir on 11 April 2019 (Feldstein 2019). The internet shutdown increased street protests, which were already causing a strain on the country.

This was not the first time the country had experienced an internet shutdown; but this time, it was different. The shutdown was coupled with reports of organised and systemic killings and looting by government forces, including the RSF (Amnesty International 2019). Before the mobile internet was shut down, the TMC had been negotiating with opposition groups to set up a transitional civilian government (Reuters 2019).

However, a few days into the shutdown, the TMC stopped the negotiations and reportedly sent the Janjaweed militia[3] to attack peaceful protesters (APC 2019). Phones and other personal belongings of the protesters were confiscated and destroyed, so that atrocities would not be shared with the world (Human Rights Watch 2019). The only forms of communication that remained active in Sudan were mobile phones, text messages and fixed-line internet provided by a few operators. It made it difficult for people to know whether their loved ones were safe.

On 4 August 2019, the TMC and the opposition Forces for Freedom of Change – a political coalition of civilian and rebel groups, which was created during the period of the protests – signed a constitutional charter for a transitional period. The charter governs a 39-month transitional period with a power-sharing agreement incorporating political and constitutional agreements (ICNL 2020). General elections will follow the end of the transitional period in late 2022; an exact date has not been set yet. The power-sharing agreement has resulted in the return of some normality to the country. However, civil society is continuously monitoring the country's situation for shifts in the state of human rights.

3 The Janjaweed Arab militia is active in Sudan, particularly in the Darfur region. Since 2003, it has been one of the main players in the Darfur conflict, which has pitted the largely nomadic tribes against the sedentary population of the region in a battle over resources and land allocation.

 DOI: 10.19088/IDS.2021.009

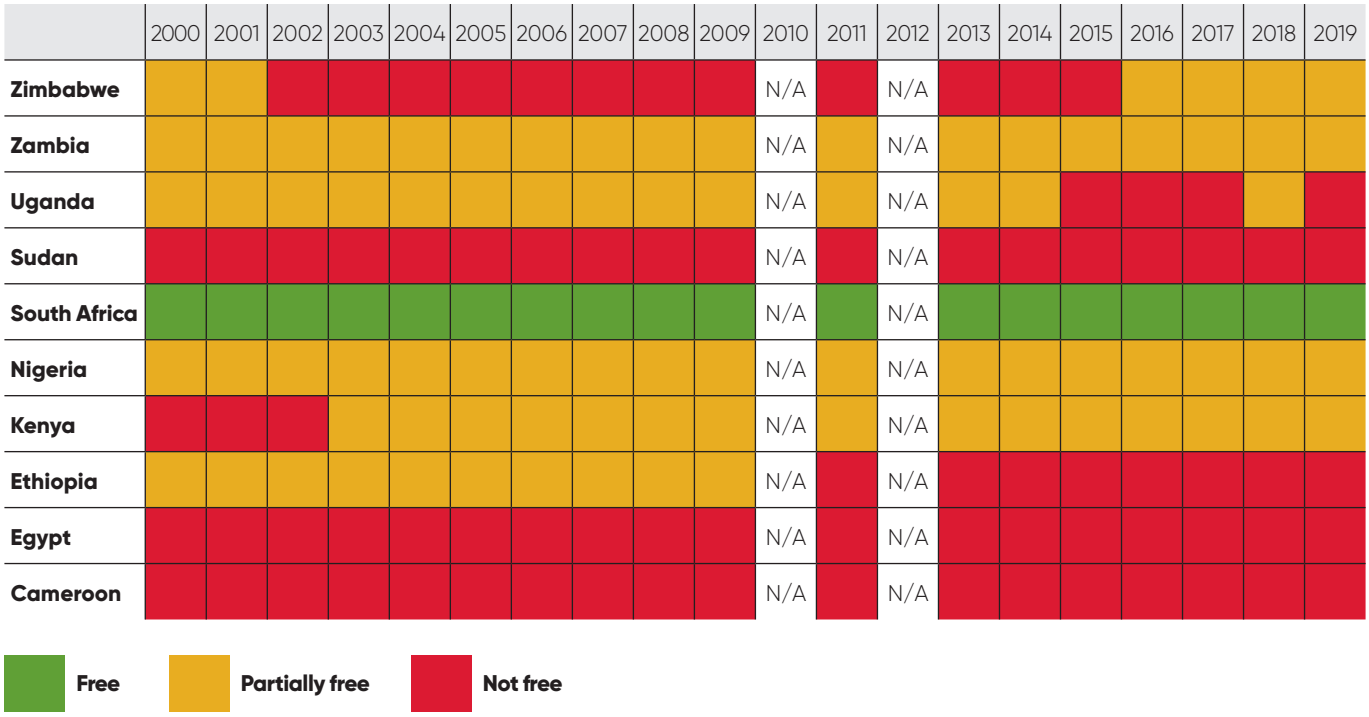
# 3. Civic space landscape

Civil society in Sudan has always played a key role in Sudan's ongoing struggle for political reform since its independence in January 1956 (Armstrong *et al.* 2011). Even though the post-colonial era in Sudan saw most civil society organisations engage in a range of social, economic, cultural and political activities, President al-Bashir ascended to power in 1989 and banned most media outlets (Moorcraft 2015). For instance, in 2012 a human rights defender stated in an interview with global civil society organisation alliance CIVICUS that all organisations promoting human rights within Sudan had been shut down or compelled to flee and establish themselves outside the country (Nigam 2019).

Civil society acts as a service provider to build active citizenship in local, regional and national governance. In the past few years, a great community of actors has been concerned with civic spaces in order to understand the phenomenon behind them better. Sudan's civic space activities have in the recent past faced significant challenges owing to the government's massive censorship and surveillance of the internet (Armstrong *et al.* 2011). According to a study by Freedom House in 2019, citizens' freedom in the civic space was 25 (not free) out of 100, 0 being the least free and 100 the freest (Reduce 2020; see Figure 3.1). Such scores demonstrate how the country is trying to limit freedom to use the internet.

 DOI: 10.19088/IDS.2021.009

## Figure 3.1 Freedom House ranking for ADRN countries, 2000–19[4]




*Note:* ADRN – African Digital Rights Network.

*Source:* Adapted from Freedom House (2019)

Civic space provides fundamental digital rights to every individual by providing a space in which everyone can communicate and share their ideas. Since 2000, internet freedom in Sudan has been limited. Al-Bashir deprived the Sudanese of their basic right to open civic space. Despite all the protests and movements, the civic space is still closed in 2020.

Civic space in Sudan has faced many challenges in the past 20 years. From 2000 to 2012, most Sudanese were unaware of their basic digital rights. Civil society created awareness among the Sudanese people and tried to open civic space for internet freedom. However, major challenges started to appear in 2012, when many organisations were working to promote human rights. Many human rights advocates were forced to flee the country.

In June 2012, journalists demonstrating for economic and political change were confronted by police, leading to many protesters being injured. In September 2013, civil society organisations faced mounting pressure as they conducted a large number of public protests when they also faced police brutality. In the whole of 2016, the government jailed many human rights activists and responded with violence to demonstrators. In the past, many human rights activists were jailed and even executed.

4 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.009

# Table 3.1 Civic space timeline

| Year | Shift | Implication |
|---|---|---|
| **2000–05** | Sudanese government oppresses the people, who are unable to enjoy basic rights. | Closed civic space. |
| **2005** | Access to Information Act is passed. | Opening of civic space. |
| **2008–11** | People are least free to enjoy political and civil rights. | Closed civic space. |
| **2012** | Sudanese government shuts down many organisations promoting human rights. | Civil society activists forced to flee the country. |
| **2013** | Increased public protests; civil society organisations face mounting pressure. | Relative opening of civic space. |
| **2016** | Sudanese government increases suppression of civic space. | Journalists and protesters arrested. |
| **2018** | Telecommunication and Post Regulation Act is passed. | Telecommunication and Post Regulatory Authority can revoke the licence of any broadcasting station or telecoms company violating the terms of the act. |
| **Feb. 2019** | Government unblocks the internet. | People express relief as they can access the internet due to the opening of online civic space. |
| **June 2019** | Provisional government shuts down access to the internet. | Widespread protests, with many injured or killed. |
| **July 2019** | Court orders Transitional Military Council to restore internet access. | Sudanese people get back online once again. |
| **June–July 2019** | Internet shutdown makes it hard to share information. | The internet has become critical to people; civic space is still closed even under the current political regime. |

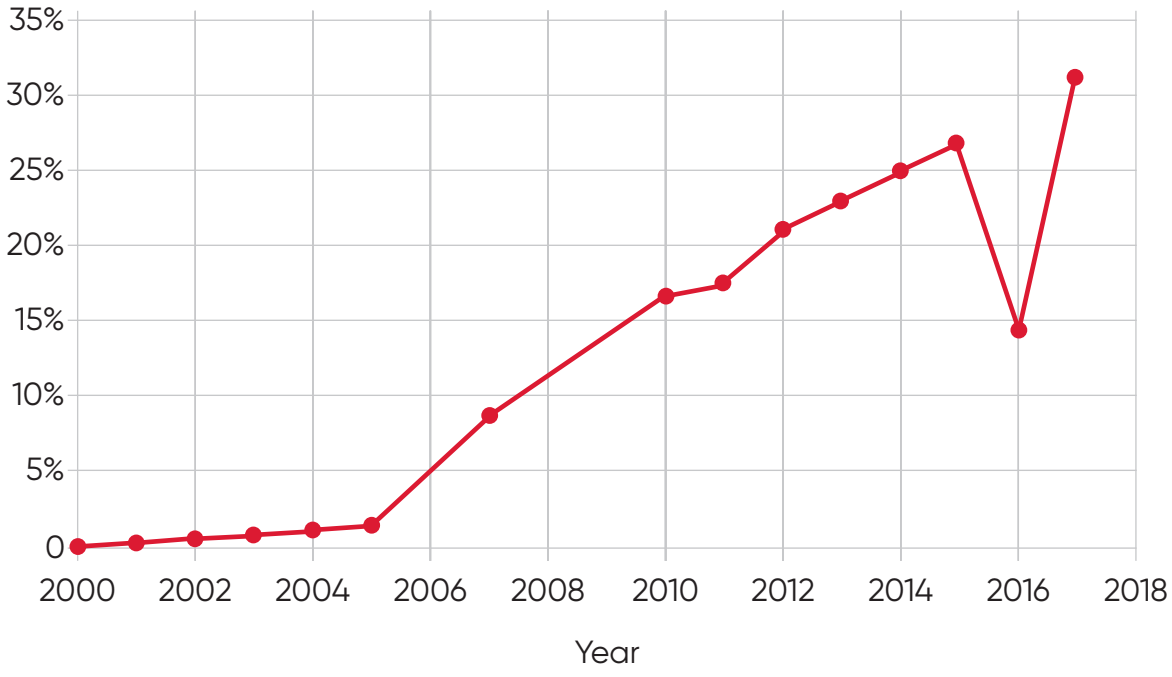
*Source:* Authors' own.

 DOI: 10.19088/IDS.2021.009

# 4. Technology landscape

Sudan has seen millions of people introduced to cyberspace since the start of the millennium, and an expansion of the ability to share information or stay informed about the latest news. As of January 2020, Sudan's internet users stood at 13.38 million people, an increase of 2.4 per cent from 2019, when the number was 316,000 people fewer (Ali 2020). Internet penetration, which measures the proportion of the population that has internet access, remains low, at 31 per cent, as reported in January 2020 (see Figure 4.1). In terms of mobile connections, the number recorded was about 32.83 million, which is an increase of 7.4 per cent from what was recorded in January 2019 (Srinivasan, Diepeveen and Karekwaivanane 2019). The same study considered the number of mobile connections and found that it was about 76 per cent of the whole population. The data show an increasing trend in the use of the internet.

## Figure 4.1 Percentage of the population with internet access in Sudan[5]




*Source:* Based on data from ITU (2020)

5 Data not available for years 2007–09.

 DOI: 10.19088/IDS.2021.009

The Sudanese National Intelligence and Security Services (NISS) control digital media use through multiple strategies, including blocking, controlling, jamming and slowing down certain websites, and hacking private accounts (email, Facebook, Twitter). The NISS acquired ProxySG servers from US cybersecurity and network management company Blue Coat Systems, which enable governments and corporations to intercept internet traffic. The government also uses software that comes from the Italian software company Hacking Team, which enables access to private devices, including data, cameras and microphones. Software and hardware purchases contravene US sanctions and the Wassenaar Arrangement for the non-proliferation of dual-use software (Lamoureux and Sureau 2018).

In 2005, Sudan's government introduced the Sudanese Access to Information Act, which stated that anyone had the right to disseminate and receive data. The act was passed due to constant pressure from foreign countries and also from civil society. However, in 2007 the country introduced the Computer Crimes Act, which mandated two years in prison as punishment for anyone found guilty of limiting access to internet services.

In 2018, the country introduced the Telecommunication and Post Regulation Act, which gave the Telecommunication and Postal Regulatory Authority the mandate to revoke communication licences to any broadcasting station or telecoms company violating the act (Suliman 2019a). Article 56 of the Constitutional Charter for the 2019 Transitional Period enshrined the right to access the internet (Suliman 2019b). However, experts argue that the charter appears vague in the sense that it contains loopholes that the government can use to close civic space and deny digital rights to citizens (*ibid.*).

There are four main internet service providers in the country: Canar, Sudatel, MTN and Zain. MTN and Zain have been able to provide internet services using mobile networks because they have licences (Mohamed Nour 2015). On the other hand, Canar lacks such a licence and therefore relies on leased lines – wireless and landlines – to provide internet services.

To get around the internet shutdowns, Sudanese protesters used various techniques to relay urgent information, but they were not as convenient as using the internet. Not all service providers were willing to prevent their customers from accessing the internet. In particular, Canar refused to switch off the internet for its subscribers. However, owing to pressure from the Sudanese government, the company was compelled to on 5 June 2019

 DOI: 10.19088/IDS.2021.009

(Suliman 2019b). Canar and Sudatel were providing internet services using fibre-optic fibre infrastructure, so some users continued to share political news with the global community. However, because it was quite expensive to access the internet this way (*ibid.*), only the few users who could afford it were able to access the service.

In April 2018, Suad Ahmed Fadel was charged for sharing information on WhatsApp about how she was dismissed from a communications company and replaced by a niece of al-Bashir (Ref World, 2018). The 2007 Cybercrime Act borrows a lot from the Criminal Act of 1991, which prohibits any dissemination of information that may be regarded to be in breach of morality as well as public order. Suad Ahmed Fadel's information was deemed to be in breach of morality, public order and the sanctity of private life.

There is a need for stakeholders to re-evaluate the cybercrime act to remove problematic laws that impinge on freedom of expression on the internet. This is not the first time: people had been using social media to express their views on politics. However, its use has grown so fast that people who use social media just to express their views on politics have started to use it for hashtag campaigns.

The so-called 'bread protests' erupted in December 2018, complemented by social media campaigns. The protests were not just a result of the increased price of bread, but about economic poverty and rising living costs, including the struggle to obtain daily necessities in the country (Mahmoud 2019). On 19 December 2018, amid the revolution that ousted al-Bashir, the government blocked access to social media sites such as Instagram, WhatsApp, Twitter and Facebook as activists had been using them to open civic spaces. However, with the help of virtual private networks (VPNs), it was still possible to use social media, but only the limited number of citizens who had the necessary technical knowledge were able to do so. This move by the government completely contravened freedom of expression on the internet.

On 26 February 2019, the government unblocked the internet for the public and people in Sudan could access social media again (Suliman 2019b). However, the move drew mixed reactions from different sectors. While the public heaved a sigh of relief, human rights defenders and digital rights activists encouraged citizens to avoid the temptation to stop using VPNs; their privacy was still at stake and the government could not be relied on to guarantee it.

On 3 June 2019, Sudan's authorities descended on peaceful protesters in the country's capital Khartoum, which saw hundreds injured. The hashtags #BlueforSudan, #SudanUprising and #StayStrongSudan trended on social media, creating awareness all over the world of what was happening in Sudan. The spike in social media activities as a result of the violent crackdown shows the strength of the internet in relaying information. In the same month, another hashtag, #SudanMealProject, started trending days after the crackdown to rally well-wishers to provide resources for those who had been injured. The hashtag earned about 400,000 followers who pledged to offer food supplies (Frattasio 2019).

At least 100 people were killed during protests to demand the restoration of civilian rule (Taye 2019). From 3 June 2019 up to 9 July 2019, the provisional government shut down internet access again, leading to widespread protests (Suliman 2019b). On 9 July 2019, a court decision ordered the TMC to restore the internet and ensure all internet service providers could provide services to all citizens (*ibid.*). The court decision saw the Sudanese people get back online once again. As mentioned above, the 2018 Telecommunication and Post Regulation Act gives the regulatory authority a mandate to disrupt any broadcasting station or telecommunications if it finds that they are violating the law (Suliman 2019a). However, legal experts argue that the act appears vague and does not go into sufficient detail, which creates an avenue for the authorities to interpret it in a way that allows them to restrict access to services (*ibid.*).

During the whole period of the internet shutdown, from June to July 2019, Sudanese people within and outside the country were worried because the shutdown made it hard to share information with loved ones or even access essential news (Suliman 2019b).

 DOI: 10.19088/IDS.2021.009

# Table 4.1 Technology timeline

| Year | Shift | Implication |
|---|---|---|
| **2003** | World Summit on the Information Society held in Geneva. | Internet access is declared a fundamental human right. |
| **2005** | Access to Information Act is passed. | Every Sudanese citizen has the right to receive and disseminate information. |
| **2007** | Computer Crimes Act introduced. | Misuse of the internet to relay data becomes a punishable offence. |
| **2018** | Telecommunication and Post Regulation Act is passed. | Telecommunication and Post Regulatory Authority can revoke the licence of any broadcasting station or telecoms company violating the terms of the act. |
| **Dec. 2018** | The government blocks social media. | The Sudanese people do not have access to social media. |
| **April 2019** | Al-Bashir government replaced by TMC. | Citizens feel safer and access the internet without VPNs. |
| **3 June 2019** | Hashtags #BlueforSudan, #SudanUprising, #StayStrongSudan and #IAmTheSudanRevolution trending on social media. | Creating awareness all over the world about events in Sudan. |
| **June 2019** | Hashtag #SudanMealProject trending. | Rallying people all over the world to offer free food to Sudanese people. |
| **Jan. 2020** | Number of internet users increases. | Internet access becomes a key issue in Sudan. |

*Source:* Authors' own.

 DOI: 10.19088/IDS.2021.009

# 5. Digital rights landscape

In the presence of the dominant political system and technological landscape, Sudanese citizens cannot easily secure their digital rights. There is much work to be done in Sudan in order to replace the political systems that are not granting the right to digital freedom. Also, the Sudanese people need to expand their technological access, understanding and capacities so that they can open civic space and defend their digital rights.

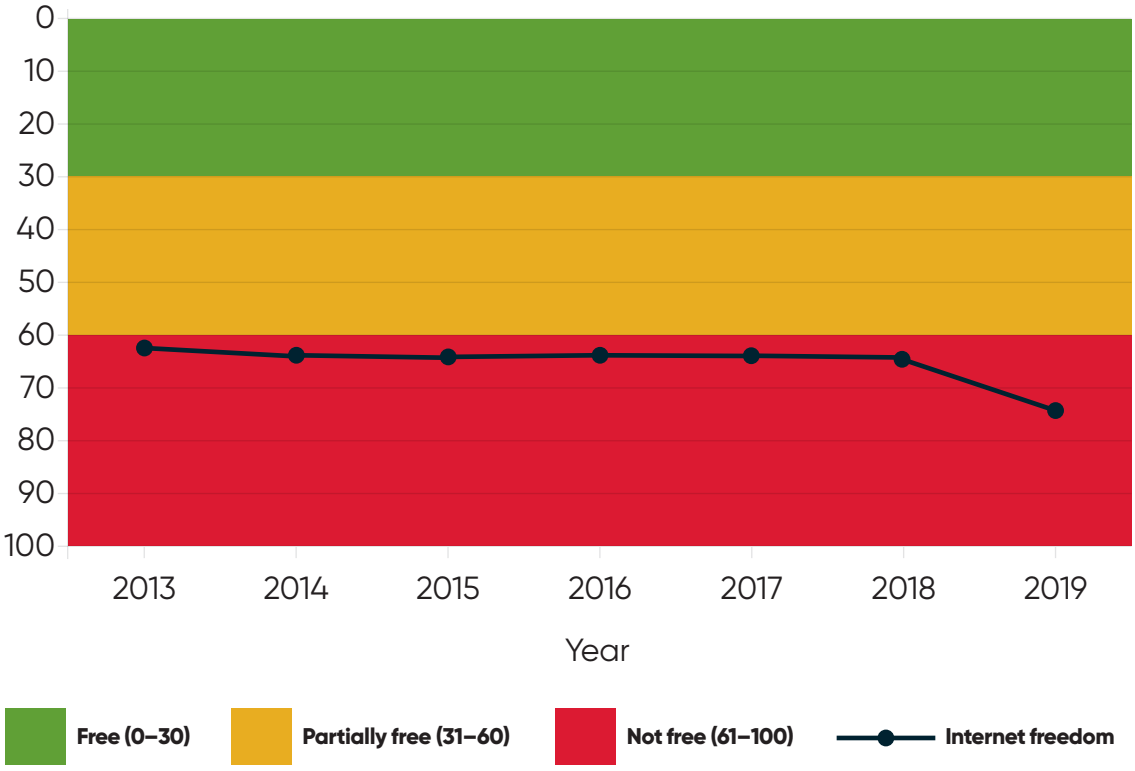
In Sudan there is a need to address vague and contradictory legislation in order to provide the people with basic digital capabilities in the worst of political or technological situations. Closing of civic spaces stands in the way of achieving internet freedom and digital rights. Key civil society actors are still unable to effectively assess the tools and methods being used by the government to close civic space. Civil society actors should work together to build spaces through which every citizen can exercise and defend their digital rights.

Many reputable international organisations recognise the right to connect to or access information as a fundamental human right. For instance, in 2003 the World Summit on the Information Society held in Geneva reached a consensus that the internet is key to providing information to society and that no one should be denied access to the internet (Access Now 2016). Also, in 2016 the United Nations Council on Human Rights passed a resolution condemning internet shutdowns and supporting human rights online, as was the case in Sudan (*ibid.*).

From 1977, Sudan was constrained by a US-imposed embargo put in place, which in turn reinforced the government's justification for oppression and control over the internet: the internet is necessary for trading and most international trading takes place through online transactions (Kehl and Maurer 2014). Due to US restrictions, citizens in Sudan were unable to download or update US-made software, thus using vulnerable and unprotected operating systems. However, between 2014 and 2017, the sanctions were lifted (Yahia *et al.* 2018). Despite the embargo, the country went from about 1 per cent of people using the internet in 2000 to about 22 per cent over the next ten years (Internet Live Stats 2016). About 30 per cent of the country's population can access the internet from the comfort of their own home. Thus, more people have internet access, but internet freedom is still not free, as shown on Freedom House's Freedom on the Net Index (see Figure 5.1).

 DOI: 10.19088/IDS.2021.009

## Figure 5.1 Sudan's Freedom on the Net Index score, 2013–19




*Source:* Based on data from Freedom House (2020)

In the past two decades, civil society organisations in Sudan have tried to build alliances with other groups in order to make it easy for them to maintain and promote their activities in a way that could influence governance. However, the government considers civil society as a threat and has improved its technical capabilities to have control over political activists since 2016 (Lamoureux and Sureau 2019). Sudan's government has invested heavily in its technical capabilities. For instance, the NISS controls digital media operating within its borders by using various strategies such as hacking private accounts and blocking websites. Also, the NISS uses controlling mechanisms and slows down or jams various websites as a way of asserting control over the use of digital media (*ibid.*).

The NISS has proxy servers it bought from the US to allow the government to intercept internet traffic. The organisation also uses spyware from Italian company Hacking Team to access private devices such as microphones and cameras, and data (Suliman 2019a). The proxies allow the NISS to control, intercept or restrict private information, which includes but is not limited to encrypted information, such as private emails and bank accounts. Also,

 DOI: 10.19088/IDS.2021.009

proxies can slow down certain websites, thus influencing what information people can access.

The Sudanese government does not rely wholly on technological means to control digital media, but also uses the idea of morality. The government's idea to use Islam to control the Sudanese people was first introduced into law in 1991, when a criminal code enabled the government to defend and control the morality of its citizens using Islamic disciplinary measures (Lamoureaux and Sureau 2018).

The increased use of social media has seen the Sudanese government use the internet to monitor communications on social media sites. Moreover, the government established a Cyber Jihad Unit that has since been used to monitor bloggers and dissenting groups (Freedom House 2016). The NISS thus seems to use both technical and social techniques to monitor the activities of Sudanese citizens. The Cyber Jihad Unit proactively monitors the activities of Sudanese people on the internet and is also involved in political influencing through trolls (Freedom House 2014).

 DOI: 10.19088/IDS.2021.009

# 6. Digital rights in times of Covid-19

The Covid-19 pandemic is a moment when countries need to reflect on how not to limit digital rights while trying to protect public health. The internet, as a platform for communication, helps inform the public about health threats at a relatively faster rate than traditional tools of communication such as radio and newspapers (Micek and Krapiva 2020). Even though health data should remain confidential, owing to their sensitivity, the government can use health data to respond faster to outbreaks. Governments around the world, not just in Sudan, may see this period as ideal to introduce controversial technology for surveillance to legitimise oppressive tools disguised as public health tools. In most Asian countries, for example, facial recognition technology is already being used for surveillance and control, and to monitor people's movements (Jeria *et al.* 2020).

As described above, Sudan's authorities have used internet shutdowns to prevent the public from sharing information and convicted citizens of sharing information perceived to cause public disorder (Suliman 2020). Therefore, if the government thinks that an open debate about the severity and extent of the Covid-19 pandemic is not right for the stability of the country or national security, it is possible that the authorities could censor information or limit access to the internet. Censorship violates the right to access information and free speech, and could also encourage the spread of the disease even further.

This last aspect could arise through disinformation. Much false information has spread in Sudan during the Covid-19 pandemic. People spread false information to either become famous or to get more likes on social media platforms. To reduce disinformation, the United Nations Children's Fund (UNICEF) set up help centres to provide all the necessary information regarding the Covid-19 outbreak, symptoms and management. A hotline has operated during the crisis to provide the public with the latest authentic information by phone. People have taken advantage of this hotline as they have no internet access by which they can get information (Madyun and Abdu 2020).

The internet can allow (deliberate) disinformation and (accidental) misinformation about the disease to spread quickly. False data about vaccines or treatments could be spread through social media sites and messaging platforms such as WhatsApp (Suciu 2020). In response, social media sites such as Twitter and Facebook, as well as the tech giant Google, have introduced official guidance from health experts for users looking for coronavirus information (Jakhar 2020). The Sudanese government, however, has not developed a specific app or tracker to trace Covid-19 cases in 2020. The main reason is that most people do not have access to the internet. The Sudanese government, like many other African governments, should thus create awareness to prevent its citizens from spreading disinformation and misinformation about the disease.

 DOI: 10.19088/IDS.2021.009

# 7. Conclusion

This report has looked at digital rights in Sudan as a case study. Like many other countries, digital penetration in Sudan has increased over the years, however, the use of digital tools by civil society to voice dissent and coordinate political activities in the country, such as the fall of the al-Bashir regime, has encouraged the authorities to shut down the internet. The opening and closing of online civic space has become key to digital rights in Sudan; specifically, freedom of expression, freedom of assembly and freedom of political opinion.

Access to information has become a fundamental right and internet shutdowns or restrictions contravene the Sudanese people's (digital) rights. Domestic civil society is working effectively to monitor and analyse the opening and closing of civic spaces to provide citizens with their basic digital rights. The government continues to rely on foreign software to spy on citizens and has taken the Covid-19 pandemic as an opportunity to use technology to increase surveillance and limit people's digital rights.

 DOI: 10.19088/IDS.2021.009

# 8. Digital rights future recommendations

The government should promote the use of digital technologies to share information and allow essential services to be offered online. Universities and civil society organisations do not currently have the research capabilities they need to effectively monitor and analyse internet shutdowns in Sudan. The Sudanese people must elect a political party that is willing to provide its people with these capabilities and help strengthen digital rights and internet freedom. The government must also find ways to open the civic space and improve technology. Digital technologies can also be used to strengthen governance processes during the pandemic when assembling people, or when traditional cash-based ways of doing business in Sudan are discouraged.

As discussed, limiting the use of the internet in relaying public health information could make Covid-19 spread even further. Therefore, Sudan's government should not discourage online activities or censor information shared through social media sites. The potential benefits of sharing public health information outweigh the risk posed by the spread of disinformation.

Sudan's government, and many other African states, need to revise their regulations on the use of digital technologies to remove or amend specific laws that encourage surveillance of private data and internet shutdowns, and restrict freedom of expression, as is evident in Sudan.

 DOI: 10.19088/IDS.2021.009

# References

Access Now (2016) **'U.N. Passes Landmark Resolution Condemning Internet Shutdowns'**, 1 July (accessed 23 October 2020)

Ali, M.A. (2020) 'E-Commerce in Sudan (Analytical Study)', in M. Ezziyyani (ed.), *Advanced Intelligent Systems for Sustainable Development (AI2SD 2019): Vol. 3 – Advanced Intelligent Systems for Sustainable Development Applied to Environment, Industry and Economy,* Cham: Springer

Amnesty International (2019) ***Everything You Need to Know About Human Rights in Sudan*** (accessed 5 November 2020)

APC (2019) ***Civil Society Organisations Issue Statement Denouncing Internet Shutdowns in Sudan***, Association for Progressive Communications (accessed 26 October 2020)

Armstrong, D.; Bello, V.; Gilson, J. and Spini, D. (eds) (2011) *Civil Society and International Governance: The Role of Non-State Actors in Global and Regional Regulatory Frameworks*, Abingdon: Routledge

CIVICUS (2016) **'Civic Space'**, *What is Civic Space?* (accessed 26 October 2020)

Feldstein, S. (2019) **'To End Mass Protests, Sudan Has Cut Off Internet Access Nationwide. Here's Why'**, *The Washington Post*, 13 June (accessed 26 October 2020)

Frattasio, E. (2019) **'Sharing, Caring, and Praying for Sudan in the Twitter Age'**, *The McGill International Review*, 17 July (accessed 26 October 2020)

Freedom House (2020) ***Freedom on the Net*** (accessed 4 December 2020)

Freedom House (2019) ***Freedom in the World*** (accessed 4 December 2020)

Freedom House (2016) ***Sudan*** (accessed 5 November 2020)

Freedom House (2014) **'Sudan'**, *Freedom on the Net 2014 – Tightening the Net: Governments Expand Online Controls* (accessed 7 November 2020)

Gil de Zúñiga, H.; Molyneux, L. and Zheng, P. (2014) 'Social Media, Political Expression, and Political Participation: Panel Analysis of Lagged and Concurrent Relationships', *Journal of Communication* 64.4: 612–34

Grobler, M. (2010) 'Strategic Information Security: Facing the Cyber Impact', Proceedings of the Workshop on ICT Uses in Warfare and the Safeguarding of Peace, Bela Bela, South Africa, 11 October 2010

Human Rights Watch (2019) **'They Were Shouting "Kill Them"'** (accessed 5 November 2020)

ICNL (2020) ***Sudan***, International Center For Not-For-Profit Law (accessed 26 October 2020)

Internet Live Stats (2016) ***Sudan Internet Users*** (accessed 26 October 2020)

ITU (2020) ***Internet Access Statistics***, International Telecommunication Union (accessed 4 December 2020)

Jakhar, P. (2020) **'Coronavirus: China's Tech Fights Back'**, *BBC News*, 3 March (accessed 26 October 2020)

Jeria, M.B.; Sharif, M.M.; Saiz, E. and Boni, A.L. (2020) ***Digital Rights in the COVID-19 Era***, United Nations Human Rights Office of the High Commissioner (accessed 26 October 2020)

Kehl, D. and Maurer, T. (2014) **'Time to Rethink Tech Sanctions Against Sudan'**, *Slate*, 30 January (accessed 26 October 2020)

Kummer, M. (2003) 'Information Society: Promise and Risks', *OECD Observer*

Lamoureaux, S. and Sureau, T. (2018) 'Knowledge and Legitimacy: The Fragility of Digital Mobilisation in Sudan', *Journal of Eastern African Studies* 13.1: 35–53, DOI: **10.1080/17531055.2018.1547249** (accessed 12 November 2020)

Lin, L. (2020) **'China Turns to Health-Rating Apps to Control Movements during Coronavirus Outbreak'**, *The Wall Street Journal*, 18 February (accessed 26 October 2020)

Madyun, A. and Abdu, L. (2020) ***Combatting Myths and Misinformation at Sudan's COVID-19 Hotline Call Centre***, New York NY: United Nations Children's Fund

Mahmoud, O. (2019) ' **"It's More than Bread": Why are Protests in Sudan Happening?'**, *Middle East Eye*, 24 January (accessed 12 November 2020)

Micek, P. and Krapiva, N. (2020) ***Protect Digital Rights, Promote Public Health: Toward a Better Coronavirus Response***, Access Now blog, 5 March (accessed 26 October 2020)

Mohamed Nour, S. (2015) 'The Demand Side of ICT', in S. Mohamed Nour (ed.), *Information and Communication Technology in Sudan*, Cham: Springer

Moorcraft, P. (2015) *Omar al-Bashir and Africa's Longest War*, Barnsley: Pen & Sword

Nigam, S. (2019) ***The Powerful Mighty State versus the Human Rights Defenders: The Courage to Challenge the Unruly Authority*** (accessed 26 October 2020)

Reduce, S. (2020) 'The Freedom House Survey for 2019: The Leaderless Struggle for Democracy', *Journal of Democracy* 31.2: 137–51

Reuters (2019) **'Sudanese Forces Storm Protest Camp, More Than 35 People Killed: Medics'**, 3 June (accessed 5 November 2020)

Srinivasan, S.; Diepeveen, S. and Karekwaivanane, G. (2019) 'Rethinking Publics in Africa in a Digital Age', *Journal of Eastern African Studies* 13.1: 2–17

Suciu, P. (2020) **'Misinformation Spreading Faster than the Actual Coronavirus'**, *Forbes*, 3 February (accessed 26 October 2020)

Sudan Tribune (2010) **'Sudan Reportedly Blocks YouTube over Electoral Fraud Video'**, 22 April (accessed 26 October 2020)

Suliman, M. (2020) **'Internet Censorship in Sudan: Rethinking Laws and Tactics that Served an Authoritarian Regime'**, *Global Voices Advox*, 15 October (accessed 26 October 2020)

Suliman, M. (2019a) **'The Right to Privacy in Sudan: A Call to Enact a Data Protection Act'**, *Global Voices Advox*, 5 November (accessed 26 October 2020)

Suliman, M. (2019b) **'Internet Shutdowns and the Right to Access in Sudan: A Post-Revolution Perspective'**, *Global Voices Advox*, 16 September (accessed 26 October 2020)

Taye, B. (2019) ***#IAmTheSudanRevolution: There's a Direct Link between Internet Shutdowns and Human Rights Violation in Sudan!***, Access Now blog, 11 June (accessed 26 October 2020)

UN Human Rights Council (2016) ***Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet***, A/HRC/32/L.20, 27 June (accessed 11 February 2021)

US Department of State (2004) *The Crisis in Darfur: Secretary Colin L. Powell, Testimony Before the Senate Foreign Relations Committee*, Washington DC: United States (US) Department of State

Waterton, E. (2010) 'The Advent of Digital Technologies and the Idea of Community', *Museum Management and Curatorship* 25.1: 5–11

Yahia, Y.E.; Liu, H.; Khan, M.A.; Shah, S.S.H. and Islam, M.A. (2018) 'The Impact of Foreign Direct Investment on Domestic Investment: Evidence from Sudan', *International Journal of Economics and Financial Issues* 8.6: 1–10

 DOI: 10.19088/IDS.2021.009

# South Africa Digital Rights Landscape Report

Tanja Bosch and Tony Roberts



This report is part of 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries'; the Introduction is also recommended reading.

© 2021 Tanja Bosch and Tony Roberts © Institute of Development Studies. DOI: 10.19088/IDS.2021.010

# 1. Introduction

This report provides an overview of the political, and civic space and technological context that have shaped digital rights in South Africa since 2000. The term 'digital rights' here refers to the right to access the internet as a means to ensure freedom of information, freedom of expression and association (UN 2011).

The report begins with an overview of the political landscape in South Africa as it influences the availability of digital rights. This is followed by a discussion of the main contours in the country's civic space landscape, where the term civic space refers to the amount of room available for citizens, organisations and the government to freely and safely discuss opinions and influence policy and governance processes.[1] The third section describes the technology landscape and explores citizens' use of mobile phones and social media platforms to mount influential advocacy campaigns using hashtags including #RhodesMustFall, #FeesMustFall and #ZumaMustFall. These are given as examples of citizens' digital technology use to open civic space discussion of issues neglected by mainstream media and politicians.

The technology landscape section also discusses technology use by the government and private companies to close civic space, using examples including internet shutdowns, surveillance technologies, and the use of automated disinformation campaigns. The report then provides an analysis of how these political, civic and technological factors affect the digital rights of South African citizens. It identifies what existing capabilities and gaps exist to monitor and effectively respond to these developments; and makes a number of recommendations for policy, practice and further research, which are designed to strengthen citizens' abilities to more effectively exercise, defend and expand their digital rights.

1 Definition adapted from CIVICUS (2020).

 DOI: 10.19088/IDS.2021.010

# 2. Political landscape

The most dramatic feature of South Africa's modern political landscape was the end of apartheid policies that outlawed freedom of political opinion, expression and association for the majority black population. However, the struggle to translate political freedoms and rights into social and economic justice continues to be contested.

The 1994 elections were the first in which all South Africans could vote irrespective of race. They marked the end of apartheid and the extension of political and human rights in South Africa, concluding four years of negotiations. The negotiations had begun in 1990 with the unbanning of liberation movements and the creation of a new constitution and bill of rights under the country's first black president, Nelson Mandela, as leader of the African National Congress (ANC), in partnership with the South African Communist Party and Congress of South African Trade Unions.

Since 1994, the ANC has consistently won at least 60 per cent of the vote, although its popularity declined by several percentage points between 2004 and 2014. The ANC's main rivals are the Democratic Alliance and the Economic Freedom Fighters (EFF), although a total of 48 political parties registered candidates for the 2019 parliamentary elections. Despite enjoying a multiparty political system, South Africa is often considered a weak or transitional democracy because of the dominance of the ANC in the absence of an effective opposition. This highlights the generally accepted notion that formal freedoms often do not necessarily translate into meaningful political participation, if one party monopolises power.

A prevailing feature of political discourse in South Africa has been the idea that opposition parties might be able to recruit the growing constituency of unemployed youth and discontented citizens. However, despite being politically active in other ways, young people have remained largely disengaged from mainstream party politics, though politically active in other ways, including the influential hashtag social media campaigns of #RhodesMustFall and #FeesMustFall, discussed in detail below. In 2019, only 16 per cent of 18–19-year-olds were registered to vote. Roberts (2019: 39) argues that this does not reflect political apathy, but rather that young people 'are highly critical of political leaders and parties who they feel have ignored their needs and fail to engage with them in a meaningful manner'.

 DOI: 10.19088/IDS.2021.010

From 2005 onwards, during the presidency of Thabo Mbeki (1999–2008), there was an upswing in community-led protests tackling poor access to water and electricity, housing, corruption and nepotism in local councils, and the lack of meaningful participation in local decision-making despite policy requiring it (Akinboade, Mokwena and Kinfack 2013; Alexander 2010; Atkinson 2007; Ballard, Habib and Valodia 2006; Booysen 2007; Burger 2009). These protests were initially united under regional banners, such as the Anti-Privatisation Forum in Gauteng and the Anti-Eviction Campaign in the Western Cape (Madlingozi 2007).

These protests reflect the co-existence of formally declared *openings* that in practice are *closures* of civic space. Howell (2019) argues that contemporary legislation in South Africa allows for the opening of civic space, along with a vibrant network of civil society organisations (CSOs) in the post-apartheid era. Citizens and CSOs can generally organise and communicate without hindrance, but the state often reneges on its duty to protect civil society, and South Africa remains politically fractured and the most unequal society on earth (World Bank 2019).

South Africa experienced two waves of extreme violence in 2008 and 2015. These waves of violence articulated responses to ongoing poverty and inequality, with foreign nationals being accused of competing for low-paying jobs (Dodson 2010). At the same time, the violence could also be seen as defining who is truly South African; and who has the right to access public services and who is excluded. In parallel with local-level forms of contestation, at the national level various accusations of corruption rocked the ANC, spurring the growth of a new political party, the EFF, which managed to secure seats in the country's parliament (Schulz-Herzenberg 2014). One key corruption scandal was around the exorbitant upgrades to President Zuma's home (Beresford 2015), leading the EFF to disrupt the 2015 state of the nation address with demands that the president 'pay back the money'.

 DOI: 10.19088/IDS.2021.010

# 3. Civic space landscape

Opening civic space for inclusive deliberation of social issues is foundational to democratic governance (Civic Space Watch 2020). Civic space is the room available to citizens and civil society organisation to engage with government to represent their perspectives on and interests to influence policy and governance issues. Such participatory governance is guaranteed in the South African Constitution and Bill of Rights, and the government has committed to its defence and extension in international conventions including the Sustainable Development Goals (UN 2015). According to Freedom House (2019), South Africa is relatively 'free' when compared to other countries in the African Digital Rights Network (see Figure 3.1). Civil society is usually conceptualised as a network of both citizen associations and CSOs that influence democratic governance via their ability to mobilise citizens on behalf of public causes (Foley and Edwards 1996). The link between civil society and democracy sees the former as providing an impetus for establishing elections, and therefore a key element of democracy (Bosch *et al.* 2019).

## Figure 3.1 Freedom House ranking for ADRN countries, 2000–19[2]


*Note:* ADRN – African Digital Rights Network.

*Source:* Adapted from Freedom House (2019)

2 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.010

Many of the key civic struggles in South Africa's recent history have been around public service delivery. The Treatment Action Campaign (TAC) was founded in December 1998 to campaign for access to AIDS treatment and came to prominence during the presidency of Thabo Mbeki due to the AIDS denialism of Mbeki and his minister of health, Manto Tshabalala-Msimang. The TAC is widely acknowledged as one of the most important CSOs on AIDS in the developing world. One of its most significant victories was the 2002 Constitutional Court ruling in which the South African government was ordered to provide antiretroviral drugs to prevent transmission of HIV from mothers to their babies during birth. Despite this judgement from the highest court in the country, along with continued public pressure, the HIV treatment programme only gained significant momentum once Mbeki and Tshabalala-Msimang had been removed from office in 2008.

Two independent studies estimate that delays in making antiretroviral treatment available in the public sector in South Africa resulted in more than 300,000 avoidable deaths (TAC 2016). The TAC campaign was instrumental in securing a universal government-provided AIDS treatment programme, which has since become the world's largest (TAC 2020). With leadership from TAC, South Africa's AIDS response united civil society and international support in a way not seen since the opposition to apartheid (Simelela and Venter 2014). The TAC campaign is highlighted here as a reflection of the existence of an open civic space in which activists were able to improve access to antiretroviral treatment and expand access to HIV treatment.

Under Zuma's presidency (2009–18), those exercising the right to peaceful protest experienced increasing police violence. The most dramatic example of this was the so-called 'Marikana massacre' at the Marikana platinum mine, where 34 striking miners were killed and 78 injured when police opened fire on them. This has been described as the most lethal use of force by South African security forces against civilians since 176 people were killed in the Soweto uprising of 1976. Dominant media narratives at first supported official claims that the police had acted in self-defence at Marikana and portrayed the miners as predisposed to violence. Only much later did the reporting shift to include the voices of mineworkers and providing alternative accounts to the police version of events (Duncan 2014). The current president, Cyril Ramaphosa, was at that time a non-executive director of Lonmin, the company running the Marikana mine. He was heavily criticised for an email in which he recommended heavy-handed action against the striking miners (for which he subsequently apologised). The strike is considered a key event in South Africa's recent history and was followed by a series of similar strikes at other mines in 2012. Events such as Marikana highlight that while the state allows individuals and CSOs formal rights, violations of these rights also take place.

 DOI: 10.19088/IDS.2021.010

The 2011 Protection of State Information Bill increased government efforts to impose a 'culture of secrecy' around investigations of government fraud and state information by attempting to control critical or inconvenient information. Otherwise known as the Secrecy Bill, it allowed for the withholding of information from the public. Discussions around the proposed bill took place alongside a government push for a media appeals tribunal in 2017, arguing against freedom of the press as an absolute right, and instead that it should be balanced against government officials' right to privacy. The ruling ANC argued that the press ombudsman was biased towards the media, and that a tribunal, appointed by Parliament, would hold the media accountable. This was dismissed as political interference, and the resolution to establish the tribunal was not tabled in Parliament. These events suggest that in instances where government has attempted to shut down civic space, there has been push back from civil society against such repressive legislation, leading to further criticism from the government.

Government departments periodically make statements alleging that local CSOs are colluding with external powers to undermine the state's authority. In March 2016, CSOs condemned the military-style armed robbery of documents and computers from the offices of the Helen Suzman Foundation at a time when the organisation was seeking to interdict the head of South Africa's corruption and crime fighting investigative unit, the Hawks (Kode 2018). In the same month, anti-mining activist Sikhosiphi 'Bazooka' Rhadebe, was brutally murdered in his home after campaigning against the mining interests of Australian mining company Mineral Commodities Ltd (*ibid.*). Taken together, such actions create a climate of fear and uncertainty among citizens who feel they do not have access to a safe and enabling civic space (CIVICUS 2016).

South African media have played a significant role in the opening and closing of civic space, particularly in terms of building negative perceptions of community protests, and criminalising and delegitimising protesters. The media affect the parameters of civic space partly due to their role in setting the frame of the Overton window (Robertson 2018): which topics it is acceptable to speak of, what it is permissible to demand and what is off the table. In South Africa, the media have arguably been complicit in encouraging xenophobic discourse. Even when the media do well in relating xenophobic conflicts, they often fail to cover the causal factors underpinning such violence (Hickel 2014). The media were at the centre of the 2015 state of the nation address conflict, when government operatives jammed communication within Parliament to suppress media coverage.

In conclusion, there is a history of contention of civic space in South Africa. In the late twentieth century, political activists successfully campaigned for an end to the racist segregation of the apartheid era and its replacement with democratic government. In post-apartheid South Africa, a range of citizen-

 DOI: 10.19088/IDS.2021.010

led social movements emerged, many expressing widespread dissatisfaction with the continued inequality and inadequate service delivery. These grassroots concerns included struggles over housing, land, health, education and service provision. The new social movements are part of the marginalised subaltern urban class in the developing world that emerged as a result of rapid global economic restructuring in the 1990s (Chiumbu 2015), intensified by the adoption of neoliberal macroeconomic policies. These movements are increasingly combining traditional mobilisation methods with new media technologies to mobilise, create networks and lobby for social justice.

Unlike other African countries, South Africa has not experienced laws designed to deregister or cut funding to civil society registration, but there has been an upward trend in restrictions and various forms of harassment (Smidt 2018). Although freedom of expression and peaceful assembly are protected in the South African Constitution, the ability to exercise these rights is often limited by restrictive and violent measures by the state to curb peaceful demonstrations (CIVICUS 2016).

## Table 3.1 Civic space timeline

| Year | Shift | Implication |
|---|---|---|
| **1994** | End of apartheid; first democratic government. | Opening of civic space follows lifting of apartheid restrictions. |
| **2002** | TAC secures ARTs for people living with HIV/AIDS (PLHIV). | Civil disobedience campaign opens civic space for PLHIV. |
| **2005** | Shack dwellers revolt and boycott local government elections, and other service delivery campaigns. | CIVICUS reports repression by police, destruction of shacks and threats to leaders. |
| **2008** | First wave of xenophobic violence. | Closing of civic space for immigrants. |
| **2009** | Zuma's term as president (2009–18) marked by corruption and repression. | Civil society vocal but not enabled or protected. |
| **2012** | Marikana massacre of striking miners. | Strikes expand and general volumes of protests increases. |
| **2016** | Helen Suzman Foundation robbery and Sikhosiphi 'Bazooka' Rhadebe murdered. | State repression limits civic space. |
| **2019** | After Zuma leaves office, service delivery protests escalate. | Citizen-led, non-partisan campaigning opens civic space across race/class/gender divides. |
| **2020** | Covid-19 lockdown enforcement kills citizens; C19 campaign launched. | The government awards itself new surveillance and policing powers, and limits digital rights. |

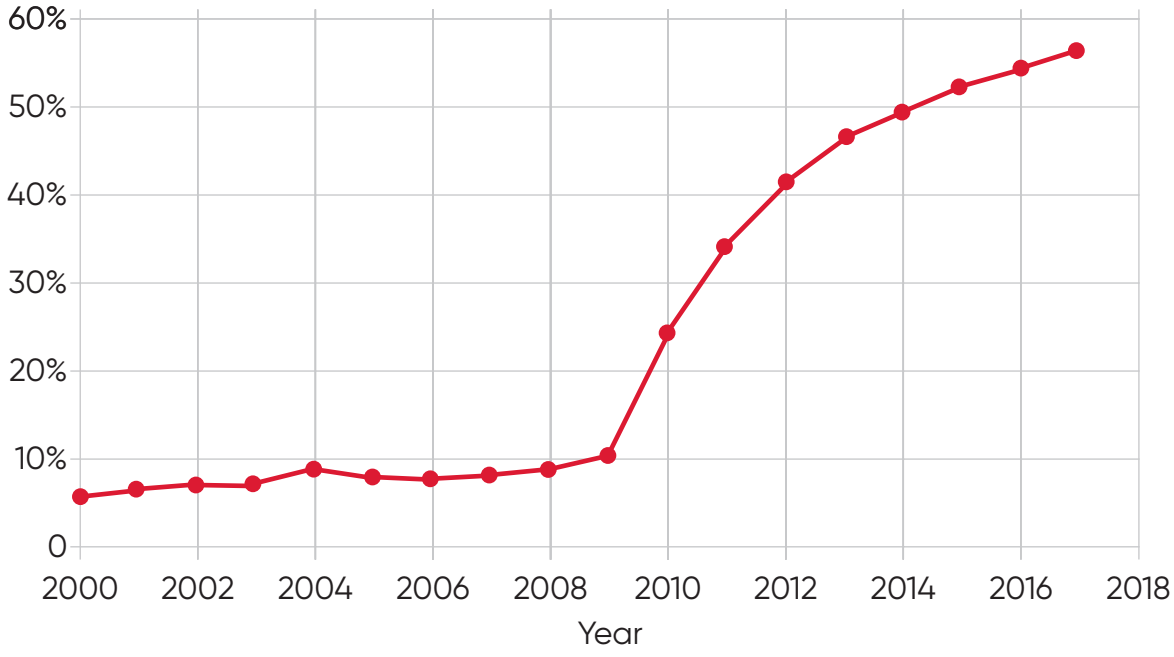
*Source:* Authors' own.

 DOI: 10.19088/IDS.2021.010

# 4. Technology landscape

Internet access in South Africa has increased rapidly, with much of the growth occurring in the last 12 years (see Figure 4.1). Between 2001 and 2011, South African national census reports showed that the proportion of households owning mobile phones had increased from 32 per cent to 89 per cent. By 2020, of South Africa's 59 million citizens 36.54 million were internet users, of which 34.93 million were mobile internet users (Clement 2019). The growth of the mobile internet has resulted in greater access in the absence of widespread broadband; but data costs are still a prohibitive factor to internet access and the opening up of civic space by digital means. Moreover, price discrimination has meant that poorer consumers are usually forced to purchase lower-priced bundles, which are valid for a shorter time and do not provide as much data as more expensive bundles, and with much higher costs per megabyte (Masweneng 2019). A further barrier to access is the impact of English literacy on wider adoption – the dominance of English limits access to those who are not proficient in the language.

## Figure 4.1 Percentage of the population with internet access in South Africa




*Source:* Based on data from ITU (2020)

 DOI: 10.19088/IDS.2021.010

In 2014, there was an increase in civic tech organisations in South Africa with the establishment of organisations including Amandla.mobi, Grassroot, and later GovChat and Vulekamali. These civic tech organisations use the affordances of digital technologies for connective action (Bennett and Segerberg 2013), opening civic space to talk about issues not well covered by mainstream media or political parties. The organisations focus on issues including transparency and accountability, education, citizen participation, open data, governance and journalism (Civic Tech 2020).

South Africa has experienced growing digital citizenship, facilitated by the use of social media applications such as Facebook and Twitter to create new online civic spaces to advocate for change. South African youth have also increasingly used social networking sites to develop a new biography of citizenship, characterised by more individualised forms of activism (Bosch 2017). This can be understood with reference to three influential hashtag campaigns in 2015: #RhodesMustFall, #FeesMust Fall and #ZumaMustFall.

The Rhodes Must Fall movement began on the campus of the University of Cape Town in October 2015 with a student activist flinging human waste at the statue of colonialist Cecil John Rhodes, which was prominently located on the campus. Students' initially demanded the removal of the statue of Rhodes, but protests developed into a broader movement for the decolonisation of education across the country. The movement used the hashtag #RMF to set the agenda for public debate in online and offline spaces, as well as in mainstream media, with the Twitter discourse playing a key role in creating a space for debate and discussion (Bosch 2017). Many of the same activists then took part in the #FeesMustFall (#FMF) protests to reduce the prohibitive cost of university tuition. The #FMF hashtag generated nearly 1.3 million tweets during the last two weeks of October 2015, with Twitter being the most used social media platform for the campaign.

While Twitter served as a choreography of assembly (i.e. to alert users to offline protest gatherings and call them to action), Facebook was also used for widespread debate and discussion (Bosch 2016), and WhatsApp and Google Docs for internal communication and debate. The 'MustFall' narrative was then re-directed towards the president in the #ZumaMustFall (#ZMF) campaign, which had gone viral by the end of 2015. The movements shared similarities in that they challenged establishment authority from outside party politics or formal civil society, and made productive use of the affordances of social media to amplify demands inexpensively, and instantly across any geography.

 DOI: 10.19088/IDS.2021.010

In the South African context, there is also evidence that the campaign built alliances across barriers of race, gender and class.[3] This was one of the largest instances of protest action in South Africa, with thousands of people taking to the streets in public marches across the country. What was particularly striking about both #FeesMustFall and #ZumaMustFall is that they represented protest across class and racial divides, as a means to express solidarity without physical or social proximity; as well as the use of digital technologies for the opening of civic space.

While most community protests in South Africa take place in the impoverished black townships, #FeesMustFall took place on university campuses in urban centres, including at former white universities; and anti-Zuma marches took place in urban centres, uniting citizens across race and class, with unusually large numbers of white protesters. While South Africans have a range of protest repertoires from the anti-apartheid era, the emergence of social media tools and hashtag activism holds the potential to amplify citizen discontent through building horizontal connections between citizens across demographic divides.

For its part, the South African state has also accumulated a range of technologies and mechanisms for influencing civic space that impact on digital rights. The rest of this section examines the use of legal, digital and violent responses to citizen expressions of the right to freedom of opinion, freedom of expression, freedom of assembly, and the rights to privacy and freedom of information.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act – better known as RICA – came into effect in 2005. It regulates when the government can surveil citizens through the interception of their communications (Omarjee 2020). RICA allows state surveillance of mobile and internet communications, but following a legal challenge from South African civil society organisation amaBhungane, the High Court ruled that some provisions of the legislation were unconstitutional (Staff Writer 2019). There is also evidence that South Africa has procured artificial intelligence surveillance technologies from Chinese telecommunications company Huawei as part of China's Safe City programme (Carnegie Endowment for International Peace 2019; Hillman and McCalpin 2019). Another instance highlighting the threat to privacy from mass surveillance was the disclosure that the South African and UK governments were tapping undersea fibre-optic cables via bulk interception of internet traffic (Farrell 2019).

3 This is not a claim that social media disappears race, gender or class; it fully recognises that the demographics of social media users are not equal to those of the wider population (Boyd and Crawford 2012; Tufekci 2014).

 DOI: 10.19088/IDS.2021.010

'Guptabots' made headlines in 2016 as South Africa had its first experience of a concerted digital disinformation campaign. Guptabots were automated Twitter accounts that promoted the agenda of the influential Gupta family – financial backers of President Zuma. The bots were programmed to talk about 'white monopoly capital' in order to deflect attention from corruption scandals (Child 2017). This orchestrated campaign of 'computational propaganda' (Howard 2020) followed the appointment of UK political PR company Bell Pottinger as spin doctors for the Gupta empire (Fraser 2017).

The Gupta bot network (botnet) was first identified in November 2016 when the former public protector's 'State Capture' Report into the Guptas was criticised by citizens for being incorrect and biased. An analyst, Jean le Roux, identified around 100 accounts that were tweeting about the report (Van Zyl 2016). He demonstrated that many of the accounts were fake automated accounts – tweeting identical content within seconds of each other – and identified certain 'control' or seeding accounts that were supplying the content for retweets (*ibid.*).

Independent social media researcher Kyle Findlay was also seeing similar activity and highlighted a strange convergence between tweets from Andile Mngxitama, president of the Black First Land First political party and those of The New Age and ANN7 media companies (Superlinear 2016). Independently of one another, le Roux and Findlay had isolated a similar phenomenon of what appeared to be a botnet of pro-Zuma and pro-Gupta fake Twitter accounts, apparently coordinated in part by political marketing companies. The EFF also used disinformation to attack both the Commission of Inquiry into Tax Administration and Governance, and the Commission of Inquiry into Allegations of State Capture, in effect creating alternative narratives about the commissions in the public mind. The effectiveness of these campaigns ushered in an era of disinformation in South Africa, where social media was weaponised to spread campaigns built on falsehoods (Haffajee 2018). The work done by these local researchers highlights the beginnings of local capacity to identify and analyse government and non-state actors' use of digital disinformation.

The Government of South Africa has on occasion used 'democratic listening' processes to tap into the political concerns of the population. Democratic listening is often employed by governments as a rhetorical exercise undertaken for instrumental reasons to boost popularity when it is at a low ebb. But Sorensen *et al.* (2019) argue that such disingenuous claims risk dismissal and derision by increasingly cynical publics who are repeatedly subjected to governments' misleading gestures.

In 2015, the South African presidency embarked on a social media listening exercise in the weeks leading up to the state of the nation

 DOI: 10.19088/IDS.2021.010

address in response to accusations of corruption and lack of government responsiveness. The presidency invited contributions from the public on Twitter, asking users to make suggestions for what President Zuma should address in his speech. The public responded with more than a thousand messages directed at the presidency, disrupting the tightly controlled listening exercise, as citizens used the opportunity to conduct their own forum for public debate and commentary. Meanwhile, the president remained silent, giving no sign of having heard the public outcry.

## Table 4.1 Technology timeline

| Year | Shift | Implication |
|---|---|---|
| **2001** | 32% mobile ownership increases to 89% by 2011; a digital divide causes asymmetric access to the internet along race/class/gender lines. | SMS (text messaging) and social media open new civic spaces online. |
| **2005** | RICA legislation grants state power to intercept email and mobile communications. | Right to privacy reduced; chilling effect. |
| **2014** | Civic tech expansion; Amandla.mobi and Grassroot launched. | New mobile internet tools added to repertoire for opening civic space. |
| **2015** | Cynical 'democratic listening' by government highjacked by citizen advocacy. | New technique for opening space for voice and debate. |
| | #RhodesMustFall; #FeesMustFall; #ZumaMustFall | Citizen-led campaigns use social media to open new civic space. |
| **2016** | PR company Bell Pottinger's campaign for Zuma funders the Guptas stokes racial tension and deploys Guptabots on social media. | Coordinated disinformation closes space for authentic dialogue in digital space. |
| **2018** | EFF launches disinformation campaigns online. | Disinformation increasingly drowns out deliberation. |
| **2019** | Ruling on legal challenge brought by media group amaBhungane finds that parts of RICA legislation are unconstitutional. | Opens civic space. |
| **2020** | Covid-19 powers are introduced that re-enable state surveillance. | Closing civic space. |
| **2020** | #NotInMyName campaign C19 Coalition resists police violence. | Defending civic space. |

*Source:* Authors' own.

# 5. Digital rights landscape

The political landscape in South Africa provides positive benefits for digital rights in the form of a rights-based constitution, and an established culture of civic activism and strategic litigation, to robustly contest breaches of human rights. South Africa also enjoys a relatively strong technical infrastructure capable of providing digital platforms for public deliberation and online democracy initiatives. Unlike in many other countries in the region, the Government of South Africa has not generally sought to limit civic space with laws or regulations, and has not resorted to internet shutdowns, or to arresting citizens, bloggers or journalists for expressing dissenting views online.

However, access to the internet, smartphone ownership and affordable mobile data are not evenly distributed throughout the population. Therefore, the right to online freedom of opinion and expression, and to freedom of information, are also unequal. The government's increased use of surveillance and intercept technology brings into question citizens' right to privacy. There is currently a low level of civic literacy and civil society capability to effectively monitor and counter these measures, which shrink effective civic space and curtail digital rights.

Given the rapid expansion and proliferation of digital technologies to open and close civic space, current levels of digital literacy about disinformation, access to technology, and social media analytics capabilities are insufficient. Many CSOs operate with restricted technology and although mobile phone ownership has become affordable, data are still prohibitively expensive. Many CSOs are reliant on donated or entry-level computers and devices, and have very limited capacity when it comes to monitoring the online space. Despite the increase in the use of tech for civil society campaigns, and the rise of hashtag activism capacity for monitoring, the ability to analyse online activity and to respond strategically remains limited. For the most part, CSOs use digital technologies and social media in instrumental ways, without having the capability to effectively monitor and analyse digital activity and act strategically.

 DOI: 10.19088/IDS.2021.010

# 6. Digital rights in times of Covid-19

In March 2020, President Ramaphosa announced a state of disaster and national lockdown to curb the spread of coronavirus (Covid-19). The majority of citizens, excluding essential workers, were confined to their homes, with all non-essential travel banned. The global Covid-19 pandemic highlighted existing digital inequalities in South Africa. Those with access to digital technologies have, for example, been able to arrange virtual and telephone medical consultations, or use online shopping, to avoid crowded waiting rooms and grocery stores (Ahmed 2020). Digital inequalities in e-learning have also become starkly apparent, with the closure of schools and subsequent move to homeschooling and online learning. Many teachers and students have been unable to afford the data – and sometimes lack the digital skills – required to sustain online learning activities. Data costs in South Africa are among the highest in the world, and are the most expensive in Africa (Business Insider SA 2020b).

The Government of South Africa has used the national state of disaster to grant itself broad powers to do what it considers necessary to save lives. This potentially includes the powers of surveillance it awarded itself with RICA, but which were ruled unconstitutional (outside of a state of disaster) by the High Court. The emergency regulations compel mobile cellular providers to disclose the locations of possible contacts who may be infected with coronavirus. When these regulations were first published in April, civil society contested central provisions of the legislation, and the government issued amendments to ease concerns around people's constitutional right to privacy. They included locating the database within the health agency to reduce the ability of police or state security officials to access data for spying or political reasons (Wild 2020).

The government also used the opportunity to pass regulations that criminalised disinformation about the Covid-19 pandemic. The new regulations criminalise statements intended to deceive any person about Covid-19 or the government's response to the pandemic. They carry penalties including fines, imprisonment or both (CPJ 2020).

The Covid-19 emergency legislation also extended new powers to the army, which was mobilised to enforce lockdown rules, resulting in a wide range of human rights abuses. Social media, including Facebook and Twitter, was used by citizen journalists to document police and soldiers kicking, slapping, whipping and shooting citizens, as well as forcing people into humiliating positions as 'punishment' for alleged lockdown violations. Three citizens died at the hands of the police in the first week of lockdown (Knoetze 2020).

 DOI: 10.19088/IDS.2021.010

South Africa's independent media and civil society responded swiftly in an effort to defend rights and hold abusers accountable during lockdown (Faul 2020). Civil society organisation #NotInMyName held several protests against police brutality, linking events in South Africa to the killing in the United States (US) of US citizen George Floyd, which took place around the same time and mobilised #BlackLivesMatter campaigning internationally.

The C19 People's Coalition has been at the forefront of efforts to defend people's rights during the Covid-19 response, and has led calls for human rights abusers – the police, army and the state – to be held accountable during the lockdown. The coalition is an alliance of more than 310 social movements, trade unions, community organisations and NGOs rooted in social justice and democratic principles. C19 relies primarily on digital tools to create civic space to highlight abuse and demand justice; and provide legal advice and support to victims including a digital legal guide, *The Law During a State of Disaster and Human Rights Risks*, under its Legal Activism working group (C19 2020).

Technology is a major part of South Africa's Covid-19 strategy, further raising key issues with respect to surveillance. The Council for Scientific and Industrial Research uses a system that combines data from mobile phones, health records and government data sets. If an individual has been infected, health authorities receive an alert with the individual's contact information and an address, and begin tracing those who have recently been in close contact with the person (Wild 2020). In South Africa, a partnership between telecoms companies Telkom and Samsung resulted in the donation of 1,500 handsets (and free data) to allow trackers to identify infected people around the country (Chaturvedi 2020).

The government has also used the messaging platform WhatsApp to deliver information about the pandemic to millions of citizens in five languages; and created a WhatsApp helpline, which is updated with information from the latest World Health Organization briefings, and local and international news outlets, to provide real-time updates. It uses artificial intelligence to provide information as well as dispel misinformation (South African Government News Agency 2020). In September 2020, the government introduced a Covid-19 tracing app, which was zero rated (i.e. free to use) by mobile networks. The app uses Bluetooth technology to alert users if they have been in contact with any other users who subscribe to the app who have tested positive for Covid-19 within the past 14 days (Business Insider SA 2020a).

 DOI: 10.19088/IDS.2021.010

# 7. Conclusion and recommendations

South Africa has existing strengths in rights-based and digital campaigning, and has experience of researching digital disinformation by non-state actors. This is a stronger starting position than many of its neighbours. However, the rapid pace of technological change, and rapidly growing repertoire of state and private sector technologies being deployed to close civic space, mean that urgent action needs to be taken. On the basis of this preliminary analysis a number of recommendations arise:

- Work with citizens to raise public awareness about digital rights and emerging threats including disinformation and online manipulation.
- Work with CSOs to build the capacity of journalists, CSOs and universities to monitor, analyse and effectively respond to the use of digital technologies to close civic space and limit digital rights.
- Work with legal rights activists and policymakers to understand emerging threats and devise regulatory, legislative and strategic litigation responses.
- Work with researchers to better understand who is using which technologies to open and close civic space, and how best to enhance citizens' ability to express, defend and expand their digital rights.

A programme of engaged participatory action research with and by with citizens and CSOs would be the best way to answer these research questions and address the gaps in knowledge and capacity identified in this preliminary research.

 DOI: 10.19088/IDS.2021.010

# References

Ahmed, A. (2020) ***How Covid-19 Exposes the Defects in South Africa's Digital Economy***, Research ICT Africa blog, 26 March (accessed 16 October 2020)

Akinboade, O.A.; Mokwena, M.P. and Kinfack, E.C. (2013) 'Understanding Citizens' Participation in Service Delivery Protests in South Africa's Sedibeng District Municipality', *International Journal of Social Economics* 40.5: 458–78

Alexander, P. (2010) 'Rebellion of the Poor: South Africa's Service Delivery Protests – a Preliminary Analysis', *Review of African Political Economy* 37.123: 25–40

Atkinson, D. (2007) 'Taking to the Streets: Has Developmental Local Government Failed in South Africa', in S. Buhlungu, J. Daniel, R. Southall and J. Lutchman (eds), *State of the Nation: South Africa 2007*, Cape Town: HSRC Press

Ballard, R.; Habib, A.; and Valodia, I. (2006) 'Conclusion: Making Sense of Post-Apartheid South Africa's Voices of Protest', in Ballard, R.; Habib, A. and Valodia, I. (eds), *Voices of Protest: Social Movements in Post-Apartheid South Africa*, Scottsville: University of KwaZulu-Natal Press

Bennett, W. and Segerberg, A. (2013) *The Logic of Connective Action*, Cambridge: Cambridge University Press

Beresford, A. (2015) 'Power, Patronage, and Gatekeeper Politics in South Africa', *African Affairs* 114.455: 226–48

Booysen, S. (2007) 'With the Ballot and the Brick: the Politics of Attaining Service Delivery', *Progress in Development Studies* 7.1: 21–32

Bosch, T. (2017) 'Twitter Activism and Youth in South Africa: The Case of #RhodesMustFall', *Information, Communication & Society* 20.2: 221–32

Bosch, T. (2016) 'Twitter and Participatory Citizenship: #FeesMustFall in South Africa', in B. Mutsvairo (ed.), *Digital Activism in the Social Media Era*, London: Palgrave Macmillan

Bosch, T. *et al.* (2019) Creativity and Strategy: How Civil Society Organizations Communicate and Mobilize in Egypt, Kenya, Serbia and South Africa, in K. Voltmer *et al.* (ed.), *Media, Communication and the Struggle for Democratic Change*, London: Palgrave Macmillan

Boyd, D. and Crawford, K. (2012) **'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon'**, *Information, Communication and Society* 15: 662–79, DOI: 10.1080/1369118X.2012.678878 (accessed 23 October 2020)

Burger, J. (2009) 'The Reasons Behind Service Delivery Protests in South Africa', *Institute for Security Studies*, 29 July

Business Insider SA (2020a) **'Ramaphosa Urges South Africans to Use the Covid-19 Tracing App – Here's How it Works'**, 16 September (accessed 23 October 2020)

Business Insider SA (2020b) **'SA Has Some of Africa's Most Expensive Data'**, 5 May (accessed 16 October 2020)

C19 People's Coalition (2020) ***The C19 People's Coalition*** (accessed 26 June 2020)

Carnegie Endowment for International Peace (2019) ***AI Global Surveillance Technology*** (accessed 23 October 2020)

Chaturvedi, A. (2020) **'How South Africa Uses Tech to Fight Covid-19'**, *GeoSpatial World*, 21 April (accessed 16 October 2020)

Child, K. (2017) **'Twitter Finally Silences Abusive Gupta Bots'**, *Business Day*, 11 December (accessed 29 June 2020)

Chiumbu, S. (2015) **'Social Movements, Media Practices and Radical Democracy in South Africa'**, *French Journal for Media Research* 4/2015 (accessed 23 February 2018)

Clement, J. (2019) ***Internet User Penetration in South Africa from 2017 to 2023***, Statista (accessed 26 June 2020)

Civic Space Watch (2020) ***Civic Space*** (accessed 23 October 2020)

Civic Tech (2020) ***Civic Tech in South Africa*** (accessed 25 June 2020)

CIVICUS (2020) ***Civic Space*** (accessed 23 October 2020)

CIVICUS (2016) ***South Africa Overview*** (accessed 24 June 2020)

CPJ (2020) **'South Africa Enacts Regulations Criminalizing 'Disinformation' on Coronavirus Outbreak'**, *Committee to Protect Journalists*, 19 March (accessed 25 June 2020)

Dodson, B. (2010) 'Locating Xenophobia: Debate, Discourse, and Everyday Experience in Cape Town, South Africa', *Africa Today* 56.3: 2–22

Duncan, J. (2014) 'South African Journalism and the Marikana Massacre: A Case Study of an Editorial Failure', *The Political Economy of Communication* 1.2

Farrell, N. (2019) **'UK and South African Government are Tapping Sea Cables'**, *Fudzilla*, 9 September (accessed 23 October 2020)

Faul, A. (2020) **'State Abuses Could Match the Threat of COVID-19 Itself'**, *ReliefWeb*, 2 April (accessed 25 June 2020)

Foley, M. and Edwards, B. (1996) 'The Paradox of Civil Society', *Journal of Democracy* 7.3: 38–52

Fraser, A. (2017) **'We Go Inside the Guptabot Fake News Network'**, *Tech Central*, 4 September (accessed 29 June 2020)

Freedom House (2019) ***Freedom in the World*** (accessed 4 December 2020)

Haffajee, F. (2018) **'How the EFF Dominates the Disinformation Market'**, *Daily Maverick*, 12 December (accessed 29 June 2020)

Hickel, J. (2014) '"Xenophobia" in South Africa: Order, Chaos, and the Moral Economy of Witchcraft', *Cultural Anthropology* 29.1: 103–27

Hillman, J.E. and McCalpin, M. (2019) **'Watching Huawei's "Safe Cities"'**, *CSIS Brief,* Washington DC: Center for Strategic and International Studies (accessed 23 October 2020)

Howard, P. (2020) *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations and Political Operatives*, London: Yale University Press

Howell, S. (2019) 'Description of the South African Context', in W. Heitmeyer (ed.), *The Codes of the Street in Risky Neighborhoods*, Cham: Springer

HSRC (2014) ***Enhancing Digital Citizen Engagement: Lessons from South Africa. Notes from the World Social Science Forum 2013***, Pretoria: Human Sciences Research Council (accessed 25 June 2020)

ITU (2020) ***Internet Access Statistics***, International Telecommunication Union (accessed 4 December 2020)

Knoetze, D. (2020) **'Details of Two Additional Alleged Lockdown Killings by Police Revealed'**, *GroundUp*, 30 April (accessed 25 June 2020)

Kode, D. (2018) ***Civic Space Restrictions in Africa: How Does Civil Society Respond?***, Conflict Trends 2018/1, Accord (accessed 24 June 2020)

Lindeque, M. (2020) **'This WhatsApp Chat Will Tell You Everything About Covid-19 in SA'**, *Eyewitness News*, 16 March (accessed 25 June 2020)

Madlingozi, T. (2007) 'Post-Apartheid Social Movements and the Quest for the Elusive "New" South Africa', *Journal of Law and Society* 34.1: 77–98

Masweneng, K. (2019) **'South Africans Pay More for Data: See By How Much Here'**, *Times Live*, 3 December (accessed 23 October 2020)

Mbali, M. (2004) 'AIDS Discourses and the South African State: Government Denialism and Post-Apartheid AIDS Policy-Making', *Transformation: Critical Perspectives on Southern Africa* 54.1: 104–22

Nordea (2020) ***The Political Framework of South Africa*** (accessed 1 July 2020)

Omarjee, L. (2020) **'Explainer: Why You Should Care that Parts of RICA are Unlawful'**, *Fin24*, 18 September (accessed 29 June 2020)

 DOI: 10.19088/IDS.2021.010

Oxfam (2018) **'Space to Be Heard: Mobilizing the Power of People to Reshape Civic Space'**, Oxfam Briefing Note, Oxford: Oxfam International (accessed 25 June 2020)

Pikoli, Z. (2020) **'Civil Society Health Organisations Launch Covid-19 Survey'**, *Daily Maverick*, 21 April (accessed 1 July 2020)

Reventlow, N.J. (2017) ***Digital Rights are *All* Human Rights, Not Just Civil and Political***, Berkman Klein Centre for Internet & Society blog, 27 February (accessed 23 October 2020)

Roberts, M. (2019) **'South African Youth, Disruptive Politics, and Apathy Towards Voting'**, *Transformer* 20.1: 39–43 (accessed 25 June 2020)

Robertson, D. (2018) **'How an Obscure Conservative Theory Became the Trump Era's Go-to Nerd Phrase'**, *Politico*, 25 February (accessed 25 February 2018)

Sabi, S. and Rieker, M. (2017) 'The Role of Civil Society in Health Policy Making in South Africa: A Review of the Strategies Adopted by the Treatment Action Campaign', *African Journal of AIDS Research* 16.1: 57–64

Schulz-Herzenberg, C. (2014) 'Voter Participation in the South African Elections of 2014', *Policy Brief* 61, Pretoria: Institute for Security Studies

Simelela, N. and Venter, W. (2014) 'A Brief History of South Africa's Response to AIDS', *SAMJ: South African Medical Journal* 104.3: 249–51

Smidt, H. (2018) ***Shrinking Civic Space in Africa: When Governments Crack Down on Civil Society***, GIGA Focus Africa 4, Hamburg: German Institute of Global and Area Studies (accessed 29 June 2020)

Sorensen, L.; FordWalid, H.; Al-Saqaf, W. and Bosch T. (2019) 'Dialogue of the Deaf: Listening on Twitter and Democratic Responsiveness during the 2015 South African State of the Nation Address', in K. Voltmer *et al.* (eds), *Media, Communication and the Struggle for Democratic Change: Case Studies on Contested Transitions*, Cham: Palgrave Macmillan

South African Government News Agency (2020) **'Access all Covid-19 Facts via WhatsApp'**, 21 March (accessed 16 October 2020)

Staff Writer (2019) **'High Court Finds that South Africa's Surveillance Act RICA is Inconsistent with the Constitution'**, *Business Tech*, 16 September (accessed 29 June 2020)

Superlinear (2019) **'The Curious Case of the Short-Lived "Ayobots"'**, 4 June (accessed 29 June 2020)

Superlinear (2016) **'Black First, Land First and #PravinMustGo'**, 4 September (accessed 29 June 2020)

TAC (2020) ***Our History***, Treatment Action Campaign (accessed 1 July 2020)

TAC (2016) **'Mbeki Shows No Remorse for Role in AIDS Deaths'**, 8 March (accessed 1 July 2020)

Tufekci, Z. (2014) 'Big Questions for Social Media Big Data: Representativeness, Validity and Other Methodological Pitfalls', in ICWSM 14: Proceedings of the 9th International AAAI Conference on Weblogs and Social Media

UN (2015) *Sustainable Development Goals*, New York NY: United Nations

UN (2011) *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Frank La Rue, Human Rights Council, Seventeenth Session Agenda Item 3, United Nations General Assembly

Van Zyl, G. (2016) **' "Sockpuppet" Twitter Accounts Used in #HandsOffGuptas Information War'**, *Fin24* (accessed 25 June 2020)

Voigt, E. (2020) **'Covid-19: Progress on Cell Phone Tracking, but Concerns Remain'**, *Spotlight*, 6 April (accessed 23 October 2020)

Wild, S. (2020) **'Antipoaching Tech Tracks Covid-19 Flare-ups in South Africa'**, *Scientific American*, 12 May (accessed 23 October 2020)

World Bank (2019) ***The World Bank in South Africa*** (accessed 23 October 2020)

Yang, G. (2009) *The Power of the Internet in China: Citizen Activism Online*, New York NY: Columbia University Press

 DOI: 10.19088/IDS.2021.010

# Nigeria Digital Rights Landscape Report

Oyewole Oladapo and Ayo Ojebode



This report is part of 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries'; the Introduction is also recommended reading.

© 2021 Oyewole Oladapo and Ayo Ojebode © Institute of Development Studies. DOI: 10.19088/IDS.2021.011

# 1. Introduction

Nigeria has witnessed a high level of adoption of digital devices and technologies in the past 20 years. Adoption of those new technologies has brought transformations to different aspects of life at the individual, group, and societal levels. Those transformations are easily observable in the civic space. What used to be private has become public and connectedness, especially via mobile telephony and social media, which now appear commonplace, were at best only imagined until recently. Thanks to digital technologies, voiceless sections of Nigerian society such as women, minority groups, and victims of violence now have a voice, which can be amplified to the extent to which they can adopt and manipulate these technologies. Political corruption has also become voiced through these technological advancements.

The disruption caused by digital technologies has also invited new laws, particularly from the Federal Government of Nigeria and its ministries and agencies: the government institutions that were not used to citizens demanding accountability from them (Bischoff 2020). All of this is happening at a time when the civic space globally has been found to be shrinking or closing. The same fate that befell Nigerian civic space in the pre-democracy era of military dictatorship is fast befalling it again in the current democratic dispensation, and its effects are extending from physical spaces into digital ones.

The civic space, which is described as 'the layer between state, business, and family in which citizens organise, debate and act' (Buyse 2018: 967) is said to be shrinking or closing when there are restrictions placed on the activities of civic actors. The restrictions, which mainly come from governments, may be executed through different strategies such as 'political, administrative and extra-legal, including violence, threats, de-legitimation, the use of the law to criminalise civic activism, and stigmatisation' (Hossain *et al.* 2019: 6). The restrictions are characterised by denial of right of access to spaces where people express views and opinions that appear to be critical of governments, and criminalisation of actions directed at demanding accountability from constituted authorities. In the last 20 years, just as the civic space has extended from geographical spaces to cover digital spaces, so have attacks on it, especially from governments.

 DOI: 10.19088/IDS.2021.011

In recognition of digital spaces as an extension of the physical civic space, governments have introduced legislations which are capable of abridging right of access to them as they do with geographical spaces. Protest mobilisation, actual protests, and other forms of civic action have been organised on digital platforms across the world, in democratic and non-democratic countries alike. In Nigeria, the first nationwide online protest so far with complementary offline protest took place on 2 January 2012, when individuals and groups from all the 36 states and the Federal Capital Territory trended the hashtag #OccupyNigeria on Twitter and other social media (Uwalaka and Watkins 2018). The protest, which was mobilised significantly online, led to the shutdown of state capitals and major towns in the demand for the reversal of fuel subsidy removal.

Since #OccupyNigeria, online protests have become common in Nigeria. Global connectivity and the rapidness with which information flows on digital platforms especially, pitches governments against the use of digital platforms for civic action such as protests. Just like the Nigerian government has been doing in the past few years, most governments across the world have been found to have taken specific actions to stifle free speech or abridge rights to freedom of association in the digital space (Bischoff 2020). In Nigeria, civil society groups and citizens have always risen up against such measures that restrict digital rights by using the same digital technologies. Despite continuous advocacy for civil rights, violations of digital rights are growing in Nigeria.

In the internet era, digital rights are described as human rights, an extension of the equal and inalienable rights of humans (Hutt 2015). The Human Rights Council of the United Nations (2016: 3) declares that:

> the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

This report presents an overview of digital rights in Nigeria with a view to highlighting the contextual realities that promote or constrain those rights.

 DOI: 10.19088/IDS.2021.011

# 2. The political landscape

The date of 29 May 2020 marks 21 years since Nigeria returned to democratic rule. The political context of the country has seen a lot of positive transformations, the most outstanding of them being that there has not been any extra-legal disruption to the four-year tenure of political office holders at the federal and state levels. Periodic election, which is a core element of democracy, has been upheld every four years. This stability has made political parties the primary formal machinery for seeking and acquiring political power in the country. This political development is unfolding at a time when access to the internet and adoption of diverse digital technologies are also growing. Different sections of Nigerian society have adopted digital technologies for different purposes: the government for general governance, information dissemination, and election administration; politicians and political parties for political mobilisation; and civil society groups and citizens for civic action, among other uses.

However, what has been most defining in Nigeria's political landscape is the adoption of digital technologies for election administration and management. This has so far had numerous implications for digital rights in Nigeria. Digital technology was first widely used in Nigerian elections in 2015. The Independent National Electoral Commission (INEC) issued the electorate the Permanent Voter's Card which is to be authenticated on election day using a biometric smart card reader. However, on election days, the technology malfunctioned in many places and election officials had to resort to manual accreditation and voting procedures. There were claims and counterclaims of deliberate sabotage of the technology to rig the elections in favour of the dominant parties. The battle was intense on social media between the supporters of the All Progressive Congress (APC) and the Peoples Democratic Party (PDP). Former President Goodluck Jonathan lost the election which was won by Gen. Muhammadu Buhari, who also won a re-election in 2019.

Since the 2015 elections, the civic space in Nigeria has been polarised with supporters of former President Goodluck Jonathan and his PDP on the one side and supporters of the current President Muhammadu Buhari on the other side. The supporters of the former are branded in social media platforms and media discourse in general as 'wailers' while those of the former are christened 'hailers' (Ibrahim 2015). This simplistic typology of actors in the civic space, which was introduced into public discourse

 DOI: 10.19088/IDS.2021.011

by Femi Adesina, Special Adviser to President Muhammadu Buhari on Media and Publicity, summed up all views critical of the government as being politically motivated. In other words, to criticise the actions of the current government or to demand accountability from it is to be seen and treated as a member of the opposition party PDP. The typology regards all civil society organisations (CSOs), non-governmental organisations (NGOs), faith-based organisations (FBOs), media organisations such as newspapers, television, radio, and blogs, and even individuals that are critical of government, as not just being against the government but also in support of the ex-ruling party. This polarisation has been defining for Nigerian civic space since 2015 when President Muhammadu Buhari assumed office.

 DOI: 10.19088/IDS.2021.011

# 3. The civic space landscape

The chaos that characterised the Nigerian political context always spills over into the civic space. In fact, Nigeria's return to democracy was not achieved without the activities of vibrant civil society groups, individual activists, and public intellectuals, radio, newspapers, and news magazines that stood up to the country's military dictators. The period between the cancellation of the 12 June 1993 presidential election allegedly won by Chief MKO Abiola and the eventual military handover to the civilian government on 29 May 1999 witnessed different shades of civic activism in the country.

For example, in 1993, *Tell* Magazine launched guerrilla journalistic reporting after its publications were seized and its premises shut by the tyrannical military government of General Sani Abacha for exposing government secrets and calling global attention to violations of human rights in the country (Ojebode 2011). That same year, four of *Tell*'s senior editors were arrested and detained by the government (*ibid.*). Activists and opposition politicians were arrested for treason and detained for months without trial even after the court dismissed the case (Immigration and Refugee Board of Canada 1997). The period was characterised by the arrest, imprisonment, murder, and disappearances of those who spoke against the inhumanity of military rule in the country. Nevertheless, the end of military rule did not end such occurrences. The rest of this section presents a highlight of landmark events which had implications for the closing and opening of Nigerian civic space between 2000 and 2020. Throughout this time, Nigeria's ranking on Freedom House's Freedom Index has hovered within the 'partially free' bracket as civic space experiences a seesaw between events that partially open and close civic space (see Figure 3.1).

 DOI: 10.19088/IDS.2021.011

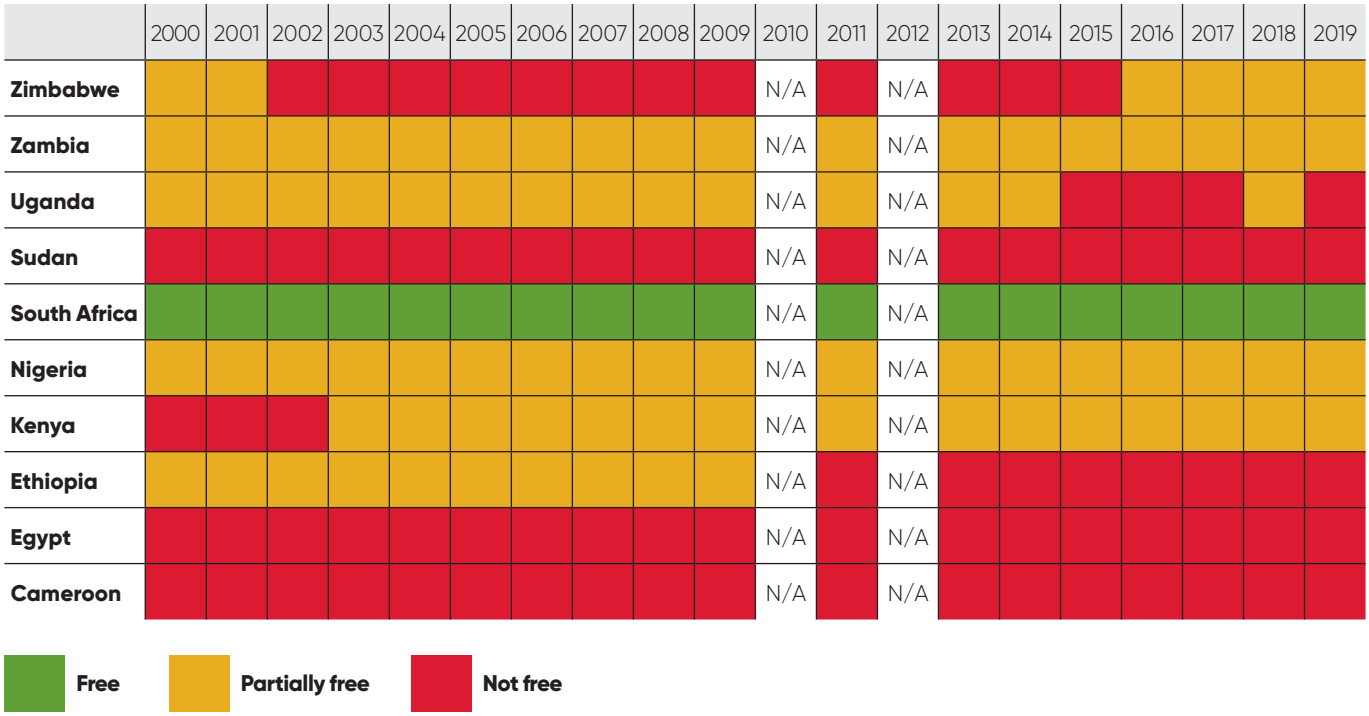
# Table 3.1 Opening of the civic space

| Year | Shift | Implications |
|---|---|---|
| **2004** | Emergence of 234Next, the country's first online newspaper | Opening of space for journalists |
| **2005** | Arrest, imprisonment, and assassination of bloggers and journalists | Closing of space for bloggers and journalists |
| **2010** | Emergence of civil society groups leveraging digital technologies to empower citizens and demand accountability from government | Opening of space for civic society groups |
| **2014** | Same Sex Marriage (Prohibition) Act | Closing of space for LGBTI and other sexually non-binary individuals and groups |
| **2015** | Licensing of first set of community radio stations | Opening of space for especially rural and underserved community dwellers |
| | Frivolous Petitions Bill rejected | Induced fear of imminent closing of space for journalists, bloggers, and social media users |
| | Arrest of activists | Closing of space for human rights activists |
| | Emergence of a woman-led KOWA Party | Opening for women politicians |
| **2015–20** | Police brutality against protesters | Closing of space for human rights activists, CSOs, journalists, and citizens |
| **2016 (reintroduced in 2019)** | Rejection of Gender and Equal Opportunities Bill by the Senate | Closing of space for girls and women |
| **2016 (revisited in 2019)** | NGO Regulation Bill, still under consideration before the Legislature | Closing for CSOs, NGOs, and FBOs |
| **2017** | Increased number of government-owned and private FM radio stations | Opening of space for journalists and media consumers |
| **2019** | Open Treasury Portal providing online access to expenses incurred by government ministries, departments, and agencies | Opening of space for civil society groups working on public accountability |
| | Nigeria Data Protection Regulation | Opening of space and protection from privacy violation for journalists, bloggers, CSOs, NGOs, and all users of social and other digital media platforms |
| | Hate Speech Bill | Closing of space for journalists, bloggers, CSOs, NGOs, and all users of social and other digital media platforms |
| | Protection from Internet Falsehoods and Manipulations and Other Related Matters Bill | Closing of space for journalists, bloggers, activists, CSOs, NGOs, and all users of social and other digital media platforms |
| | Digital Rights Bill – presidential assent withheld | Closing of space for journalists, bloggers, CSOs, NGOs, and all users of social and other digital media platforms |
| **2020** | Proposed licensing of online radio and television | Closing of space for journalists |
| | Corporate and Allied Matters Act 2020 empowers government agencies to reconstitute board of trustees of CSOs, NGOs, and FBOs | Closing of space for CSOs, NGOs, and FBOs |

*Source:* Author's own.

 DOI: 10.19088/IDS.2021.011

## Figure 3.1 Freedom House ranking for ADRN countries, 2000–19[1]




*Note:* ADRN – African Digital Rights Network.

*Source:* Adapted from Freedom House (2019)

The information presented in Table 3.1 reveals that events and decisions that can open the Nigerian civic space and those that can further close it have been happening concurrently over the years. It is striking to note that the media landscape has become diverse and has widened to reach previously underserved sections of the country. With the commencement of community radio licensing, rural communities have gained access to information and the right to be creators of media content. An increased rate of licensing government-owned and commercial FM radio stations also has improved radio penetration across the country. All of these, coupled with the emergence of online newspapers, radio, and television, pluralise the country's information landscape, providing people with alternative information sources. As the media and journalism space widens for journalists to practise in, it also opens for citizens to consume and co-create information.

Despite that, certain actions of government are either closing or threatening to close the Nigerian media space and the civic space in general. Of particular interest among such actions is legislations (Ibezim-Ohaeri 2017) which are capable of stifling free speech, especially on digital

1 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.011

communication technologies. For example, the Protection from Internet Falsehoods and Manipulation and Other Related Matters Bill (2019)[2] criminalises sharing information that can diminish public confidence in the performance of any duty or function of, or in the exercise of any power of, the Nigerian government. This is a problematic provision whose lack of specificity can be taken advantage of to silence voices that are critical of government.

The same bill also criminalises the operation of parody accounts on social media and stipulates a fine and/or a prison term for its violation. In spite of the fact that the bill has not been passed into law, the Nigerian police arrested Babatunde Olusola, a Nigerian university student, for operating on Twitter a parody account in the name of former President Goodluck Jonathan (Akinkuotu 2020). The bill poses a danger to activists that may employ creative devices for communicating their critique of government. The Hate Speech Bill (2019) also prescribes a life sentence or a death sentence for propagating hate speech (Abdulrauf 2019). Journalists from media companies that are perceived to be in opposition to the government are at greater risk of falling victim to the provisions of these legislations. For example, Nigeria's Department of State Services (DSS) arrested a student journalist Ayoola Babalola for criticising President Muhammadu Buhari and another member of the ruling All Progressive Congress (APC), Bola Tinubu. The court later granted him bail on a bond of N150,000 (Sahara Reporters 2020). Activists and CSOs that are often critical of government are equally at risk. The chilling effects of legislations such as these ones are capable of closing the civic space.

Furthermore, women and sexually non-binary people are potential victims because policymakers guard the country's hegemonic positions on issues of gender and sex. The Nigerian Senate's rejection of the Gender and Equal Opportunities Bill (2016) is a setback to the campaign for gender equality in the country. Analysts consider 2015 to be the inception of the worst era for civic actors in Nigeria since the end of military rule in 1999, in terms of government restriction of rights (Ibezim-Ohaeri 2017). As reflected in the information presented in Table 3.1, more restrictive laws were introduced between 2015 and 2020 than in the preceding 15 years. The year 2015 is significant because it marked the ascension to power of former military dictator Muhammadu Buhari as a democratic president of Nigeria. From the trend established in Table 3.1, Nigerian civic space under the leadership of President Muhammadu Buhari cannot be said to be thriving as it should in an ideal democracy.

2 See **Protection from Internet Falsehoods and Manipulation and Other Related Matters Bill 2019**, SB 132, 9th National Assembly.

 DOI: 10.19088/IDS.2021.011

# 4. The technology landscape

Nigeria has witnessed a great deal of technological transformation in the last 20 years. The most fundamental of them is the introduction of Global System for Mobile (GSM) communication in 2001. In the last two decades, the number of mobile network service providers has increased, just as their range of services has. All service providers offer call, text, and internet services and the majority of Nigerians access the internet on their mobile phones. The quality of internet service in the country varies based on service provider and user location. By 2019, all operating mobile network service providers have upgraded their services from 2G and 3G to 4G. Table 4.1 provides an overview of mobile telephone penetration in the last 20 years.

## Table 4.1 Uptake of mobile telephone services in Nigeria

| Mobile telephone subscription | 2002 | 2005 | 2010 | 2015 | 2020 (May) |
|---|---|---|---|---|---|
| **Number of subscribers** | 2,271,050 | 19,519,154 | 88,348,026 | 151,017,244 | 192,267,890 |
| **Percentage increase (%)** | 0 | 759.5 | 352.6 | 70.9 | 27.3 |
| **Teledensity**[3] | 1.89 | 16.27 | 63.11 | 107.87 | 100.72 |

*Source:* NCC.[4]

One year after the inception of GSM in Nigeria, in 2002, there were less than 2.3 million subscribers. Four years later, in 2004, the number of subscribers has increased more than seven times. The percentage increase predictably slowed down by 2015 because more people had already subscribed to the service. It is also noteworthy that compulsory Subscriber Identity Module (SIM) card registration began in 2015. This registration could also have played a role in the observed trend. As of May 2020, there are over 192 million subscribers in the country. Internet subscribers have also been increasing in the last 20 years.

3 Teledensity was calculated based on a population estimate of 126 million up to December 2005; from December 2006, teledensity was based on a population estimate of 140 million; from December 2007 it was based on active subscribers; from December 2001 to 2006, it was based on connected subscribers.

4 See **Nigerian Communications Commission Industry Statistics: Annual (2002–19)**.

 DOI: 10.19088/IDS.2021.011

## Table 4.2 Mobile (GSM) internet subscribers

| Date | Internet subscribers | New subscribers | Percentage increase (%) |
|---|---|---|---|
| **December 2012** | 30,939,112 | 0 | |
| **December 2013** | 64,229,097 | 33,289,985 | 107.6 |
| **December 2014** | 76,324,632 | 12,095,535 | 18.8 |
| **December 2015** | 97,032,543 | 20,707,911 | 27.1 |
| **December 2016** | 91,880,032 | -5,152,511 | -5.3 |
| **December 2017** | 98,391,456 | 6,511,424 | 7.1 |
| **December 2018** | 111,632,516 | 13,241,060 | 13.5 |
| **December 2019** | 125,728,328 | 14,095,812 | 12.6 |
| **May 2020** | 140,761,851 | 15,033,523 | 12 |

*Source:* NCC.[5]

The number of internet subscribers has also been increasing in the last 20 years. It was only in 2016 when the Nigerian economy was in recession that the country recorded a decrease in the number of internet subscribers. As of May 2020, there are over 140 million internet subscribers in Nigeria and broadband penetration has also been increasing in the last 20 years.

## Table 4.3 Internet broadband services in Nigeria

| Date | January 2017 | January 2018 | January 2019 | January 2020 |
|---|---|---|---|---|
| **Number of subscriptions** | 41,403,821 | 38,117,147 | 61,732,130 | 73,466,093 |

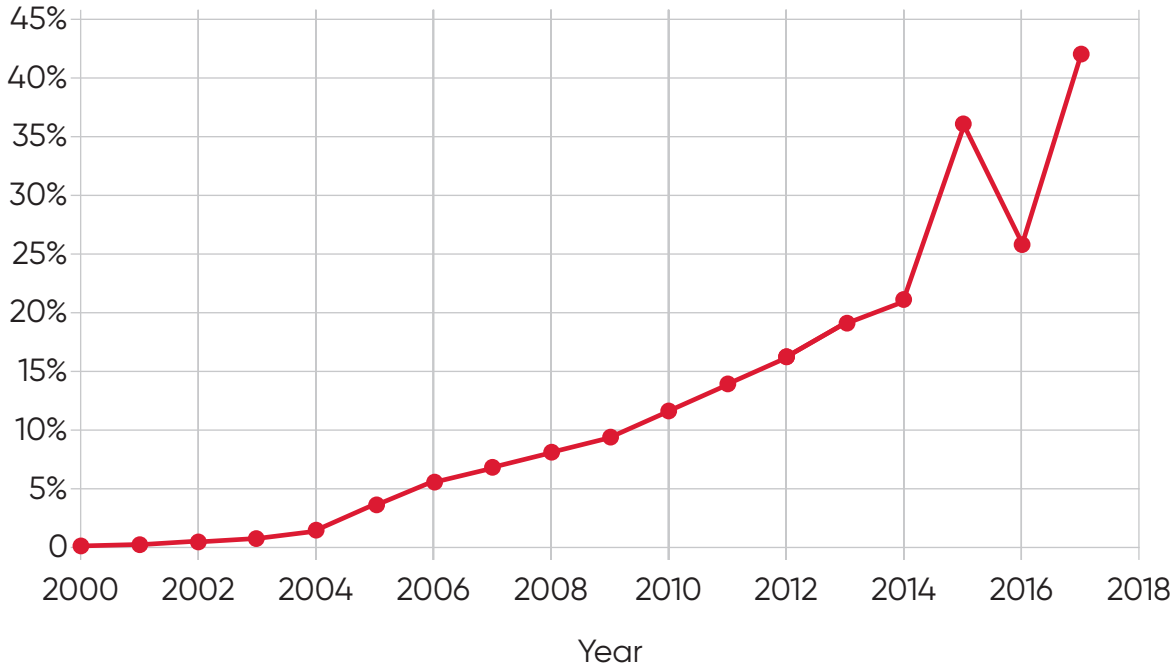
*Source:* NCC.[6]

Internet broadband penetration is slower than the general internet penetration rate.

5 See **Nigerian Communications Commission Industry Statistics: Annual (2002–19)**.
6 See **Nigerian Communications Commission Industry Statistics: Annual (2002–19)**.

 DOI: 10.19088/IDS.2021.011

## Figure 4.1 Percentage of the population with internet access in Nigeria




*Source:* Based on data from ITU (2020)

The number of internet users in Nigeria as presented by ITU is far lower than given by the country's communications body, the Nigerian Communications Commission (NCC – see Table 4.2). This is understandable because NCC data are based on telecommunications services subscribers. As a result, the data do not exclude cases of multiple subscriptions by individuals – a common practice in Nigeria – and neither do they account for business and corporate subscribers. ITU data are modelled based on individuals using the internet and thus give a more realistic picture of internet penetration in the country. As shown in Figure 4.1, individual internet users in Nigeria rose from 0.064 per cent of the population in 2000, to 11.5 per cent in 2010, and to 42 per cent in 2019. Therefore, although approximately 60 per cent of Nigerians remained without internet access in 2019, one could say that it has been a near-steady climb.

## 4.1 Social media use in Nigeria

Nigerians across age, sex, and literacy level use social media for different purposes. However, the use of social media for civic action is popular in Nigeria. Facebook, established in 2004, was the first social media platform that became popular in Nigeria. When Twitter was established in 2006, Nigerians also adopted it in large numbers. While some migrated completely to Twitter, some keep both Facebook and Twitter accounts. It is common in the country to operate multiple social media accounts. Instagram and

 DOI: 10.19088/IDS.2021.011

other platforms that were introduced later have also seen Nigerians open accounts on them in large numbers. Nevertheless, Twitter and Facebook remain the foremost social media platforms in use. According to Statista.com, Nigeria's social media users totalled 27.6 million in 2017, 29.3 million in 2018, an estimated 30.9 million in 2019, and an estimated 32.4 million in 2020 (Statista 2020). Simon Kemp's DataReportal, which puts total social media users in the country at 27 million, states that there was an increase of 3.4 million between 2019 and 2020 with a 13 per cent penetration (Kemp 2020).

Individuals and groups in Nigeria have come to depend on social media for public engagement. The development is not out of place as Nigerian political leaders have also become largely visible on the various social media platforms. Facebook, with a 59.57 per cent penetration of the country's total internet users, ranks first among the social media platforms that Nigerians use for public discourse. It is followed by Twitter with a 24.54 per cent penetration of internet users (GlobalStats 2020). Both Facebook and Twitter have contributed significantly to the opening of online civic spaces in Nigeria. Users have always been on alert to protest any attempt by the government to restrict access to the platforms or to silence critical voices. Between 2012, when #OccupyNigeria trended on Twitter and Facebook, to the present, offline protests have become risky as a result of the frequent police brutalisation of protesters. Nigerians have taken to social media as alternative platforms for voicing their dissatisfaction with the government and for demanding accountability.

One advantage that online civic action has over offline is the immediacy of global attention to it without a dependence on the mainstream media. Nigerians have attracted global attention to local issues on a number of occasions. Hashtag trending is one of the major strategies employed to pursue their causes. Some of the popular hashtags are presented in Table 4.4.

## Table 4.4 Key digital hashtag campaigns and actors

| **Year** | Hashtag | Actor |
|---|---|---|
| **2012** | #OccupyNigeria | Opposition politicians, celebrities, and activists |
| **2014** | #BringBackOurGirls | Bring Back Our Girls movement |
| **2015, 2019** | #NoToSocialMediaBill | Social media influencers |
| **2017** | #ENDSARS | Social media influencers |
| **2019** | #SexForGrade | BBC, social media influencers |
| **2019–2020** | #Buharimustgo | Social media activists |

*Source:* Authors' own.

 DOI: 10.19088/IDS.2021.011

Led by opposition politicians, celebrities, and activists, #OccupyNigeria was a hashtag that trended in 2012 to mobilise the public against an increase in fuel prices by the government. The movement later brought people onto the streets, resulting in the complete shutdown of important cities across the country. #BringBackOurGirls called attention to the 2014 abduction of over 200 Chibok girls abducted by Boko Haram terrorists in Northern Nigeria.

The #NoToSocialMediaBill hashtag trended in 2015 (Oladapo and Ojebuyi 2017) and again in 2019 to protest bills that sought to criminalise social media use for critical political commentary in the country. #ENDSARS has been trending since 2017 to call government attention to the abuse of power by members of the Special Anti-Robbery Squad of the Nigeria Police. The BBC was behind the #SexForGrade hashtag with a documentary which exposed the sexual exploitation of students of Nigerian and Ghanaian universities for grades. The documentary drew attention to the plights of women in a Nigerian higher institution of learning where sexual predatory behaviour was common (Malaea 2019).

## 4.2 The government's capacity to respond

There have been speculations that the Nigerian government planned to launch spy satellites, block websites and blogs that are critical of the government and its performance, and place mobile phones under surveillance (Okunoye 2017). Beyond the speculations, in 2013, the Nigerian government under President Goodluck Jonathan contracted an Israeli company, Elbit Systems, for US$40 million to monitor online communication in the country (Ogala 2013). Carnegie Endowment for International Peace, which describes Nigeria as an electoral autocracy, states that the Nigerian government uses artificial intelligence technology from China's Huawei tech giant to monitor citizens (Carnegie Endowment for International Peace 2020).

The foregoing revelations reveal that the Nigerian government has for a long time been developing surveillance capacity which can undermine citizens' fundamental rights. Although Section 3.3 of the Nigerian Communications Commission's (NCC) Internet Code of Practice specifically directs that no service provider can block internet access to contents, devices, and applications that are lawful except for the purpose of network management (NCC 2019a), no one can be too sure how long the government will respect this provision given its increasing appetite for citizen surveillance.

Meanwhile, as a counterinsurgency strategy, the Nigerian Army in 2013 shut down GSM services in Adamawa, Borno, and Yobe, the three states that were most affected by Boko Haram terrorism (Jacob and Akpan 2015). This suggests that the government can exploit the state of unrest around the

 DOI: 10.19088/IDS.2021.011

country to implement this kind of shutdown nationwide if it serves its purpose. Also, Nigerians cannot be too sure that the government will not subject social media use in the country to overt surveillance and strict regulation. The position of the country's communications regulatory body is revealing in this regard. The NCC recommends that organisations should install social media monitoring devices or set up a monitoring team to avoid being implicated by the social media activities of their employees (NCC 2019c). This recommendation subtly reveals the stance of the NCC as positively disposed to social media monitoring. It could be argued that at the call of a government with a similar agenda, the NCC would not hesitate to deploy surveillance technology to monitor the public use of social media.

Furthermore, the Nigerian government has taken other decisions that have implications for the digital rights of citizens. One of them is SIM registration. All subscribers were directed to register their SIM card by the 30 June 2013 deadline and new SIM cards only become usable upon registration (NCC 2019b). Also, all old lines that were not registered by the stated date were deactivated. In addition, in 2015, the NCC directed that network service providers should deactivate all pre-registered SIM cards (*ibid.*). The latest directive on SIM card registration in 2020 makes National Identification Numbers (NINs) a mandatory requirement. The directive is likely to restrict access to mobile telephone networks in Nigeria as NIN registration services are not easily accessible (Kolawole 2020).

SIM registration raises data privacy concerns as the NCC is empowered to share subscriber data with security agencies (Olowogboyega 2020). Popular social media sites require mobile numbers for registration and SIM registration makes it all too easy for security agencies to track activists and anyone perceived to be anti-government. The NCC also allows GSM service providers to reissue mobile numbers after a period of inactivity. The practice resulted in Anthony Okolie spending ten weeks in prison for purchasing a SIM card which was previously used by Hanan, President Muhammadu Buhari's daughter (Sahara Reporters 2020). The privacy danger in this practice is high, as buying a reissued SIM card may give the buyer access to the contacts of the previous users who may still call the number, and to banking and other vital information linked to the SIM card.

It was also alleged that in 2017 President Muhammadu Buhari established a troll firm named the Buhari Media Centre (BMC), which later changed its name several times (Adebulu 2020). The trolls at the firm are said to be employed to attack the president's opponents through fake social media accounts. Prior to the 2019 presidential election as well, the Buhari Media Organisation, which is in fact the Buhari Media Centre, accused the PDP presidential candidate Atiku Abubakar of contracting an American lobbyist

 DOI: 10.19088/IDS.2021.011

Brian Ballard for US$90,000 a month to propagate fake news about the APC candidate Muhammadu Buhari (The Cable 2018). Also in 2018, it was revealed that Cambridge Analytica meddled in Nigeria's 2015 presidential election to increase the winning chances of the then incumbent President Goodluck Jonathan (Ekdale and Tully 2020). All these point to the fact that the Nigerian government has been experimenting with technologies that are capable of monitoring the activities of citizens online and accessing their data without consent.

The BMC is also alleged to be behind pro-government hashtags that are trended to counter any hashtag that is critical of the government. An instance was the #ReturnOurGirls hashtag that trended counter to the #BringBackOurGirls hashtag (Aina *et al.* 2019). The goal of the counter-hashtag was to show that the BBOG movement was wrong to demand that the government secure the release of the abducted schoolgirls. Rather, activists were asked to redirect their demand to the terrorists to return the girls they had abducted (*ibid.*). Nevertheless, the greatest threat to Nigerian civic space appears to be from restrictive anti-freedom legislations (Ibezim-Ohaeri 2017). Nigeria has some laws and bills being considered for law which pose a danger to the rights of freedom of speech, expression, and association, both offline and online. Among those legislations are the Terrorism Prevention Amendment Act 2013; the Cybercrime Act 2015; the NGO Regulation Bill 2016, which was revisited in 2019; the Protection from Internet Falsehoods and Manipulations and Other Related Matters Bill 2019; and the Hate Speech Bill 2019.[7] Should all these bills pass into law, they are capable of rolling back all the gains the country has made in terms of the contributions of digital actions to the strengthening of democratic institutions.

7 See Federal Republic of Nigeria National Assembly **Bill Tracker**.

 DOI: 10.19088/IDS.2021.011

# 5. Technology assessment

Since digital rights exist on digital technologies, technology capabilities define the extent to which those rights can be exercised and protected. As noted earlier, digital technologies have facilitated an overlap of spaces with the interests of the state (government), civil society, and individuals intersecting, converging, and diverging at different times. When those interests conflict, each party will be able to protect its interests to the extent that it can manipulate the technologies or defend itself from the manipulation carried out by other parties. The government appears to be at an advantage over others in terms of its enormous power to regulate the activities of individuals and civil society groups. It may be argued that the Nigerian government has a history of abusing its power, and thus individuals and civil society groups have constantly put the government under check.

As a way of checking the excesses of government, Nigerian civil society groups concentrate on efforts to ensure that citizens are empowered to hold government officials accountable. Foremost CSOs in Nigeria that are concerned about digital rights include BudgIT, Paradigm Initiative, Enough is Enough (EiE) Nigeria, and Dubawa. BudgIT has a platform for monitoring: budget implementation (Budget Access[8]); government project implementation (Tracka[9]); utilisation of Covid-19 funds (CovidFund Track[10]); and natural resources extraction (Extractives[11]). EiE Nigeria[12] promotes good governance and citizen engagement in governance and political processes while Paradigm Initiative[13] engages in digital rights advocacy. Dubawa[14] builds the capacity of journalists and other interested individuals to fact-check information online.

These actors appear to have enormous capacities to respond to most of the challenges posed by the contentious nature of Nigerian politics. For example, Dubawa and other digital fact-checking bodies are always quick to verify claims made by government officials and other social actors. BudgIT and EiE Nigeria are always ready to enlighten citizens on why they should demand accountability. BudgIT goes as far as analysing budgets to detect cases of inconsistency and tracking implementation. Besides their websites, all the organisations utilise social media extensively for engagement, especially Twitter and Facebook, and convene occasional offline events. They appear to have a mastery of the technology and have attracted large followings on different platforms. Also, the organisations appear to have standard digital security

8 See **BudgIT**.
9 See **Tracka**.
10 See **Civic Hive**.
11 See **Fix Our Oil**.
12 See **EiE Nigeria**.
13 See **Paradigm Initiative**.
14 See **Dubawa**.

 DOI: 10.19088/IDS.2021.011

measures in place. At no point did any of them report a case of hacking or important data loss. Attempts to undermine their digital security cannot be ruled out as their work is always critical of government at different levels.

CSOs and individual Nigerians utilise a wide range of off-the-shelf applications for gathering data. CSOs at times do develop and customise data-mining software to address their specific needs. Nevertheless, an obvious gap exists in their ability to respond to a case of internet shutdown should it happen in Nigeria. Nigerian digital actors depend mostly on consultation and formal requests, hashtag trending, online protests and petitions, and legal procedures to hold the government accountable. With the Covid-19 lockdown measures fully implemented in Abuja, the country's capital, where the headquarters of government ministries, departments, and agencies are located, traditional access to government information became constrained. Only digital access remained open.

## Table 5.1 Technology assessment

| Existing capacity | Individuals | Civil society | State/corporations |
|---|---|---|---|
| **Bespoke technology used** | None | | AI surveillance (China AI technology) |
| | | | Government disinformation trolls and bots (alleged) |
| **Off-the-shelf tools used** | Tweetdeck | Self-developed software and API-based applications | Tweetdeck |
| | Twitter Analytics | Refined data-mining skillsets | Social media Analytics (likely) |
| | | Data analysis software such as *R* | |
| **Manual methods used** | Manual scrape | | |
| | Qualitative analysis | | |

*Source:* Authors' own.

The information presented in Table 5.1 reveals that there is a general lack of knowledge about the technologies that are being used by the state to abridge digital rights and by non-state actors to protect these rights. It also reveals that the government is far ahead of the country's civil society in the deployment of technologies. As a result, civil society actors most likely lack the technological capacity to put government activities under watch. To measure up, CSOs will need to upgrade their technologies as well. They will be more effective in protecting the digital rights of Nigerians if they have superior technologies that can detect government surveillance and protect themselves and others from it.

 DOI: 10.19088/IDS.2021.011

# 6. The digital rights landscape

The state of digital rights in Nigeria is defined by uncertainty with presidential assent withheld from the Digital Rights and Freedom Bill (2019)[15] already passed by the National Assembly. The current government of President Muhammadu Buhari does not disguise its animosity to digital rights and freedom with its support for legislations that are capable of abridging those rights. The legislations in this category, as presented in Table 3.1, include the Hate Speech Bill (2019) and the Protection from Internet Falsehoods and Manipulations and Other Related Matters Bill (2019). All of these, coupled with the government's use of Chinese AI technology for monitoring activities on digital platforms and devices, and a history of military shutdown of GSM services as counterinsurgency strategy, suggests that there is a lot to worry about with regard to digital rights in Nigeria. Confirming these ominous signals, CIVICUS downgraded the state of Nigeria's civic space from obstructed to repressed (CIVICUS 2019). This means that Nigeria's civic space is just one step from becoming closed, a situation that can only be imagined under a democratic government.

## 6.1 Digital rights in the time of the Covid-19 pandemic

The Covid-19 pandemic has brought a lot of change to personal and public life in Nigeria. The most fundamental was the government lockdown of entire states and a restriction on inter-state movement except for essential services. Despite this emergency situation in which the government made binding pronouncements to abridge citizens' rights, the Nigerian government did not make any attempt to restrict internet use during this period. Government responses to the explosion of fake news and conspiracy theories about Covid-19 were limited to advisories about fact-checking and seeking information only from trustworthy sources.

Nevertheless, the Control of Infectious Diseases Bill 2020 introduced in the Federal House of Representatives contains some injurious provisions. For instance, it empowers the Director General of the National Centre for Diseases Control (NCDC) to forcefully access and seize information based on personal judgement (Onaleye 2020). This provision puts journalists and others in possession of vital information at risk (Chinda 2020). A similar bill titled the National Health Emergency Bill 2020 introduced in the Senate also grants far-reaching powers to government agents at the expense of the citizens (Umoru 2020). The two bills are still before the National Assembly for consideration. Again, all of this suggests that the Nigerian government is ready to take advantage of an emergency situation such as the Covid-19 pandemic to undermine fundamental rights, especially those that thrive on digital technologies.

15 See **Digital Rights and Freedom Bill, 2019**.

 DOI: 10.19088/IDS.2021.011

# 7. Conclusion and recommendations

For many years, the political space in Nigeria has generated conflicts whose ripples polarise the civic space. The government in power has often taken advantage of this polarisation to propose legislations which summarily categorise all views that are critical of it as hate speech punishable by fines, or life or death sentences. These legislations have been a source of fear to users of digital technologies for civic actions. The situation is worse for CSOs, NGOs, FBOs, media organisations, and activists that are critical of the government because the government is far ahead of them in terms of technology capabilities. With the government's AI surveillance technology, it can pry into what those civil actors do on digital platforms and deploy legislations against them. All of this indicates that Nigeria's repressed civic space is not far from outright closing.

Therefore, the future of digital rights in Nigeria hangs mostly on efforts to discourage politicians' penchant for anti-freedom laws. The existing laws in Nigeria are enough to discourage civic actions online while the proposed ones are even more ominous. Should those bills be passed into law, digital rights in Nigeria will be negatively affected. To forestall such development, individuals and groups working on or interested in digital rights need to make the discourse a prominent part of the political process, such that the protection of digital rights becomes prominent on the political agenda.

In addition, civic actors in Nigeria need to develop urgent technology capabilities to withstand the government surveillance of digital platforms. Since Nigeria's Data Protection Regulation (2019)[16] forbids unauthorised access to personal and organisational data, the right of the Nigerian government to deploy AI technology to monitor digital platforms is unknown to law. Nigerian civic actors need urgent knowledge of anti-surveillance technology if digital rights are to continue to thrive in the country. Also, further research into the national security implications of digital technology use in Nigeria is of utmost importance. The findings of such research can uncover positive alternatives to restrictive legislations as measures for ensuring the positive use of digital technologies. They can also inform policies that will preserve digital rights without compromising national security.

16 See Nigeria Data Protection Regulation 2019, National Information Technology Development Agency.

 DOI: 10.19088/IDS.2021.011

# References

Abdulrauf, A.A. (2019) **'Nigeria Bill Aims at Punishing Hate Speech with Death'**, *DW*, 26 November (accessed 20 August 2020)

Adebulu, T. (2020) **'Kperogi: I'm One of the Reasons Thousands of Buhari's Media Trolls Were Employed'**, *The Cable*, 2 January (accessed 20 August 2020)

Aina, T.A.; Atela, M.; Ojebode, A.; Dayil, P. and Aremu, F. (2019) ***Beyond Tweets and Screams: Action for Empowerment and Accountability in Nigeria – The Case of the #BBOG Movement***, IDS Working Paper 529, Brighton: Institute of Development Studies

Akinkuotu, E. (2020) **'Student Arrested for Opening Jonathan Parody Account Denied Access to Lawyers'**, *Punch Newspaper*, 25 July (accessed 20 August 2020)

Bischoff, P. (2020) **'Internet Censorship 2020: A Global Map of Internet Restrictions'**, *Comparitech*, 15 January (accessed 21 August 2020)

Buyse, A. (2018) **'Squeezing Civic Space: Restrictions on Civil Society Organizations and the Linkages with Human Rights'**, *The International Journal of Human Rights* 22.8: 966–88, DOI:10.1080/13642987.2018.1492916 (accessed 26 October 2020)

Carnegie Endowment for International Peace (2020) ***AI Global Surveillance Technology*** (accessed 20 August 2020)

Chinda, K. (2020) **'Nigeria: What Nigerians Should Not Know About the Control of Infectious Diseases Bill, 2020'**, *All Africa*, 11 May (accessed 21 August 2020)

CIVICUS (2019) **'Nigeria Downgraded in New CIVICUS Monitor Report After an Increase in Restrictions on Civic Space'**, *CIVICUS* press release, 4 December, (accessed 21 August 2020)

Ekdale, B. and Tully, M. (2020) **'How the Nigerian and Kenyan Media Handled Cambridge Analytica'**, *The Conversation*, 9 January (accessed 20 August 2020)

Freedom House (2019) ***Freedom in the World*** (accessed 4 December 2020)

GlobalStats (2020) ***Statcounter Social Media Stats Nigeria Aug 2019–Aug 2020*** (accessed 17 September 2020)

Hossain, N. *et al.* (2019) ***Development Needs Society: The Implications of Civic Space for the Sustainable Development Goals***, Geneva: ACT Alliance (accessed 19 October 2020)

Human Rights Council (2016) ***Human Rights Council Thirty-Second Session: The Promotion, Protection and Enjoyment of Human Rights on the Internet***, 27 June (accessed 21 August 2020)

Hutt, R. (2015) **'What Are Your Digital Rights?'**, *World Economic Forum*, 13 November (accessed 21 August 2020)

Ibezim-Ohaeri, V. (2017) **'Confronting Closing Civic Spaces in Nigeria'**, *International Journal on Human Rights* 14.26: 129–40 (accessed 26 October 2020)

Ibrahim, M. (2015) **'Under Fire: Twitter Rages at Adesina Over Controversial Christmas Wish to "Wailing Wailers"'**, *The Cable*, 25 December (accessed 21 August 2020)

Immigration and Refugee Board of Canada (1997) ***Treatment of Political Opponents, Human Rights Activists and Journalists*** (accessed 19 August 2020)

ITU (2020) ***Internet Access Statistics***, International Telecommunication Union (accessed 4 December 2020)

Jacob, J.U. and Akpan, I. (2015) **'Silencing Boko Haram: Mobile Phone Blackout and Counterinsurgency in Nigeria's Northeast Region'**, *Stability: International Journal of Security & Development* 4.1: 1–17 (accessed 19 August 2020)

Kemp, S. (2020) **'Digital 2020: Nigeria'**, *DataReportal*, 18 February (accessed 21 August 2020)

Kolawole, O. (2020) **'Why Nigeria's New Sim Registration Requirements May Be Unrealistic in 2020'**, *Techpoint Africa*, 11 February (accessed 20 August 2020)

Malaea, M. (2019) **'Call for Action in Response to Undercover "Sex for Grades" University Scandal'**, *Newsweek*, 8 October (accessed 20 August 2020)

NCC (2019a) ***Internet Code of Practice*** (accessed 20 August 2020)

NCC (2019b) **'NCC Insists SIM Card Registration is Mandatory: Holds Sensitization Workshop'**, 3 April (accessed 20 August 2020)

NCC (2019c) ***Technical Framework for the Use of Social Media Network in Nigeria***, Abuja: NCC (accessed 20 August 2020)

Ogala, E. (2013) **'Exclusive: Jonathan Awards $40million Contract to Israeli Company to Monitor Computer, Internet Communication by Nigerians'**, *Premium Times*, 25 April (accessed 20 August 2020)

Ojebode, A. (2011) 'Nigerian Former Guerrilla Journalists Ten Years into Democracy: Reformists and Revolutionaries', *Fort Hare Papers* 18: 19–40

Okunoye, B. (2017) **'Digital Rights in Nigeria 2017: The Darkening Clouds'**, *Paradigm Initiative*, 16 November (accessed 17 September 2020)

Oladapo, O.A. and Ojebuyi, B.R. (2017) 'Nature and Outcome of Nigeria's #NoToSocialMediaBill Twitter Protest Against the Frivolous Petitions Bill 2015', in O. Nelson, B.R. Ojebuyi and A. Salawu (eds), *Impacts of the Media on African Socio-Economic Development*, Hershey PA: IGI Global

Olowogboyega, O. (2020) **'Nigeria's SIM Card Registration Laws are "Invasive", New Report Says'**, *Techcabal*, 10 January (accessed 20 August 2020)

Onaleye, T. (2020) **'Controversy Trails Nigeria's Proposed Infectious Diseases Bill, But is it as Bad as People Claim?'** *Technext*, 5 May (accessed 21 August 2020)

Sahara Reporters (2020) **'DSS Detains Man Unlawfully For 10 Weeks After Purchasing MTN SIM Card Previously Used By President Buhari's Daughter'**, 6 January (accessed 20 August 2020)

Statista (2020) ***Number of Social Network Users in Nigeria from 2017 to 2025*** (accessed 17 September 2020)

The Cable (2018) **'Exclusive: PDP Hires Trump's Lobbyist for $90k per month'**, 2 November (accessed 20 August 2020)

Umoru, H. (2020) **'COVID-19: Senate's National Health Emergency Bill 2020 is Anti-People – Senator Melaye'**, *Vanguard Media*, 17 May (accessed 21 August 2020)

Uwalaka, T. and Watkins, J. (2018) **'Social Media as the Fifth Estate in Nigeria: An Analysis of the 2012 Occupy Nigeria Protest'**, *African Journalism Studies* 39.4: 22–41, DOI: 10.1080/23743670.2018.1473274 (accessed 19 October 2020)

# Kenya Digital Rights Landscape Report

Nanjala Nyabola



This report is part of 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries'; the Introduction is also recommended reading.

© 2021 Nanjala Nyabola © Institute of Development Studies. DOI: 10.19088/IDS.2021.012

# 1. Introduction

This report covers political and social developments in Kenya and connects them to the situation in the technological sector, with the aim of identifying opportunities to protect digital and civil rights. Kenya is a notable case of digital uptake in the global South, with a startling increase beginning in 2007, making it one of the most digitally connected countries in Africa. Until discoveries of oil and titanium in the 2000s, the country did not have any notable natural resources and the economy depended on tourism and agriculture. After post-election violence in 2007, Kenya witnessed a dramatic uptake in digital services, including the development of mobile money and other platforms for transport, fintech,[1] tax services and so on, which resulted in an explosion in the digital sector.

Moreover, digital technology has been a major part of politics in Kenya since 2007. The so-called 'Silicon Savannah' is today a frontrunner in many aspects. It is a world leader in mobile money use (*The Economist* 2015) and the second-largest fintech market in Africa; and holding the second digital election in Africa, among others (Ernst & Young 2019). In 2017, Kenya conducted a much celebrated but ultimately disappointing fully digital election. Digital platforms are increasingly a part of public life in Kenya, in part because of deliberate efforts by the government, but also because of organic uptake by citizens, nudged by political and social developments (Nyabola 2018). By 2019, the country had a mobile penetration rate of 88 per cent, with most people connecting through their phones. In 2017, the Kenya National Bureau of Statistics reported that internet subscription rates grew from 29.6 per cent to 41.1 per cent in the same year (Communications Authority 2018).

In fact, the Kenyan government has so far failed to create an adequate policy and legislative framework, particularly around privacy, digital identities and general regulation. Policymaking remains a haphazard affair and the state remains on a constant collision course with activists and citizens' rights groups. Laws passed to regulate online risks are routinely used to silence critics.

In 2018, for example, the Bloggers Association of Kenya (BAKE) successfully sued to suspend 25 provisions of the Computer Misuse and Cybercrimes Act (2018) because it was unconstitutional (CIPESA 2018). The court concurred that the suspended provisions 'contravened constitutional provisions on freedom of opinion, expression, the media, security of the person, the right to

1 Fintech: financial technology.

 DOI: 10.19088/IDS.2021.012

privacy, the right to property and the right to a fair hearing' (*ibid.*). The ruling was subsequently overturned by a superior court, but has been appealed by BAKE and is pending admission by the Supreme Court. Arguably, since the change in government in 2013, the information and communications technology (ICT) policymaking space in Kenya has been characterised by a constant, high stakes push and pull between citizens and the state as the state increasingly seeks to impose itself on the sector without any perceived investment in growing it.

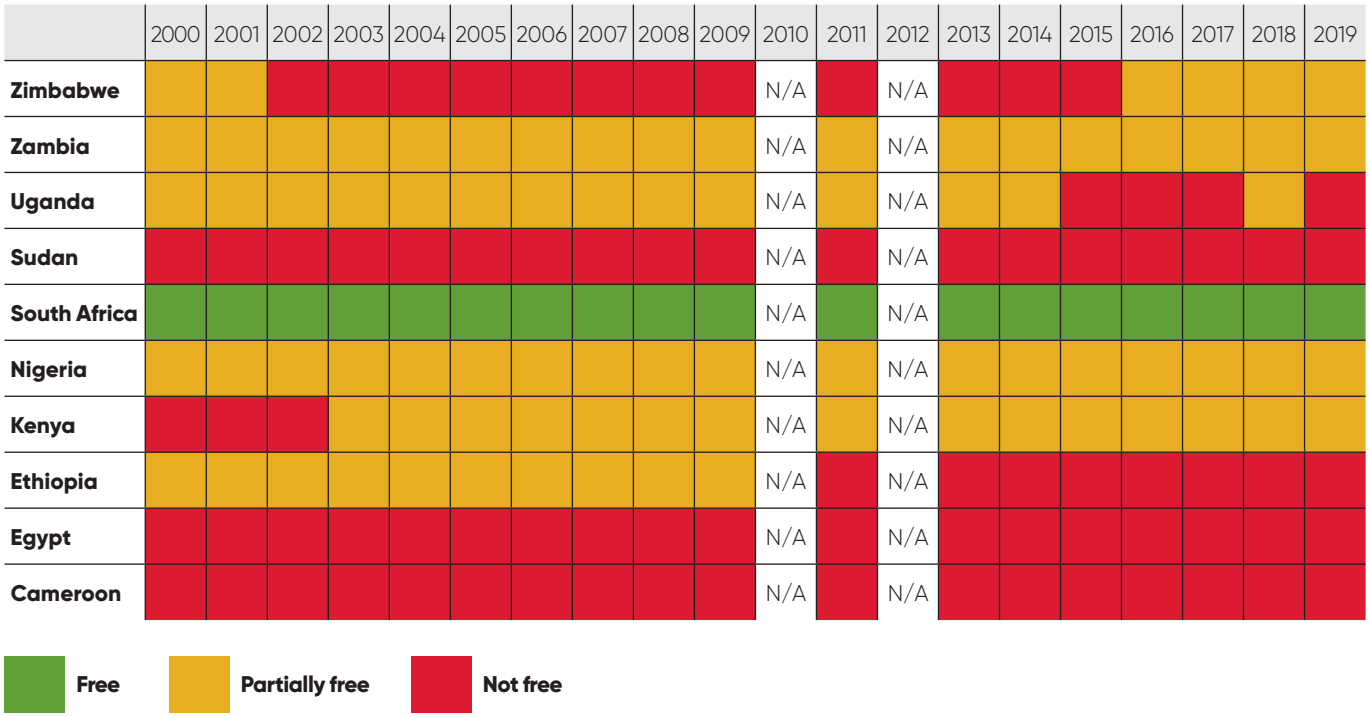
This paper finds that Kenya's fluctuating political climate has both enabled and stifled digital rights, and that there is significant room for action from domestic and international actors to better protect these rights. It also finds that while there is significant capacity in civil society in Kenya, particularly with the advent of specialist digital rights organisations, a lot of this capacity is hampered by the lack of resources to effectively take on both the state and large multinational corporations that dominate the digital space in Africa.

 DOI: 10.19088/IDS.2021.012

# 2. Political landscape

According to human rights watchdog Freedom House, Kenya is a partially free democracy, scoring 48 out of 100 on the group's Freedom in the World rankings, although the state of freedom in the country has fluctuated significantly within the 'partially free' brackets since 2000 (Freedom House 2019; see Figures 2.1 and 2.2). Between independence in 1963 and the end of the one-party state in 1988, Kenya was ruled by two authoritarian leaders who were notorious for cracking down on political dissidents, students and organised political groups. Nor did the advent of multi-party democracy in 1988 automatically lead to democratic gains as the authoritarian regime of Daniel arap Moi, through widespread electoral violence and use of force against members of the opposition, extended its rule by another ten years. Thus, even though the country had multi-party elections in 1992 and 1997, between 2000 and 2002 Freedom House ranked Kenya as 'not free'.

## Figure 2.1 Freedom House ranking for ADRN countries, 2000–19[2]



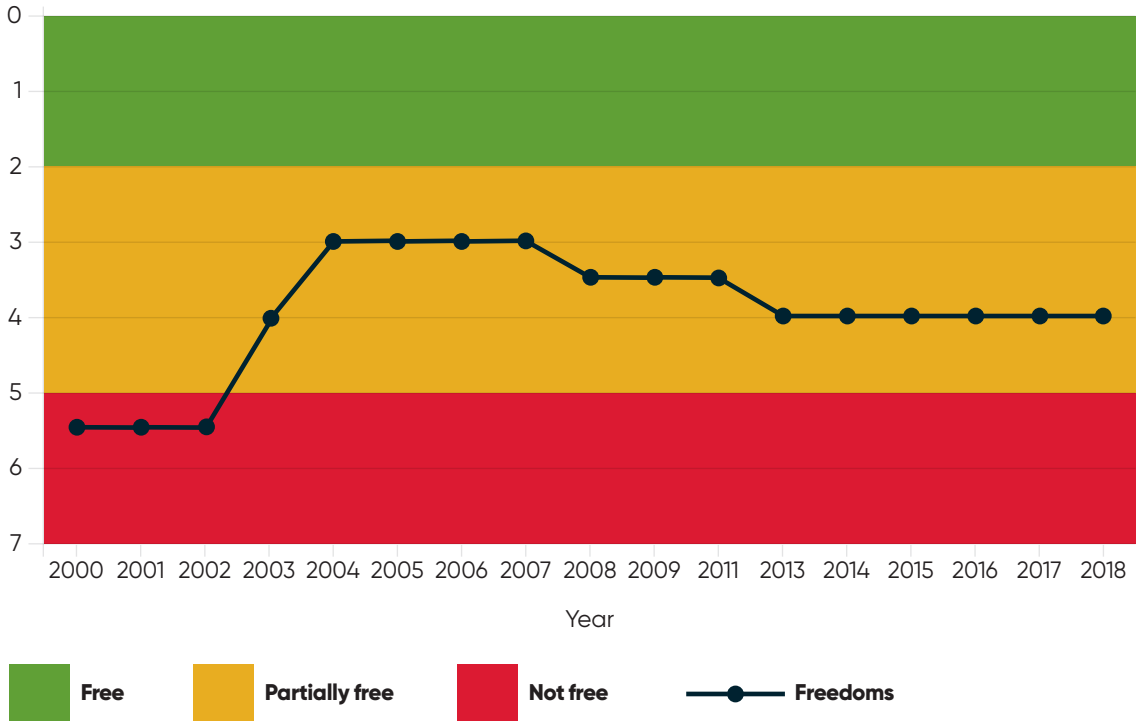

*Note:* ADRN – African Digital Rights Network.

*Source:* Adapted from Freedom House (2019)

2 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.012

## Figure 2.2 Kenya's Freedom Index score, 2000–18[3]




*Source:* Based on data from Freedom House (2020)

This ranking improved dramatically in 2002 after the opposition won the general election, but declined once again after the 2007 election and subsequent votes in 2013 and 2017. The surprisingly peaceful election in 2002 ended the 40-year Kenya African National Union (KANU) regime and ushered in a short-lived period of tremendous growth in political and social freedoms. But this was quickly compromised by the return of past practices to limit press freedom and individual rights. The 2007 election was preceded by notable instances of media intimidation and state-led violence, while the election itself marked the worst of electoral violence, which left at least 1,500 people dead and another 100,000 displaced (Nyabola 2018).

Meanwhile, inequality in the country has increased considerably, as reflected by the annual United Nations Development Programme (UNDP) global Human Development Index and specifically the Gini coefficient. In 2005, for example, the country had a Gini coefficient of 46.5, but ten years later, the figure was 40.8 (UNDP 2019). According to international non-governmental organisation Oxfam, less than 0.1 per cent of the country's population owns more assets than the remaining 99.9 per cent, and the numbers of the super-rich in the country are growing at one of the fastest rates in the world

3 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.012

(Oxfam 2020). Organisations such as Oxfam argue that this significant inequality drives Kenya's high rates of crime and institutional violence. Given all this, the state in Kenya remains highly fragile, particularly in election years. Civil liberties also deteriorate considerably in the build-up to and aftermath of elections, while corruption in the country remains high.

The ushering in of a new constitution in 2010 fundamentally reorganised government, creating hundreds of new elected positions – and thereby increasing public spending – as well as new constitutional rights and freedoms. Public awareness of these new rights and freedoms generally remains low, but particularly with regards to digital rights. The government has been slow to implement the new dispensation. For example, Article 35 of the Constitution provides in part that the state shall publish any important information affecting the nation (Republic of Kenya 2010) and this creates a constitutional obligation for public participation. Regulations based on these laws have interpreted this to mean, among other things, that the public shall be invited to participate in the processes of lawmaking through public forums, media outreach and other efforts. Yet proposed laws are rarely subjected to public scrutiny and where comments are provided, they are rarely reflected in the final draft of the law.

In 2017, four days after a peaceful August vote, the Independent Election and Boundaries Commission (IEBC) announced that the incumbent, Uhuru Kenyatta, had won the presidential election with approximately 56 per cent of the national vote (enough to avoid a run-off) (Kimutai and Okumu 2019). His main challenger, Raila Odinga, quickly filed a petition against the result and was granted a hearing before the Supreme Court (Al Jazeera 2017). On 1 September, the Supreme Court held that the presidential election had not been conducted to a constitutional standard and ordered a fresh election to be conducted within 90 days (de Freytas-Tamura 2017).

In the interim period, the IEBC struggled to demonstrate that it had addressed many of the shortcomings that had led to the dismissal of the first round of voting. The remaining uncertainty around the electoral register fuels many of the concerns in Kenya around digital privacy and data protection in elections. Elections are one of the largest data collection exercises in the country, and anxieties over how the electoral roll was built and administered underpin much of the ambivalence towards digital government.

 DOI: 10.19088/IDS.2021.012

The experience of the election affirmed that many of the anxieties were well founded. For example, concerns around OT-Morpho Safran (now known as IDEMIA), the French company that built the software that administered the election, drew parliamentary attention to data expropriation and triggered new impetus to pass a data protection law. Moreover, details of Kenya's electoral register are in the semi-public domain (i.e. they can be purchased from the IEBC for a specified fee). Any company or individual is able to purchase all or portions of the register under the current regulatory framework.

Taken together, this political context means that Kenya's digital development is constantly under threat of reprisal from an insecure administration with authoritarian tendencies, on the one hand, and a systemic lack of investment and institutional apathy triggered by corruption on the other.

 DOI: 10.19088/IDS.2021.012

# 3. Civic space landscape

Civic space in Kenya has also fluctuated widely between 2000 and 2020. Regionally, Kenya has had a reputation for a historically strong civil society despite authoritarian regimes, shaped by notable mobilisations and mass protests such as the Saba Saba (7 July 1997) , and the continued action of civil society leaders despite significant reprisals (*The Economist* 1997). Mobilisation for the end of one-party rule subsumed all other forms of organisation; and so, for example, women's rights organising has been less visible, also in part because of the co-opting of formal women's rights institutions such as Maendeleo ya Wanawake (Progress for Women). Although there had always been multiple print media outlets, after the end of the one-party state there was also a proliferation of television and radio stations, which increased and diversified access to information. Protest actions in universities and civil society were the main way through which civic space was opened up, culminating in the end of KANU rule in 2002.

Between 2002 and 2007, the situation in Kenya oscillated between extreme opening up of civic space and rapid contraction. The first three years of the Mwai Kibaki administration saw significant gains in law, truth and reconciliation, civil society and other sectors. There was also massive expansion in media and internet communications. However, as criticism shifted towards the administration, many authoritarian practices resurfaced. For example, both the first lady and the cabinet secretary for the interior were involved in two separate and highly visible instances of press intimidation captured on camera and broadcast live (Nyabola 2018). By the 2007 election, there were significant indications that all was not well in Kenyan politics.

Between 2007 and 2013, Kenya remained in political limbo due to reconciliation efforts between the two principals who fought after the 2007 election, and the growing pressure to change the Constitution. The passing of the new Constitution inspired a new wave of activism and organising, but this was quickly curbed as anti-International Criminal Court and anti-accountability rhetoric surged (Nyabola 2018).

After the 2013 election, civic space in Kenya declined considerably. A 2014 report from the Poverty Eradication Network (PEN), a coalition of civil society actors in the country, noted:

> Kenyan civil society has been billed as one of the most vibrant in the region... operating in more than 26 sectors... [but is] currently facing their biggest challenge with the state trying to manipulate the regulatory laws with the purpose of controlling it.
>
> (Keter 2014)

 DOI: 10.19088/IDS.2021.012

A 2016 Kenya Human Rights Commission report noted 'actors in the civic sector in Kenya, from donors to grassroots networks, media to workers unions all experience... attack and threats to their existence and effectiveness' (KHRC 2016). In 2018, anti-corruption watchdog Transparency International found that 368 journalists were murdered between 2012 and 2017, and out of these 70 were murdered while covering corruption stories (Nyakio 2018).

Elections are a foundational part of Kenya's civic space, as most political action even between election years is geared towards winning the subsequent vote. Since 2007, there has been a dramatic contraction in civic space due to reduced freedoms of expression, assembly, protest and other key pillars of democratic participation designed to influence electoral participation, although there have been some victories, particularly those gained through the courts. Many unconstitutional threats are usually advanced and consolidated in the interests of preserving electoral advantage. With regards to digital rights, for example, the impetus for designing governance architecture on data protection stems in part from the history of misuse of the electoral register.

On 19 December 2014, President Uhuru Kenyatta signed into law the controversial Security Laws (Amendment) Bill 2014, a day after Parliament approved the law amid nationally televised chaos involving heckling and fistfights, as some members sought to air their strong opposition to the proposal (KTN News 2014). It amended 21 laws, including the Penal Code, Criminal Procedure Code, Evidence Act, Prevention of Terrorism Act and the National Police Service Act. Critics argued that this law was a major setback for civic space in Kenya as it gave the government unprecedented powers of surveillance, arrest and detention, and to silence dissenters and critics (KHRC 2014).

In all of this, the judiciary has emerged as an inconsistent last resort for the protection of civic space. Legal challenges to legislative action have had mixed results, particularly as they pertain to digital rights. For example, in April 2019 the High Court found that the state could not make registration for the Huduma Number (Namba) digital ID system that in 2019 was abruptly announced to be mandatory as this was unconstitutional, but allowed the programme to continue pending legal determination of its constitutionality (Kakah 2019). The court also struck down 26 provisions of the Computer Misuse and Cybercrimes Bill, and while a superior court reversed this decision, an appeal was filed in the Supreme Court (Lolyne 2020).

 DOI: 10.19088/IDS.2021.012

# Table 3.1 Civic space timeline

| Year | Shift | Implication |
|---|---|---|
| **2002** | Multi-party election. First election in which the opposition defeats the incumbent. | Opens civic space to engage millions in political discourse and democratic participation. |
| **2005** | Constitutional Referendum November–December: voters reject a proposed new constitution in what is seen as a protest against President Kibaki. | Increases momentum for the opposition in the lead-up to the election; more radical constitutional proposals are protected. |
| **2007** | Contentious election leading to post-election violence. | Pushes increased uptake in mobile money and use of blogging and online platforms as the media retreat. |
| **2010** | August: new constitution designed to limit the powers of the president and devolve power to the regions approved in referendum. | Expansive Bill of Rights and explicitly states new rights that will affect the digital landscape including the right to privacy in Article 31. |
| **2012** | National Intelligence Service Act (2012). | Gives security agencies powers to monitor communications but does not set out what kind of communications might be monitored or what kind of interception is permitted. |
| **2013** | Access to Information Bill (never passed). | Law designed to encourage proactive disclosures by the state and its agencies, as well as creating a framework in which citizens can demand information from the government, as set out in Article 35 of the Constitution. |
| | PBO Act (2013) passed but not implemented. | The law would provide more support for civil society organisations. |
| | Media Law (2013). | Media owners criticise the law for expanding the executive's role in media. |
| | Kenya Information and Communications (Amendment) Act (2013). | Critics argue that it expands the executive's oversight role over the CA. The law also creates criminal penalties for what should ordinarily be civil or professional standards violations. |
| **2014** | Security Laws. | Gives the country's national security organs broad, unchecked surveillance powers. |
| **2019** | Kenya Information and Communication (Amendment) Bill. | Attempts to curb criticism in online spaces; introduces heavy fines for hacking and other cybercrimes. |
| | Data Protection Act. | Creates regulatory framework for data privacy and protection. |

*Source:* Author's own.

# 4. Technology landscape

Kenya's technology landscape is characterised both by rapid advances and by a growing gap between those who have the most access to and capacity for technology, and those who have the least. Because of its reputation as the Silicon Savannah, many of the technology advances developed elsewhere for use in the developing world are tested in Kenya; for example, Google's 'internet balloons' (BBC News 2020). After several years of dramatic developments, with only marginal regulatory changes, since 2013 the government has attempted to pass a rash of measures designed to constrain behaviour on the internet, which critics argue is an indirect effort to curb freedom of expression in the country.

First, the government has frequently used legislation to try to curb online civic space, and notably avoids meaningful public participation on contentious legislation. As such, legislation in the digital space is frequently subject to litigation by interested parties, owing to the government's failure to consult the public and to respond adequately to social challenges. The case of the Huduma Namba digital identity initiative points out the significant ways in which the government is failing to adhere to constitutional standards and creating a climate where trust in digital technology becomes increasingly elusive. The cabinet secretary for the interior abruptly announced in February 2019 that everyone over the age of six who was resident in Kenya had 30 days to register for the new digital ID system, but there was no effective public participation in the design or implementation plan for the initiative. As such, civil society leaders sued the government over the implementation of the programme, culminating in a stop order against the ministry (Privacy International 2020).

On 11 August 2017, Kenya held the first of two rounds of what would be one of the most contested elections in the country. Prior to the vote, there were queries about the methods by which French company OT-Morpho Safran had been contracted to build the electoral database – queries that were not addressed before election day (Nyamori 2019). This was also nominally the country's first fully digital election and the second digital election in Africa. The digital process involved the deployment of electronic voter identification, biometric voter registration, electronic results transmission, and other computerised standards. However, instead of a fully digital process, two weeks before the vote the IEBC declared that voting in at least one-third of polling stations would be analogue (Menya 2017).

Surveillance and lack of privacy remain key threats to civil rights in Kenya, with international governments such as the US and China providing funding and hardware for an elaborate surveillance network in the country (Kapiyo

 DOI: 10.19088/IDS.2021.012

and Gathaiga 2014). Given Kenya's experience of terrorism, there has been and will likely continue to be resistance to creating a legal framework that obscures the state's ability to intercept, collect and process citizens' data. Much of the justification for the elaborate surveillance regime is that it helps the country address terrorism, but human rights defenders have raised the alarm that Kenya's surveillance architecture is part of a broader threat to freedom of association and to critics of the state (PBI 2012).

In fact, state-led efforts at data collection have only grown more intense, including the Huduma Namba initiative to create a centralised database of citizen information and supplant the national ID cards envisioned in the Registration of Persons (Amendment) Act (2009) (Government of Kenya 2019). Abruptly announced in February 2019, the Huduma Namba initiative was the culmination of a multi-year initiative to reform and then digitise identity systems in the country. The government estimated that the project would cost between $5m and $6m and promised it would streamline service provision (Nyawira 2019). Critics of this initiative pointed out that without a data protection law, the Huduma Namba project posed major human rights challenges, including hardening identity discrimination against minority groups and allowing for the unchecked collection, processing and commercialisation of citizen data (Yousuf 2019).

Evidently, corporations are part of the tension around data privacy and protection in Kenya. Safaricom, the largest telecommunications company in the country and a provider of multiple data-rich services, has been implicated in numerous violations of rights to privacy and protections from surveillance in Kenya (Privacy International 2017). Given its size and domination of the communications landscape, coupled with the government's 35 per cent shareholding in the corporation, legal policy in communications is often built around protecting Safaricom; for example, the state regulator of corporations refused to declare the corporation dominant and therefore subject to a separate regulatory regime from other mobile companies (Mwita 2019). But foreign companies are also part of the mix; OT-Morpho Safran has received two high-profile, irregularly allocated tenders to build technology for a digital ID system and for the 2017 election, while Chinese hardware giant Huawei, has built the country's surveillance architecture.

 DOI: 10.19088/IDS.2021.012

# Table 4.1 Technology timeline

| Year | Shift | Implication |
|---|---|---|
| **1993** | Internet access first available in Kenya. | |
| | Launch of the national fibre-optic backbone. | Dramatic increase in connectivity. |
| **1999** | Break-up of Kenya Posts and Telecommunications. Telkom Kenya maintains control over communications hardware and infrastructure. Safaricom takes charge of the mobile phone network. The Communications Commission of Kenya oversees regulation and licensing. Posta Kenya overseas postal services. | Privatisation of the communications sector, shifting to a profit-based model, dramatically increases connectivity in the country. |
| **2007–08** | December 2007–April 2008, post-election violence. First week of January 2008, Nairobi lockdown. | Mobile money launched earlier in the year. Uptick in mobile money use, launch of Ushahidi crowdmapping to monitor election violence. |
| **2009** | SEACOM, Kenya's first subsea cable system. The East Africa Marine System (TEAMS) fibre-optic cable is launched in July, connecting Kenya to the Middle East. | Significant boost in internet speeds in the country, which stimulates more digital connectivity. |
| **2013** | Launch of the Integrated Financial Management Information System (IFMIS). | Designed to stimulate open governance/digital governance systems. |
| | General election in Kenya; Cambridge Analytica contracted by the Jubilee Alliance. | |
| **2016** | First IFMIS scandal revealed, involving the National Youth Service, in which just under $8m was misappropriated from the Ministry of Devolution. | |
| **2017** | Controversial fully digital election. | |

*Source:* Author's own.

 DOI: 10.19088/IDS.2021.012

# 5. Digital rights landscape

There is more capacity to respond to digital rights threats in Kenya than in many similarly situated countries around the world, but there is still a significant gap between where the country is and where it should be. Similarly, there are a growing number of specialist organisations responding to digital rights, but for the most part, the work of defending digital rights has fallen to non-specialist human rights organisations with limited internal capacity to respond to rapidly emerging threats.

Key civil society actors working explicitly on digital rights include the Bloggers Association of Kenya (BAKE), which has been the national leader in civil and constitutional litigation on digital rights in the country. The Lawyers Hub, a private corporation focusing on the legal aspects of the digital landscape has also developed a robust advocacy arm and is looking to expand into research and activism. The Centre for Intellectual Property and Information Technology Law (CIPIT) at Strathmore University also provides significant academic capacity for digital rights activism through research and publications.

Other less specialist organisations moving into digital rights advocacy include the Katiba Institute, which specialises in constitutional litigation and led the case on the Huduma Namba initiative alongside the Nubian Rights Forum. Amnesty International Kenya has also developed a digital rights advocacy strategy, as has Mzalendo, a civil society organisation that focuses on legislative monitoring and tracking of parliament. Regionally, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) also has a researcher based in Nairobi and regularly contributes to conversations on digital rights in the country. International actors such as Privacy International and Article 19 are also active in the digital rights space in Kenya.

Key state actors in the digital rights space include the Ministry of Information and Communications Technology, currently led by Cabinet Secretary Joe Mucheru. The ministry develops government policy and government-sponsored litigation, as well as representing Kenya in international negotiations with ICT companies. The Communications Authority (CA) is also a key actor in the space. It primarily provides licensing and regulation, but through laws pertaining to the governance of broadcast signals also has the capacity to switch media on and off as directed by the government. The CA also oversees the licensing and regulation of telecommunications company and manages Kenya's fibre-optic network. Finally, the Office of the Attorney General oversees litigation on behalf of the government.

 DOI: 10.19088/IDS.2021.012

Major private sector actors touching on digital rights in Kenya include a network of hubs inspired by the iHub, a space for technology enthusiasts and makers founded on the success of Ushahidi. Similar hubs such as Nairobi Garage, Metta and Lawyers Hub have become meeting points for those thinking about and working on digital issues in the country. Funders also play a pivotal role in the landscape through their convening power, including Luminate, Open Society Initiative for East Africa (OSIEA), the Open Society Foundation's Justice Initiative and the Ford Foundation. Other related players include independent digital media (The Elephant, Africa Uncensored) and data visualisation firm Odipo Dev.

Still, a great deal of organising around digital rights in Kenya occurs around hashtags and spontaneous citizen mobilisations on WhatsApp and other platforms. Similarly, because most of the space for pushback against state overreach exists purely online and in the courts, much of the organisation and mobilisation happens in courts and around legal and technical action.

 DOI: 10.19088/IDS.2021.012

# 6. Conclusion and recommendations

Developments in Kenya's digital space have greatly outpaced developments in digital rights advocacy and protection. There must be a concerted effort to support organisations active in this space, and those active in human rights in general, to develop a digital rights consciousness and encourage activism. These recommendations are premised on strengthening the capacity of local organisations to respond to ongoing changes at a reasonable pace, and empower communities to advocate for these rights themselves.

- For civil society: increase South–South partnerships in digital rights advocacy given that many of the initiatives rolled out in Kenya are first piloted in other countries of the global South such as India and Brazil.
- Encourage demands for transparency and accountability from technology companies working in the region to allow for public scrutiny of their contracts and agreements with the government.
- For universities and knowledge sectors: push for investment in research and research partnerships between academic institutions in Kenya and those in other parts of Africa and the world to deepen knowledge on digital rights in the region.
    - Deepen technical knowledge on collecting and analysing information on automated political campaigning and the influence economy.
    - Develop permanent research chairs and positions on digital rights and the digital economy.
- For government: invest in local language initiatives to translate digital rights language into locally useful terms.

 DOI: 10.19088/IDS.2021.012

# References

Al Jazeera (2017) **'Kenya Opposition Files Challenge Over Election Results'**, 19 August (accessed 2 August 2020)

BBC News (2020) **'4G Internet Balloons Take Off Over Kenya'**, 7 July (accessed 28 September 2020)

CIPESA (2018) **'Sections of Kenya's Computer Misuse and Cybercrimes Act, 2018 Temporarily Suspended'**, Collaboration on International ICT Policy in East and Southern Africa, 30 May (accessed 21 May 2020)

Communications Authority (2018) *Fourth Quarter Sector Statistics Report for the Financial Year 2017/2018 (APRIL–JUNE 2018)*

De Freytas-Tamura, K. (2017) **'Kenya Supreme Court Nullifies Election'**, *The New York Times*, 1 September (accessed 2 August 2020)

Ernst & Young (2019) *Fintechs in Sub-Saharan Africa: An Overview of Market Developments and Investment Opportunities*, London: Ernst & Young

FIDH (2014) **'Kenya: The Security Laws (Amendment) Act Must be Repealed'**, International Federation for Human Rights (FIDH), 19 December (accessed 28 October 2020)

Freedom House (2020) ***Freedom on the Net*** (accessed 4 December 2020)

Freedom House (2019) **'Kenya'**, *Freedom in the World 2020* (accessed 26 August 2020)

Government of Kenya (2019) ***Huduma Namba*** (accessed 15 October 2020)

Kakah, M. (2019) **'High Court Allows Huduma Namba Listing But With Conditions'**, *Daily Nation*, 2 April (accessed 2 August 2020)

Kapiyo, V. and Gathaiga, G. (2014) ***Global Information Watch 2014: Communications Surveillance in the Digital Age***, Global Information Society Watch (accessed 26 August 2020)

Keter, S. (2014) *State of Civil Society in Kenya: Challenges and Opportunities. Report of CSO Dialogues in Kenya*, CSO Dialogue Report, Nairobi: Poverty Eradication Network

KHRC (2016) ***Towards a Protected and Expanded Civic Space in Kenya and Beyond: A Status Report and Strategy Paper Developed for the Civil Society Sector in Kenya***, Nairobi: Kenya Human Rights Commission (accessed 26 August 2020)

Kimutai, C. and Okumu, P. (2019) **'Uhuru Kenyatta got 8.2 Million votes against Raila Odinga's 6.7 Million'**, *The Standard*, 12 August (accessed 2 August 2020)

KTN News (2014) '**Chaos and Drama Follow up after the Controversial Security Laws Amendment Bill 2014 Passed**', 18 December (accessed 29 October 2020)

Lolyne (2020) ***Update of our Computer Misuse and Cybercrimes Case***, Bloggers Association of Kenya (BAKE) blog, 29 August (accessed 31 August 2020)

Menya, W. (2017) **'Chebukati and Chiloba Blamed over Poll Failures'**, *Daily Nation*, 21 September (accessed 2 August 2020)

Mwita, M. (2019) **'Safaricom is Big on Investment, Not Dominant – Michael Joseph'**, *The Star*, 26 October (accessed 28 October 2020)

Nyabola, N. (2018) *Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya*, London: Zed Books

Nyakio, S. (2018) ***Stop Attacks on Journalists***, International Commission of Jurists – Kenya Section (accessed 28 October 2020)

Nyamori, M. (2019) **'Legislators Vow to Ban OT Morpho Safran from Sh3 Billion Deal'**, *The Standard*, 12 February (accessed 2 August 2020)

Nyawira, L. (2019) **'All You Need to Know about the Huduma Namba'**, *The Star*, 2 April (accessed 26 August 2020)

 DOI: 10.19088/IDS.2021.012

Opala, K. (2019) **'Kenya: IEBC Dilemma After Ban of Controversial KIEMS French Firm'**, *The Nation*, 28 April (accessed 28 September 2020)

Oxfam (2020) ***Kenya: Extreme Inequality in Numbers*** (accessed 26 August 2020)

PBI (2012) ***An Assessment of the Feasibility and Effectiveness of Protective Accompaniment in Kenya***, London: Peace Brigades International (accessed 13 February 2021)

Privacy International (2020) **'Kenya Court Ruling on Huduma Number Identity System: The Good, the Bad, the Ugly'**, 24 February (accessed 28 September 2020)

Privacy International (2017) **'In Kenya, Surveillance Communications is a Matter of Life or Death'**, 15 March (accessed 2 August 2020)

Republic of Kenya (2010) *The Constitution of Kenya*, Nairobi: National Council for Law Reporting, Government of Kenya

*The Economist* (2015) **'Why Does Kenya Lead the World in Mobile Money?'**, 2 March (accessed 22 May 2020)

*The Economist* (1997) **'Brutal Seventh'**, 17 July (accessed 28 September 2020)

UNDP (2019) ***Human Development Report 2019***, New York NY: United Nations Development Programme (accessed 13 February 2021)

Yousuf, M.M. (2019) **'Why Huduma Namba Bill Raises Tough Questions'**, *The Business Daily*, 29 July (accessed 2 August 2020)

# Ethiopia Digital Rights Landscape Report

Iginio Gagliardone and Atnafu Brhane



This report is part of 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries'; the Introduction is also recommended reading.

© 2021 Iginio Gagliardone & Atnafu Brhane © Institute of Development Studies. DOI: 10.19088/IDS.2021.013

# 1. Introduction

Ethiopia is a country of many paradoxes. It has some of the lowest levels of internet penetration in the world, yet applies some of the severest measures for surveilling and censoring online communication (HRW 2014). It has charted new avenues of collaboration with emerging donors, especially China, but also continues to be Africa's largest recipient of development aid from traditional Western donors (Fourie 2015; Gagliardone 2019). Ethiopia has championed uses of information and communication technologies (ICTs) that have later been adopted elsewhere in Africa, from videoconferencing for government communication to commodities exchanges, and yet it is considered backward when it comes to digital innovation (Rashid 2015).

The Ethiopian government, led since 1991 by the Ethiopian People's Revolutionary Democratic Front (EPRDF) coalition, has developed a distinctive approach towards digital media in Africa. Defending its monopoly of telecommunications, while almost all other countries on the continent liberalised their markets, the government sought to balance developmental opportunities offered by ICTs with their destabilising potential – with mixed results. On the one hand, through support from the Export-Import Bank of China (Exim Bank) and telecom giants ZTE and Huawei, it managed to expand access without competition. Its tight control of digital space enabled the government to enforce drastic measures to curb dissent, including pervasive censorship and surveillance, and internet shutdowns in moments of crisis (Dahir 2016; Marchant and Stremlau 2020).

And yet, Ethiopian citizens displayed significant abilities in making use of digital media to mobilise and challenge the government: first in 2005, in the aftermath of the only contested elections in the country; and later in the sustained waves of protests that emerged first in the Oromia region, then spread to other corners of the country, ultimately leading to a significant change in the balance of power, with the appointment of the first prime minister of Oromo descent, Abiy Ahmed.

The new prime minister initiated a significant process of reform, freeing imprisoned journalists and activists, and allowing greater freedoms to opposition parties and media outlets. Ongoing transformations, however, have created new tensions, leading to another wave of protests in 2020

 DOI: 10.19088/IDS.2021.013

and to the resurgence of older forms of repression, including internet shutdowns and imprisonments. These left Ethiopia at a crossroads between normalising of the relationship between the government and oppositional forces, or continuing the authoritarian rule that had characterised the country for more than two decades. The civil war that erupted in November 2020, between the central government in Addis Ababa, and the Tigrayan People's Liberation Front (TPLF), once the dominant force within the EPRDF coalition, represents a tragic turn in the process of transformation initiated by Abiy Ahmed, and has had significant repercussions on online debates among Ethiopians in Ethiopia and in the diaspora, leading to a polarisation among opposing factions (Wilmot 2020).

 DOI: 10.19088/IDS.2021.013

# 2. Political landscape

The Ethiopian government's approach to digital media has to be located in the longer history of the relationship with opposition politics and traditional media, and what can be considered the 'original sin' in the contemporary history of communication in Ethiopia: the fact that when the new leaders came to power, after two decades of civil war, they opened the space for debate but refused to engage with the very debates they had allowed to bloom (Gagliardone 2014b).

In the early 1990s, the EPRDF had to show it was different from its oppressive predecessors. In the ostensibly unipolar world that emerged after the fall of the Soviet Union, the pressure to respect certain rights and freedoms was significant and freer media represented an opportunity to boost the new government's international legitimacy (Stremlau 2011). At the domestic level, liberalisation of the press also helped signal to a population traumatised by decades of war that a new breed of rulers was now in power.

The Transitional Government of Ethiopia, which was established to write a new constitution and build the foundations for a new Ethiopian state, soon created the conditions for the first private newspapers to start publishing and later spelled out their rights in the relatively progressive press law passed in 1992. However, these measures were to be undermined by the EPRDF's lack of commitment to the freedoms it had allowed, and its failure to understand what it really meant to allow a plurality of voices to compete in a post-war scenario.

The criticism in the private press took on an increasingly adversarial tone, but the EPRDF leadership stuck to its policy, ignoring dissenting voices and labelling them as 'anti-peace' and 'anti-constitution'. This stemmed from a belief that those writing for the private press were not part of the EPRDF's constituency in any case, so there was little need to expend political capital either repressing or engaging them (*ibid.*). Over time, however, the trading of accusations and the inability of opposing factions to command each other's attention progressively poisoned the debate in ways that would have repercussions beyond the press.

When the internet started to be employed as a space to discuss Ethiopian politics, debates were rapidly captured by the polarised tones that had characterised the press. Platforms such as Ethiopian Review, Nazret and Ethiomedia, all launched by Ethiopians in the diaspora, hosted articles that equally could have appeared in the newspapers printed in Addis Ababa. Indeed, from the very beginning it became common to find references and connections between online and printed articles.

 DOI: 10.19088/IDS.2021.013

The new media, rather than being seized by a new generation of leaders and advocates as an opportunity to test innovative ideas, were largely captured by 'old politics'. Instead of debating new issues, as occurred in nearby Kenya, authors returned to old grievances that had their roots in the 1960s and 1970s when the movements challenging Emperor Haile Selassie, and later the Derg military dictatorship, started to appear. While some middle ground did emerge, both online and offline, the discussions the more moderate outlets promoted tended to remain in the background and were unable to galvanise or mobilise passions and political energy in the same way as more extreme pieces that polarised debate.

The early 2000s represented a moment of transition, when the EPRDF, still allowing oppositional forces to voice their criticism, sought ways to develop a more aggressive strategy to seize the opportunities offered by digital media. In 2001, the prime minister, Meles Zenawi, emerged from the split within the EPRDF that followed the two-year war with Eritrea with his leadership called into question. He responded by launching an ambitious project to reinforce the state. The institutional connections between the centre and the peripheries were strengthened and the state was reformed to function as a more active player in social and economic renewal. Digital media came to play a central role in this strategy of transformation and capacity building.

This time, rather than hastily adopting a policy it could not master, or refusing to adopt a technology for fear of its destabilising potential, the government closely connected its strategy in the ICT sector to the principles on which its larger political project was based; in particular, the ideas of revolutionary democracy, ethnic federalism and the developmental state (Bach 2011; Abbink 2011b).

The concepts of revolutionary democracy and ethnic federalism emerged during the guerrilla war waged against the Derg, which was initially fought in the name of the right to self-determination for the people of Tigray, but later expanded in scope to include the goal of national liberation. Once the guerrilla fighters came to power, the ideology of ethnic federalism was used to reframe Ethiopia, no longer as a unitary nation but as a federation of ethnicities, which at least on paper were all entitled to the same right to self-determination. By connecting the Tigrayan minority to other oppressed groups and offering them, at least in principle, the opportunity to participate in the re-founding of the nation, the EPRDF presented its *de facto* capture of the state as a victory for all marginalised groups.

Ethnicity emerged as both a means and an end. It served as an operational principle for the redistribution of resources to those recognised as separate ethnic groups, but the provision of material benefits along ethnic lines was also aimed at convincing people on the ground that it was in their interests

 DOI: 10.19088/IDS.2021.013

to be recognised as ethnically diverse. By building the state and creating new institutions and new rules for citizens to relate to central and local authority and claim their rights, the EPRDF aimed to be building the nation, offering new categories and ideational referents for Ethiopians to think of themselves as citizens (Aalen 2006; Pausewang, Tronvoll and Aalen 2002).

The concept of revolutionary democracy also emerged during the struggle in the bush, but its definition continued to evolve after the EPRDF came to power. Revolutionary democracy rejects the focus on the individual that characterises liberal democracy, preferring to stress group rights and consensus. It favours a populist discourse, claiming a direct connection between the leadership and the masses, bypassing the need to negotiate with other elites that advance competing ideas of the nation state and the role different groups have within it (Bach 2011; Hagmann and Abbink 2011). Through the contribution of Meles Zenawi himself, new concepts were progressively added to the core tenets of ethnic federalism and revolutionary democracy, borrowed largely, but selectively, from the models of the developmental state; and stressing in particular the importance of state stability and the role of a determined developmental elite in supporting economic performance and avoiding rent-seeking (Fisher and Anderson 2015).

At the turn of the millennium, various large-scale projects sought to implement these principles on the ground, becoming their technological embodiments. Woredanet and Schoolnet – an e-government and e-learning project, respectively – used digital media to sustain a complex process of state and nation building. Woredanet, which stands for 'network of district [*woreda*] administrations' employs the same protocol that the internet is based upon. But rather than allowing individuals to independently seek information and express their opinions, it enabled ministers and cadres in Addis Ababa to videoconference with regional and *woreda* offices, and instruct them on what they should be doing and how. Schoolnet uses a similar architecture to stream pre-recorded classes for a variety of subjects, from mathematics to civics, to all secondary schools in the country, while also offering political education to schoolteachers and other government officials.[1]

The faith in this complex process of state and nation building, the roll-out of large-scale projects, and their combined ability to create a stronger connection between the political vanguard and Ethiopian citizens, were among the reasons that convinced the Ethiopian government to allow the first contested elections to take place in 2005. Prior to this, elections in Ethiopia had mostly been held for the EPRDF to reaffirm its control over the country and for external consumption, rather than to provide a real opportunity for political competition (Abbink 2011a).

1 For more information on these systems, see Gagliardone (2014a, 2016).

 DOI: 10.19088/IDS.2021.013

The results of this political gamble, however, were unexpected. After election day, when the EPRDF realised it had suffered greater losses than it was ready to accept and people started protesting over the delay in issuing the results (Carter Center 2005), government repression led to the imprisonment of most political leaders, and the censoring of some of the communication channels that had been used to support mass mobilisation (see section 4). As the EPRDF closed avenues for popular protest and forcefully consolidated power, it also began an ambitious project to legitimise these measures and weave them into a more coherent strategy (see section 3).

The government also sought, and found, new partners that could support it in this new endeavour. China emerged as the most significant ally. At an ideational level, China's ability to balance control of information and the dramatic growth of internet users became a model and source of legitimation for the restrictive practices the Ethiopian government employed in the aftermath of the elections. The Chinese government not only aided Ethiopia indirectly, by offering legitimation for alternative models of media engagement, but also directly, through the provision of essential technical and financial support (see section 4).

In the decade that followed the 2005 elections, the system created by the EPRDF through trial and error appeared to hold, ensuring two rounds of uncontested elections and the apparent consolidation of power at the centre. Some of the steps taken reinforced elements commonly perceived as characteristic of a developmental state model, such as strengthening the bureaucracy and reinforcing the power of the developmental elite, together with its autonomy (Leftwich 1995; Aalen and Tronvoll 2009; Hagmann and Péclard 2010).

Behind the shell of the vast majorities ensured by the EPRDF in parliament, however, a number of events progressively undermined the party's hegemonic project. The death of Meles Zenawi in 2012 represented a challenge not only for its political allies, but also for a larger network of political and economic actors who had embraced his vision of developmentalism. A controversial figure, at both national and international levels, Meles had emerged not only as a political leader, but also as an ideologue able to support a distinctive idea of African development (de Waal 2013; Lefort 2013). The apparently smooth transition, managed behind closed doors by the main power brokers within the EPRDF, and the handling of the premiership to Meles' deputy, Hailemariam Desalegn, only for a short while appeared to guarantee the legitimacy of the same coalition of forces and political project to continue guiding the country.

 DOI: 10.19088/IDS.2021.013

Following uncontested elections in 2015, which were marked by the apathy of both opposition parties and activist groups, in a somehow unexpected turn of events there were widespread protests that broke out first in the Oromia and Amhara regions in 2015–16, and later expanded to the rest of the country. They were to significantly reconfigure the power balance in Ethiopia. Echoing features that characterised protests in Tunisia and Egypt in 2011 and 2012, the loss of credibility of elections as instruments of change, and their securitisation to avoid outbursts of violence, had elevated other, apparently less critical phenomena – such as the proposal of a new policy to extend the administrative borders of Addis Ababa further into the Oromia region – to the level of possible catalysts of participation and protest.

The protests, framed not as a generic attempt by activists to overthrow an authoritarian government, but in the context of the very type of ethnic politics promoted by the EPRDF to rule over a diverse society, asserted how the largest ethnic group in the country, the Oromo, had been excluded from power, and shook the EPRDF's ability to maintain control over power. They ultimately led to the replacement of Hailemariam Desalegn by the first Ethiopian prime minister of Oromo descent, Abiy Ahmed. The new prime minister initiated a wave of reforms that dramatically reopened civic and political space, freeing journalists and activists who had received long jail sentences and promising a redefinition of political competition in Ethiopia (Workneh 2020; Fisher and Gebrewahd 2019). A new wave of protests in 2020, however, has called some of these reforms into question and has seen the resurgence of old forms of repression by Abiy's regime, including internet shutdowns, and imprisonment of protesters and journalists (Ayana 2020).

 DOI: 10.19088/IDS.2021.013

# 3. Civic space landscape

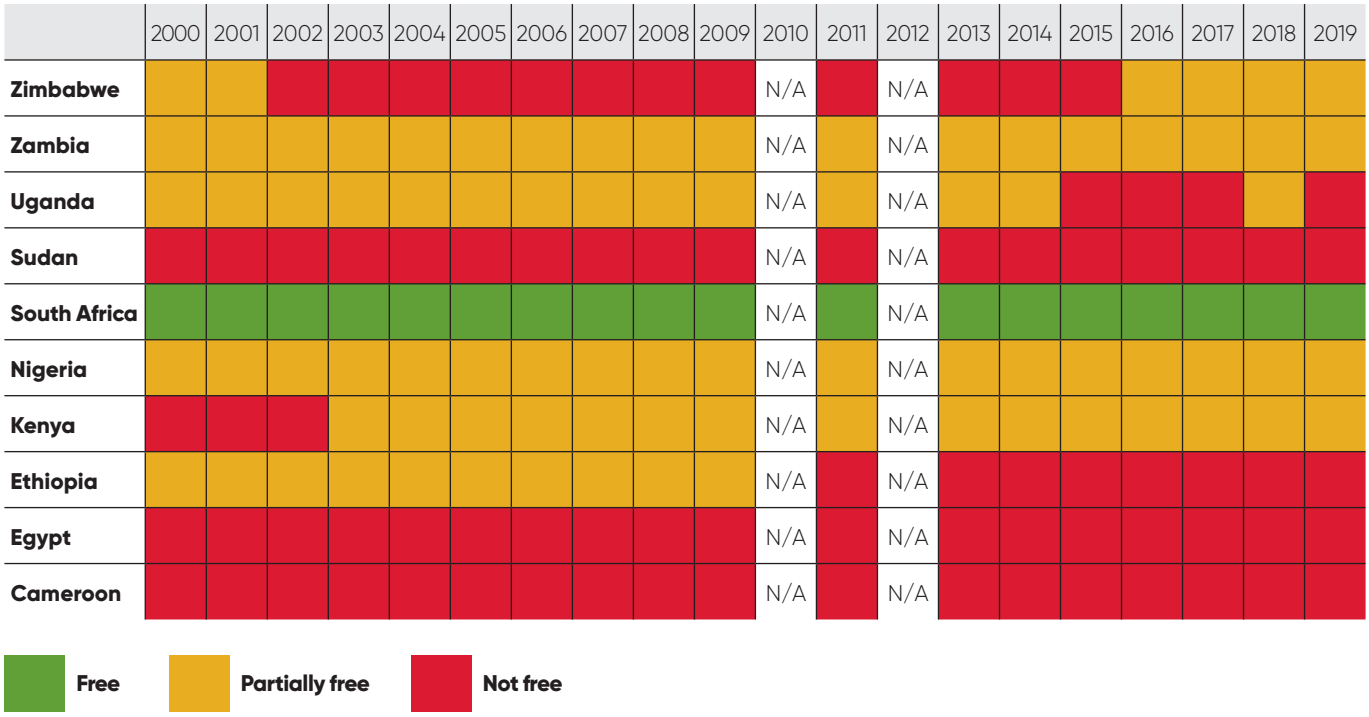
Ethiopia has a long history of tension with civil society organisations, tempered in some periods by the need to attract foreign aid and to appease requests from donors to channel some of their funds through non-governmental organisations (NGOs). During the Derg regime (1974–91) NGOs were tightly tied to the government (apart from those created by guerrilla groups in control of some areas in the north of the country). Since the EPRDF came to power in 1991, there has been greater liberalisation of the sector, allowing international NGOs to operate in the country and the emergence of some national NGOs, but also trying to exert control on large government-organised NGOs, able at the same time to attract donor funding, but also to make use of it in ways strongly controlled by the central power.

Similar to the case of the media (see section 2), this situation drastically changed after the contested elections of 2005, when the government began to seek ways to contain the influence of civil society organisations and close civic space in ways that would not irk the international community. The main tactic used by the government has been to exploit the United States (US)-backed securitisation agenda and promote laws that, on paper, were meant to contain the emergence of organisations that might threaten national security and stability, but in practice created a new space to pursue dissenters and critics (Roberts 2019).

In August 2009, the Ethiopian parliament enacted its first piece of legislation aimed specifically at combating terrorism. Framed as an attempt to comply with requests from the United Nations (UN) and the US to take the fight against international terrorism to global level, it created the legal preconditions to actually prosecute critical voices within Ethiopia (or Ethiopians in the diaspora). As indicated by the incarceration of journalists, bloggers and political opponents that followed, a legal provision aligning with international demands was used not only to fight terrorists, but also to stifle dissent. It was around this time that Ethiopia's ranking on Freedom House's Freedom Index descended from 'partially free' to 'not free' (see Figure 3.1).

 DOI: 10.19088/IDS.2021.013

# Figure 3.1 Freedom House ranking for ADRN countries, 2000–19[2]




*Note:* ADRN – African Digital Rights Network.

*Source:* Adapted from Freedom House (2019)

Ethiopia was relatively late to enact domestic anti-terrorism legislation, compared to other countries that introduced similar laws in the aftermath of the terrorist attacks in the US on 11 September 2001 (9/11) to comply with UN Security Council Resolution 1373, which requires states to ensure 'terrorist acts are established as serious criminal offences in domestic laws' (UN Security Council 2001). Coming into force only in mid-2009, Ethiopia's Anti-Terrorism Proclamation was framed nonetheless as a response to the resolution passed eight years earlier and international pressure to combat terrorism.

However, when the proclamation is considered not just in relation to the evolution of international and domestic terrorism, but also to other legal instruments the Government of Ethiopia has been developing during the same period and to the type of individuals who have been targeted, it acquires a different, more pernicious, meaning. The Anti-Terrorism Proclamation shares with the Charities and Societies Proclamation (2009), the Telecom Fraud Offences Proclamation (2012) and the Regulation for the Re-establishment of the Information Network Security Agency (INSA) (2013) the common goal of extending the government's 'legitimate' sphere of action, while limiting the possibility for other actors – domestic and international – to influence policy and politics in Ethiopia.

2 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.013

A powerful example of how governments have been able to exploit the negative sentiment emerging against civil society organisations mentioned above and use it to increase control over them, is how the Charities and Societies Proclamation has restricted NGOs that receive more than ten per cent of their financing from foreign sources from engaging in human rights and advocacy activities. The Telecom Fraud Offences Proclamation has re-affirmed the state monopoly over telecommunications, imposing severe sanctions on any operator trying to compete with or bypass Ethio-Telecom, and has extended the provisions of the Anti-Terrorism Proclamation to the online sphere (Article 6).

Since its creation, the INSA, shaped in the guise of the US National Security Agency (NSA), has taken on the responsibility of 'protecting' the national information space, 'taking counter measures against information attacks', which the law frames as any 'attack against the national interest, constitutional order, and nation's psychology by using cyber and electromagnetic technologies and systems' (Government of Ethiopia 2013). Examining the profiles of individuals convicted under the Anti-Terrorism Proclamation helps to further clarify the motivations behind the law and to understand how, similar to what had been experienced in other countries – including Colombia, Nepal, the Philippines and Uganda – the Ethiopian government interpreted the global war against terrorism as an opportunity to pursue domestic enemies while fending off external pressure and condemnation.

Out of the 33 individuals convicted under the Anti-Terrorism Proclamation between 2009 and 2014, 13 were journalists. Some of them were accused of planning terrorist attacks on infrastructure, telecommunications and power lines (Woubshet Taye and Reeyot Alemu); others of supporting Ginbot 7, an organisation led by Berhanu Nega, who in the 2005 elections had won the seat of mayor of Addis Ababa, and was included on the country's terror list soon after its establishment (Eskinder Nega, Abebe Gelaw, Fasil Yenealem and Abebe Belew). Two journalists (Solomon Kebede and Yusuf Getachew) who worked for the newspaper *Ye Musilmoch Guday* were charged with plotting acts of 'terrorism, intending to advance a political, religious, or ideological cause' (HRW 2013), as part of a broader crackdown on Ethiopian Muslims. Two Swedish journalists, Johan Persson and Martin Schibbye, who had embedded themselves with the Ogaden National Liberation Front to cover the conflict in southern Ethiopia were also charged under the Anti-Terrorism Proclamation, but were pardoned by the president after having served 450 days in prison. Some journalists have been charged in absentia; those apprehended in Ethiopia have been sentenced to up to 18 years in prison.

 DOI: 10.19088/IDS.2021.013

Numerous international organisations, including the Committee to Protect Journalists, Reporters Without Borders, Amnesty International and Human Rights Watch have accused the Ethiopian government of taking advantage of a law they have labelled as 'deeply flawed' to persecute and silence critical voices. The government has responded to this criticism by re-asserting the legitimacy of its acts.

The reliance on the Western-backed anti-terrorism agenda to pursue domestic goals, however, does not end with legal norms, but extends to the material and technological innovations that have come with it. As revealed by the leaks of security contractor Edward Snowden, in the aftermath of 9/11 the US NSA:

> set up the Deployed Signals Intelligence Operations Center – also known as 'Lion's Pride' – in Ethiopia's capital, Addis Ababa… It began as a modest counterterrorism effort involving around 12 Ethiopians performing a single mission at 12 workstations. But by 2005, the operation had evolved into eight US military personnel and 103 Ethiopians, working at '46 multifunctional workstations'.
>
> (Turse 2017)

In a leaked document, the officer-in-charge of Lion's Pride in 2005, Katie Pierce, explained, 'The benefit of this relationship is that the Ethiopians provide the location and linguists and we provide the technology and training' (*ibid.*).

Alongside Lion's Pride, the Ethiopian government's hunger for tools that could expand its ability to control communications led it to uniquely combine technologies purchased from a diverse range of actors. ZTE, as the largest telecommunication provider in the country, offered a customer management database, which, in addition to collecting records of calls made in Ethiopia, could allow access to the content of text messages and phone call audio when needed. Another tool developed by ZTE, called ZXMT, which used deep packet inspection to scan internet traffic, is also likely to have been used in Ethiopia, even if irrefutable evidence is missing (Marczak *et al.* 2014).

The Ethiopian authorities have actively shopped in the European market for advanced surveillance technologies, acquiring tools to spy not only on individuals living in Ethiopia, but also on Ethiopians in the diaspora. The government purchased FinSpy, a surveillance system sold by a firm first headquartered in the UK and later in Germany, to allow remote access to computers infected with FinSpy software. Hacking Team, an Italian company that provided 'eavesdropping software' that 'hides itself inside target devices' – which, ironically, was hacked in 2015, leading to 400GB of private communications entering the public domain – provided services

 DOI: 10.19088/IDS.2021.013

to the Ethiopian government allowing it to acquire communications from opposition leaders and journalists in the diaspora (Marczak *et al.* 2014; HRW 2014; Gagliardone 2019).

As this complex web of legal and technical resources indicates, far from being pushed into complying with an agenda imposed from above, either by partners in the West or in the East, the Ethiopian government has displayed a remarkable ability to exploit the weaknesses of different agendas to strengthen its own political plan.

## Table 3.1 Civic space timeline

| Year | Shift | Implication |
|---|---|---|
| **2000–05** | New media plurality. | Opening of civic space to engage millions in political discourse and democratic participation. |
| **2009** | Restrictive NGO law. | Disengagement. |
| | Restrictive anti-terrorism law. | Increasing use of global anti-terrorism agenda to stifle dissent. |
| **2010** | Arrests of activists. | Chilling effect and closing of space. |
| **2015** | First wave of protests in the Oromia region. | Unprecedented threat to EPRDF dominance over Ethiopia. |
| **2018** | Abiy Ahmed becomes prime minister. | Wave of reforms and opening up. |
| **2020** | New wave of protests in Oromia. | New tightening of civic and political space. |

*Sources:* Authors' own, based on Gagliardone (2014); Stremlau (2011); Mulualem (2019); Chala (2015); Bach (2011).

 DOI: 10.19088/IDS.2021.013

# 4. Technology landscape

The strategy elaborated by the EPRDF-led government to shape digital technologies in Ethiopia has been fairly distinctive in Africa. The evolution of this strategy can be mapped following two parallel trajectories: one charting the efforts to maintain a strong, centralised control over expanding access to digital media; the other in response to attempts by opposition forces to use digital technologies as instruments for political change.

While most countries on the continent slowly overcame their scepticism towards liberalising internet provision, only to later introduce regulatory or technical mechanisms to contain the tensions these measures unleashed, the Ethiopian government decided from the very beginning to sacrifice access for control and security. In the 1990s, when the first initiatives to promote internet access in Africa began to take shape, in Ethiopia, as elsewhere on the continent, there were great expectations regarding the internet's potential. Eventually, however, the government's concerns prevailed in defining the initial and future steps that the internet would take in the country.

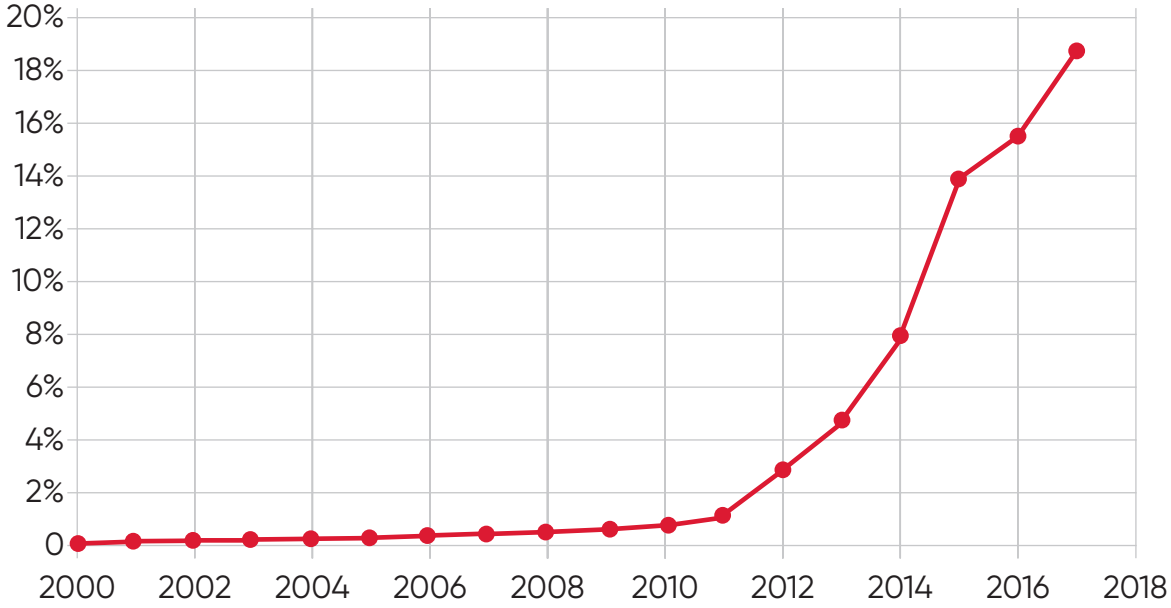
The initiative launched to structure Ethiopia's first moves in the internet era, called BITE (Bringing Internet to Ethiopia), is a vivid example of this approach. Initiated in 1995 by Dawit Yohannes, the speaker of the House of Peoples' Representatives, BITE was aimed at producing concrete recommendations on how policymakers could handle the internet effectively. Initial debate benefited from the active participation of representatives from NGOs and professional bodies, who were trying to strike a balance between the hype coming from the West and the initial scepticism and conservatism shown by the EPRDF. BITE's suggestion was to create a public network service provider, a 'not-for-profit service organisation with the main objective of serving the public and developing services' (Furzey 1995), independent from any actor in particular and accessible to all. The Ethiopian government, however, rejected the idea and decided to place service provision under its direct control.

This was only the first of a series of frustrations the private sector and civil society faced in their attempts to import tools, regulatory norms and best practices emerging at the international level. The efforts made by actors other than the government to develop a more dynamic information environment were strongly opposed. This reaction was motivated by the need to slow down the pace of transformation in order to exert more control over it; and by the desire to occupy the new political space that was created by the internet in ways that would primarily benefit the government and its national project.

 DOI: 10.19088/IDS.2021.013

This stubborn project, however, had the result of containing mobile and internet expansion for many years to come. As neighbouring countries – Kenya above all – marked rapid progress in extending connectivity across their national territories, Ethiopia languished at the bottom of digital rankings. In a dramatic move, in 2006 the government managed to secure a unique form of support that would allow it to maintain control over digital technologies while extending connectivity. In 2017, internet penetration in Ethiopia stood at just 18.6 per cent (see Figure 4.1).

## Figure 4.1 Percentage of the population with internet access in Ethiopia




*Source:* Based on data from ITU (2020)

On 8 November 2006, Chinese telecom giant ZTE and the Ethiopian Telecommunication Corporation signed the largest agreement in the history of telecommunications in Africa. Backed by China Development Bank, ZTE offered a loan of US$1.5bn (to which it added US$0.4bn for engineering) to overhaul and expand Ethiopia's telecommunications system. The loan, to be repaid over 13 years, was disbursed in three phases. The first phase had a particularly symbolic value. Branded the 'Millennium Plan', it was expected to produce its results – laying down more than 2,000km of fibre-optic cable connecting Ethiopia's 13 largest cities – by 11 September 2007, the day marking the beginning of the new millennium on the Ethiopian calendar.

 DOI: 10.19088/IDS.2021.013

The second and third phases similarly focused on infrastructure development, expanding coverage to rural areas and building the capacity of the system to support 20 million mobile users (from the initial 1.2 million) and more than a million internet broadband users. Resources also went towards upgrading the government's ambitious Woredanet and Schoolnet projects, allowing some public administrations and schools served by the two systems to progressively switch from expensive and inefficient satellite connections to terrestrial broadband.

China's support allowed the Ethiopian government to reach goals no other African country had achieved before, dramatically expanding access under a monopoly. Elsewhere in Africa, liberalisation of the market has driven expansion in coverage and lowered costs. Countries that opted for a system tightly controlled by the state, such as neighbouring Eritrea, have severely lagged behind in developing information infrastructure and services. By providing capital, equipment and expertise, all with no strings attached in terms of policy changes (e.g. liberalising the market), ZTE not only brought the Ethiopian government out of the cul-de-sac in it had put itself into by stubbornly defending its monopoly; it also helped it realise its vision of a tightly controlled but developmentally oriented national information society.

On 7 June 2011, the now rebranded Ethio-Telecom issued a tender to further boost the capacity of Ethiopia's mobile phone network to 50 million subscribers by 2015 and to introduce 4G connectivity in selected areas. The tender was similarly based on a vendor-financing scheme, as had previously been the case with ZTE. However, in contrast to 2006, the tender was public and various companies competed. As *The Wall Street Journal* put it, however, 'again, financing won the day, with the two [ZTE and Huawei] pledging a total of US$1.6bn. Western equipment suppliers, such as Ericsson and Alcatel Lucent SA, couldn't match the Chinese offer' (Dalton 2014).

With the signing of two separate contracts of US$800m each with Huawei and ZTE, competition was introduced in the shape of a rivalry between two Chinese companies that have been contending for shares of the Chinese market for a long time. China's contribution, therefore, served not only to support the unique vision elaborated by the EPRDF, but also to introduce and experiment with limited forms of competition that would not threaten the government's hegemonic position in shaping Ethiopia's information society.

Shifting the attention towards digital activism, Ethiopia has similarly charted a distinctive trajectory. During the events that followed the contested parliamentary elections of 2005, Ethiopian protesters combined new and traditional communication channels in ways that closely resembled the use of media that would characterise the 'Arab Spring' in 2011 (Gagliardone 2016; Harlow and Johnson 2011). Yet during these protests, Facebook was still in its infancy, with no presence in Africa, and Twitter had yet to be launched.

 DOI: 10.19088/IDS.2021.013

In Ethiopia in 2005, bloggers represented a new critical node that allowed innovative forms of communication to be experimented with. In the 1990s, Ethiopians in the diaspora had already created platforms that allowed bloggers to voice their opinions (e.g. Nazret), in ways that pre-dated the approach later adopted by online magazines such as Slate or *The Huffington Post* (Skjerdal 2011).

By 2005, however, a younger generation of journalists and activists (e.g. Enset, Ethio-Zagol), who were less aggrieved by long-term power struggles, had begun to experiment with new ways of reporting that eschewed the most polarised tones (*ibid.*), becoming representative of a new willingness to embrace technology to promote political change. In a move that dramatically increased their reach, commentaries and political manifestoes published online began to be printed and were turned into leaflets for distribution on the ground in Ethiopia. Before and after the 2005 elections, mobile phones, and especially SMS (text messages) were also widely used to mobilise protests in real time and disseminate calls to action initially posted on web forums.

This convergence of different media channels used in 2005 deeply resonates with the 'media relays' that characterised the protests in Tunisia and Egypt in 2010, when activists combined different media to reach those who had no access to the latest technologies (Wilson and Dunn 2011; Aouragh and Alexander 2011). Yet, in striking contrast to the media and scholarly attention given to the Arab Spring, similar use of new media in Ethiopia five years earlier received negligible international attention. International news coverage mostly focused on the political violence around the elections and not on this revolutionary use of new media *avant la lettre*.

While international commentators did not understand or report on these early forms of digital activism in Ethiopia, the Ethiopian rulers took notice. So much so that, after the protests and the violence had subsided, the Ethiopian government started to progressively trim the complex communication network that had assembled different voices across a plurality of media. First, the SMS network was interrupted (June 2005). A few months later, some of the most vocal Ethiopian journalists who challenged the results of the elections and called for greater democracy were arrested and their papers forced to close (November 2005). Finally, one year after the contested elections, the government started to block access to blogs and websites where dissenting opinions were found (May 2006).

This 'failed revolution' represented the beginning of a complex process of negotiation between the Ethiopian government and various generations of digital activists seeking to use new media to promote political change. Two events epitomise the evolution of this process, indicating significant shifts in the power dynamics between government and civil society.

 DOI: 10.19088/IDS.2021.013

The first was the emergence and repression of yet another generation of digital activists seeking to use social media to engage and seek to constructively challenge the Ethiopian government. Centred on Zone9, a collective of bloggers created in 2012, the criticism that emerged in this phase distanced itself from older grievances and accusations. Instead, it advocated reform from within, rather than beyond the political framework created by the EPRDF. Unlike bloggers posting on diaspora-led platforms such as Nazret or Ethiomedia, they decided not to attack core elements of the EPRDF's ideology (i.e. ethnic federalism and revolutionary democracy). The Zone9ers, on the contrary, asked Ethiopian rulers to #RespectTheConstitution, the hashtag used for one of their campaigns pressuring the government to live up to the principles it had established to rebuild the nation after the civil war, including the right to freedom of expression.

In contrast to many bloggers in the Ethiopian diaspora who tended to write in English, most Zone9ers privileged Amharic in their posts, signalling a willingness to contribute to national debates and reach a broader audience within Ethiopia. Rather than considering Ethiopian rulers as enemies to confront and attack, they exploited the power of social networking platforms such as Twitter to initiate conversations with those in power; for example, engaging in unprecedented debates with Foreign Minister Tedros Adhanom, the government's most active presence on social media.

Despite efforts to build a middle ground from which to engage with the Ethiopian government, and calling for reform from within rather than an overthrow of the regime, on 25 April 2014, six of the bloggers – Abel Wabella, Atnaf Berhane, Mahlet Fantahun, Natnail Feleke, Zelalem Kibret and Befekadu Hailu – were arrested, along with three other journalists – Asmamaw Hailegeorgis, Tesfalem Waldyes and Edom Kassaye. The initial charges included working with international human rights organisations and taking part in digital security training (BBC News 2014). The group was subsequently also charged with terrorism. The accusations included collaborating with outlawed opposition groups such as Ginbot 7 and conspiring with foreign organisations to use social media to destabilise Ethiopia. Some of the evidence given in support of the charges of terrorist activity during the court cases included the use of Tactical Technology Collective's 'Security in a Box: Tools and Tactics in Digital Security' and blog commentary on Wael Ghonim's book *Revolution 2.0* about the use of social media during the Arab Spring and its potential relevance for Ethiopia.

The arrests stirred a high-profile international social media campaign to free the arrested bloggers, which spread online behind the #FreeZone9Bloggers hashtag. The popularity of the campaign was unprecedented in Ethiopia. After its launch, the campaign gained visibility internationally, including the first Africa-wide 'tweetathon' organised in solidarity by Nigerian and Tanzanian bloggers, and legal petitions addressed to the African Union and the UN Human Rights Council.

 DOI: 10.19088/IDS.2021.013

The campaign was especially active during the initial months of imprisonment, and was promoted by international human rights and freedom of speech organisations such as the Committee to Protect Journalists, Human Rights Watch, Global Voices, the Media Legal Defence Initiative, Electronic Frontier Foundation and Reporters Without Borders. After tens of delayed court hearings and over 500 days in prison without charge, the Zone9 bloggers were finally acquitted of terrorism charges in October 2015 (BBC News 2015).

## Table 4.1 Technology timeline

| Year | Shift | Implication |
|---|---|---|
| **1995** | Bringing internet to Ethiopia (BITE) commission. | First failed attempt at multi-stakeholder engagement in Ethiopia; it poisons the relationship between government and civil society in the digital space. |
| **Late 1990s** | Launch of first blogging platforms by the Ethiopian diaspora (e.g. Ethiomedia, Nazret, Ethiopian Review). | First attempts with online media are very antagonistic towards the EPRDF-led government, creating a perception that online media are by nature adversarial. |
| **2004** | State-sponsored projects Woredanet and Schoolnet go online. | These projects represent the first attempts by the Ethiopian government to use digital media to empower its communication and control with the peripheries of the state. |
| **2005** | First openly contested elections in Ethiopia and widespread censorship online. | After losing control of more seats in parliament than expected, and blaming digital media for some of the losses, the government begins its first experiment with online censorship, building the foundations for subsequent measures to control and contain online dissent. |
| **2006** | First contract with ZTE for network expansion project. | Largest Chinese intervention in ICTs in Africa. |
| **2011** | Second contract with ZTE and Huawei to further expand mobile and internet connectivity. | Consolidation of relationship with China. |
| **2016** | First internet shutdown in Ethiopia. | Proclaimed by the government as a measure to prevent cheating in national exams – but it will become increasingly pervasive in the country in stifling political dissent. |
| **2017** | Qero and Faro hashtags and memes. | Opening up of new space with new actors outside formal civic organisations. |
| **2018** | Rise to power of Abiy Ahmed and opening up of online spaces. | Greater freedom allowed for online media, as well as for the press. |
| **2019** | Return to internet shutdowns and repressive measures. | Initial opening by Abiy's government called into question; return to 'old tactics'. |

*Sources:* Authors' own, based on Chala (2019); 2018; Mulualem (2019); Marchant and Stremlau (2020); Gagliardone (2013); Skjerdal (2011); Gagliardone (2016).

 DOI: 10.19088/IDS.2021.013

# 5. Digital rights landscape

As mentioned in previous sections, the Ethiopian government has been able to combine skills and tools acquired from different partners (e.g. surveillance training from the US government; software sold by European, Israeli and Chinese companies) to develop a complex apparatus of surveillance. It has also developed unique systems to project its control over the country, while improving service delivery. An example is TeleCourt, a system offering remote trials through plasma-screen TVs disseminated in government offices (Beyene, Zerai and Gagliardone 2015). Its centralised control of telecommunications has also made it relatively easy to enact internet shutdowns at local and national levels. Internet shutdowns became a recurring feature starting from 2016, affecting either specific regions where protests emerged (e.g. Oromia), or extending to the whole country (sometimes with the exception of the capital Addis Ababa) when protests became more generalised.

The threat posed by the rising discontent ultimately leading to widespread protests in the Oromia and Amhara regions, and the role social media played in fuelling and coordinating the protest, also led the Ethiopian government to develop and sharpen its computational propaganda tools (Chala 2018; Bradshaw and Howard 2019). Available evidence illustrates how the government has mostly made use of human agents (e.g. paid trolls or individuals belonging to party ranks) to steer public opinion, on issues related to the causes and motivations of protests, but also in the preparation of events of national relevance (e.g. religious or public events), as well as promoting fake news that could undermine support for dissenting groups (Chala 2018). As political competition became fiercer after the rise to power of Abiy Ahmed, new fronts of disinformation emerged, pitting members of the EPRDF coalition against one another (Chala 2019). Also, oppositional voices have joined the fray and popular representatives of political parties that have emerged as an alternative to the EPRDF have been accused of fomenting disinformation in ways that can lead to violence among competing ethic groups (Meseret 2020).

Individuals and civil society organisations are caught in a complex conundrum. In the past (e.g. during the 2005 elections discussed in section 2), Ethiopian journalists and activists displayed great ingenuity in combining old and new media, and a variety of tactics to amplify their messages and reach different types of audiences. Collaborations have emerged between activists and academics to assess digital rights in the country (e.g. between the OpenNet Initiative and The Citizen Lab to uncover surveillance; collaborations with the University of Oxford to map hate speech online) but these have not led to a consolidation of skills in the country that can be easily deployed when required (Marczak *et al.* 2014; OpenNet Initiative 2007; Gagliardone *et al.* 2016).

 DOI: 10.19088/IDS.2021.013

# 6. Conclusion

Ethiopia is at a complex crossroads. On the one hand, the rise to power of Abiy Ahmed built the foundations for important reforms in the media and civic space. Since 2018, media outlets have blossomed, also allowing long-time critics of the regime to launch publications and voice their opinions. Telecommunications have been liberalised, ending the anachronistic monopoly that had characterised Ethiopia for decades. Greater opportunities for political competition have been created and future elections – originally planned for August 2020, but postponed due to Covid-19 – may be the most contested since 2005.

On the other hand, Abiy's reforms have created tensions within the EPRDF coalition, especially with the once hegemonic Tigrayan People's Liberation Front. In 2020, new waves of protests led to the resurgence of repressive techniques used by rulers who preceded Abiy, including internet shutdowns and the imprisonment of critics of the regime. Digital activism holds the promise of engaging the government on new grounds, allowing the consolidation of digital rights and new alliances between extra-parliamentary and formal politics. But these avenues are fragile and it is unclear how they will evolve in the short and medium terms.

 DOI: 10.19088/IDS.2021.013

# References

Aalen, L. (2006) 'Ethnic Federalism and Self-Determination for Nationalities in a Semi-Authoritarian State: The Case of Ethiopia', *International Journal on Minority and Group Rights* 13.2–3: 243

Aalen, L. and Tronvoll, K. (2009) 'The End of Democracy? Curtailing Political and Civil Rights in Ethiopia', *Review of African Political Economy* 36.120: 193–207

Abbink, J. (2011a) 'Democracy Deferred: Understanding Elections and the Role of Donors in Ethiopia', in J. Abbink and M. de Bruijn (eds), *Land, Law and Politics in Africa: Mediating Conflict and Reshaping the State*, Boston MA: Brill Academic Publishers

Abbink, J. (2011b) **'Ethnic-Based Federalism and Ethnicity in Ethiopia: Reassessing the Experiment after 20 Years'**, *Journal of Eastern African Studies* 5.4: 596–618 (accessed 16 October 2020)

Aouragh, M. and Alexander, A. (2011) 'The Arab Spring – The Egyptian Experience: Sense and Nonsense of the Internet Revolution', *International Journal of Communication* 5: 15

Ayana, R. (2020) **'How the Murder of an Ethiopian Singer Triggered an Uprising Against a Disintegrating Democracy'**, *Time*, 24 July (accessed 16 October 2020)

Bach, J.-N. (2011) ***'Abyotawi* Democracy: Neither Revolutionary nor Democratic, a Critical Review of EPRDF's Conception of Revolutionary Democracy in Post-1991 Ethiopia'**, *Journal of Eastern African Studies* 5.4: 641–63 (accessed 16 October 2020)

BBC News (2015) **'Ethiopian Zone 9 Bloggers Cleared of Terrorism Charges'** 16 October (13 November 2020)

BBC News (2014) **'Ethiopia Zone 9 Bloggers Charged with Terrorism'**, 18 July (accessed 13 November 2020)

Beyene, Z.; Zerai, A. and Gagliardone, I. (2015) **'Satellites, Plasmas and Law: The Role of TeleCourt in Changing Conceptions of Justice and Authority in Ethiopia'**, *Stability: International Journal of Security and Development* 4.1 (accessed 13 November 2020)

Bradshaw, S. and Howard, P.N. (2019) *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Oxford: The Computational Propaganda Project, University of Oxford

Carter Center (2005) **'Final Statement on the Carter Center Observation of the Ethiopia 2005 National Elections'**, 15 September (accessed 13 November 2020)

Chala, E. (2019) ***How Ethiopia's Ruling Coalition Created a Playbook for Disinformation***, Global Voices blog, 18 October (accessed 13 November 2020)

Chala, E. (2018) ***Leaked Documents Show that Ethiopia's Ruling Elites Are Hiring Social Media Trolls (and Watching Porn)***, Global Voices blog, 20 January (accessed 13 November 2020)

Chala, E. (2015) **'Violent Clashes in Ethiopia over 'master Plan' to Expand Addis'**, *The Guardian*, 11 December (accessed 13 November 2020)

Dahir, A.L. (2016) **'Internet Shutdown Could Cost Ethiopia's Booming Economy Millions of Dollars'**, *Quartz*, 19 October (accessed 16 October 2020)

Dalton, M. (2014) 'Telecom Deal by China's ZTE, Huawei in Ethiopia Faces Criticism', *Wall Street Journal*, 7 January

De Waal, A. (2013) 'The Theory and Practice of Meles Zenawi', *African Affairs* 112.446: 148–55

Freedom House (2019) ***Freedom in the World*** (accessed 4 December 2020)

Fisher, J. and Anderson, D.M. (2015) 'Authoritarianism and the Securitization of Development in Africa', *International Affairs* 91.1: 131–51

Fisher, J. and Gebrewahd, M.T. (2019) ' "Game over"? Abiy Ahmed, the Tigrayan People's Liberation Front and Ethiopia's Political Crisis', *African Affairs* 118.470: 194–206

Fourie, E. (2015) 'China's Example for Meles' Ethiopia: When Development "Models" Land', *The Journal of Modern African Studies* 53.3: 289–316

 DOI: 10.19088/IDS.2021.013

Furzey, J. (1995) *A Critical Examination of the Social, Economic, Technical and Policy Issues, with Respect to the Expansion or Initiation of Information and Communications Infrastructure in Ethiopia*, A Country Study for the United Nations Economic Commission for Africa High-Level Working Group on Information and Communication Technologies in Africa: Empowering Socio-Economic Development in Africa Utilizing Information Technology, Philadelphia PA: African Studies Center, University Of Pennsylvania

Gagliardone, I. (2019) *China, Africa, and the Future of the Internet*, London: Zed Books

Gagliardone, I. (2016) *The Politics of Technology in Africa*, Cambridge: Cambridge University Press

Gagliardone, I. (2014a) ' "A Country in Order": Technopolitics, Nation Building, and the Development of ICT in Ethiopia', *Information Technologies and International Development* 10.1

Gagliardone, I. (2014b) 'New Media and the Developmental State in Ethiopia', *African Affairs* 113.451: 279–99

Gagliardone, I. *et al.* (2016) ***Mechachal: Online Debates and Elections in Ethiopia-From Hate Speech to Engagement in Social Media***, DOI: 10.2139/ssrn.2831369 (accessed 16 October 2020)

Hagmann, T. and Abbink, J. (2011) **'Twenty Years of Revolutionary Democratic Ethiopia, 1991 to 2011'**, *Journal of Eastern African Studies* 5.4: 579–95 (accessed 16 October 2020)

Hagmann, T. and Péclard, D. (2010) 'Negotiating Statehood: Dynamics of Power and Domination in Africa', *Development and Change* 41.4: 539–62

Harlow, S. and Johnson, T.J. (2011) 'The Arab Spring: Overthrowing the Protest Paradigm? How The New York Times, Global Voices and Twitter Covered the Egyptian Revolution', *International Journal of Communication* 5: 16

HRW (2014) *'They Know Everything We Do': Telecom and Internet Surveillance in Ethiopia*, New York NY: Human Rights Watch

HRW (2013) **'Ethiopia: Terrorism Law Decimates Media'**, 3 May (accessed 13 November 2020)

ITU (2020) ***Internet Access Statistics***, International Telecommunication Union (accessed 4 December 2020)

Lefort, R. (2013) 'The Theory and Practice of Meles Zenawi: A Response to Alex de Waal', *African Affairs* 112.448: 460–70

Leftwich, A. (1995) 'Bringing Politics Back in: Towards a Model of the Developmental State', *The Journal of Development Studies* 31.3: 400–27

Marchant, E. and Stremlau, N. (2020) 'The Changing Landscape of Internet Shutdown in Africa: A Spectrum of Shutdowns: Reframing Internet Shutdowns From Africa', *International Journal of Communication* 14: 18

Marczak, B.; Guarnieri, C.; Marquis-Boire, M. and Scott-Railton, J. (2014) ***Hacking Team and the Targeting of Ethiopian Journalists***, The Citizen Lab blog, 12 February (accessed 16 October 2020)

Meseret, E. (2020) **'Hate Speech and Disinformation Concerns Escalate in Ethiopia'**, *Devex*, 6 May (accessed 13 November 2020)

Mulualem, D.T. (2019) 'Qeerroo Fi Qarree: The Engine of Current Transition in Ethiopia Politics', *International Journal of Scientific and Research Publications* 9.5

OpenNet Initiative (2007) ***Ethiopia*** (accessed 23 October 2020)

Pausewang, S.; Tronvoll, K. and Aalen, L. (2002) *Ethiopia since the Derg: A Decade of Democratic Pretension and Performance*, London: Zed Books

Rashid, S. (2015) **'Commodity Exchanges and Market Development: What Have We Learned?'**, paper for International Conference of Agricultural Economists 'Agriculture in an Interconnected World', Università degli Studi di Milano, Milan, Italy, 8–14 August 2015 (accessed 13 November 2020)

Roberts, T. (2019) ***Closing Civic Space and Inclusive Development in Ethiopia***, IDS Working Paper 527, Brighton: Institute of Development Studies (accessed 13 November 2020)

Skjerdal, T.S. (2011) 'Journalists or Activists? Self-Identity in the Ethiopian Diaspora Online Community', *Journalism* 12.6: 727–44

Stremlau, N. (2011) 'The Press and the Political Restructuring of Ethiopia', *Journal of Eastern African Studies* 5.4: 716–32

Turse, N. (2017) **'How the NSA Built a Secret Surveillance Network for Ethiopia'**, *The Intercept*, 13 September (accessed 16 October 2020)

UN Security Council (2001) *Resolution 1373*, United Nations

Wilmot, C. (2020) **'Ethiopia's Cracking down in Tigray. But Activists Are Spreading the News'**, *The Washington Post*, 11 November (accessed 4 December 2020)

Wilson, C. and Alexandra, D. (2011) 'Digital Media in the Egyptian Revolution: Descriptive Analysis from the Tahrir Data Sets', *International Journal of Communication* 5: 1248–72

Workneh, T.W. (2020) **'Social Media, Protest, & Outrage Communication in Ethiopia: Toward Fractured Publics or Pluralistic Polity?'**, Information, Communication and Society (advance online publication), DOI: 10.1080/1369118X.2020.1811367 (accessed 16 October 2020)

# Egypt Digital Rights Landscape Report

Mohamed Farahat



This report is part of 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries'; the Introduction is also recommended reading.

© 2021 Mohamed Farahat © Institute of Development Studies. DOI: 10.19088/IDS.2021.014

# 1. Introduction

Egypt has experienced many political and social changes prior to and since the 2011 uprising. These changes have had a significant impact on civic space offline, as well as online. Digital rights are simply human rights in online spaces and are recognised as being of central importance. This is especially true when closing civic space in the physical world means that opening civic space online is a necessary last resort. The coronavirus (Covid-19) pandemic has highlighted the importance of digital rights, especially for vulnerable groups such as refugees and people in rural and remote areas.

The main objective of this report is to give an overview of digital rights in Egypt, especially in the context of freedom of expression and freedom of assembly, the right to access the internet, and for access to information, and the right to knowledge; and to explore the impacts of the political context on civic space in general and digital rights in particular.

Social media played a significant role during the political mobilisation of 2011 that led to the removal of the regime of Hosni Mubarak, the Middle East and North Africa region's longest-surviving regime at the time. Subsequent regimes have paid special attention to digital rights and social media, and taken all possible measures to control internet access and target activists, whether using technical means through censorship and surveillance of their online activities; or through legislative tools that legalise internet shutdowns, banning websites and criminalising the right to freedom of expression by labelling anything that challenges the government as fake news. These practices have proliferated during the Covid-19 pandemic, which has been dealt with as a national security issue. As a result, bloggers, journalists and doctors who share information about the number of infected people have been targeted and jailed, accused of publishing fake news.

 DOI: 10.19088/IDS.2021.014

# 2. Political landscape

Undoubtedly, civic space and its actors and dynamics in general are affected positively and negatively by the political environment. There is a positive direct relationship between the political environment and civic space in terms of how open or closed it is. The political environment is described as an open environment when it allows and accepts criticism, and accommodates different variables and positively interacts with different components of the political environment.

Egypt has witnessed significant political openings and closings throughout the past 20 years. For the purposes of this report, the political landscape will be addressed during two main phases. The first phase extends from 2000 to 2010. The second phase extends from 2011 to the present.

## 2.1 First phase (2000–10)

This phase was under the Mubarak regime, which was in power from 1981 until the 2011 'revolution'. The political situation was stable during the period from 2000 to 2010 as regards civic space and digital rights. The Mubarak regime adopted policies that led to a relatively open civic space. Irrespective of the human rights situation, human rights activists enjoyed the freedom to speak out about the human rights situation and establish new organisations.

Although, the political atmosphere under the Mubarak regime permitted some level of openness in civic space, it did not prevent the eventual uprising against the regime. Many factors contributed to the uprising, including corruption (Hassan 2011), control of the political space and human rights violations (Rastegari 2012), but there were two main triggers: firstly, electoral fraud during the 2010 legislative elections, which resulted in the National Party controlling the vast majority of seats in parliament (Bakr 2016: 61, 66); and secondly, the death of Khaled Saeed, a youth who was reportedly tortured to death by Egyptian police in June 2010 (*ibid.*: 65).

## 2.2 Second phase (2011–present)

The second phase is divided into two main landmark periods of political and social changes: the first period from 2011 to the end of June 2013; and the second period from July 2013 up to the present day. During the first period, also known as the Arab Spring, civil society played a significant role and was the main engine of the social and political mobility that took place not only in Egypt but in all countries that witnessed political regime change during the period (ANND 2020).

 DOI: 10.19088/IDS.2021.014

Egypt saw a transitional period from the end of February 2011 until Mohamed Morsi was elected as president in June 2012. The Supreme Council of the Armed Forces (SCAF) managed the transitional process, implementing laws and regulations, and issuing a constitutional declaration to regulate the interim period between the revolution and the adoption of the new constitution. 'Other issues of national interest addressed by the SCAF included electoral law reform, adoption of pro-freedom of association measures and media related reforms such as appointment of new editors' (Dube, Simiyu and Ilori 2020: 26). Thus, this period could be characterised as a period of relative political opening.

## 2.3 Muslim Brotherhood regime (2012–13)

The Muslim Brotherhood regime came to power in Egypt after the presidential election on 30 June 2012, which resulted in Mohamed Morsi being elected as president. Ten months later, the Tamarod protest movement was established and began collecting signatures to 'withdraw confidence' from President Morsi and mobilise citizens for a demonstration on 30 June 2013. Social media was the main tool used to mobilise for the demonstration, which led to the removal of Morsi and the Muslim Brotherhood regime from power. In July 2013, the General Command of the Armed Forces issued a statement that led to the ousting of the regime (Arab Republic of Egypt 2013). The political situation and civic space changed significantly after July 2013, resulting in a closing of civic space.

 DOI: 10.19088/IDS.2021.014

# 3. The civic space landscape

Civic space is one of the most influential factors in Egyptian political dynamics. In light of weak political parties, civil society has become the real political opposition to the regime. It is recognised that civil society does not operate or develop in a vacuum, but instead reflects the general political situation. The political context in Egypt as described in section 2 has a significant impact on the degree of openness of civic space in Egypt. Civic space in Egypt could not be described as completely closed, but it is relatively restricted (ANND 2019). In contrast, Egypt has consistently received a score of 'not free' by Freedom House (see Figure 3.1).

## Figure 3.1 Freedom House ranking for ADRN countries, 2000–19[1]


*Note:* ADRN – African Digital Rights Network.

*Source:* Adapted from Freedom House (2019)

In light of the political changes in Egypt since 2011, civil society took the lead in demanding political regime change; the use of technology and social media for social mobilisation that facilitated the 2011 uprising and, later, the removal of the Mubarak regime, marked the beginning of the closure of civic space in Egypt, and different measures were taken to reduce the activities of civil society or totally stop activities.

1 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.014

The period from 2000 until the 2011 uprising had witnessed an increase in the activities of non-governmental organisations (NGOs) and the establishment of new organisations (ANND 2020). Although international and internal pressure led the Mubarak regime in this period to take steps to open civic space (*ibid.*) and take the lead in democratic transition from the top down, this does not reflect the fact that Egypt's NGO laws were flexible or in line with international human rights law and standards.

For example, Law No. 84 of 2002 concerning national associations required that all NGOs register with the Ministry of Insurance and Social Affairs; banned any civil society activities that threatened national unity or violated public order or morality, and prohibited groups from receiving foreign funding without advance approval; and made the establishment of new NGOs subject to authorities' absolute discretion. Despite the restrictive nature of the law, civic space at that time could be described in general as relatively open compared to the current Egyptian civic space landscape. Civil society organisations (CSOs) and activists enjoyed the freedom to criticise the political situation and the regime:

> The NGOs legal framework did not serve to ban civil society outright but rather gave enormous discretionary powers to the Ministry of Social Solidarity and other government agencies. In practice, this authority was brought to bear against certain organizations and individuals that crossed the government's 'red lines' in pushing for social reform and political liberalization. (ICNL 2020)

Thus, political regimes in Egypt, whether during the Mubarak era or since 2011, 'have selectively used civil society restrictions to ensure civic mobilization did not cross the ruling regime's red lines' (Brechenmacher 2017: 37).

Following the 2011 uprising, the civil society environment became more repressive. The new regime took action to close civic space with measures targeted at NGOs:

> 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 uprising in 2011 was a short-lived relief for the civil society as the civic space closed and the government began to implement repressive practices under the current presidency of Abdel Fattah el-Sisi. (Dube *et al.* 2020: 26)

 DOI: 10.19088/IDS.2021.014

Egypt has used various tactics to close civic space, and reduce and control the activities of civil society activists and organisations, or force them to give up their activities to avoid being targeted. These tactics include criminalisation of public dissent in the name of national security and counterterrorism, use of legal reforms and decrees to institutionalise previously extrajudicial repressive practices, public vilification, sweeping legal measures, and civil society co-optation. For instance, the regime has used sweeping antiterrorism and anti-protest measures to institutionalise previously extrajudicial practices.

Egyptian authorities have targeted human rights groups with travel bans, asset freezes and legal harassment, while local development and civic initiatives struggle to access resources for their work (Brechenmacher 2017: 45; Dube *et al.* 2020). The government engaged in a more overt and sweeping crackdown on civil society including a criminal case launched in 2011, focused on Egypt-based international organisations alleged to have received foreign funding without government permission, which was reopened and expanded in 2016 to focus on Egyptian organisations.

The Penal Code also contributed to the closing of civic space in Egypt. Under the Penal Code, assets could be frozen and travel bans imposed for vague criminal charges mostly associated with terrorism. Article 78 of the Penal Code was amended by the 2014 presidential decree to enforce penalties of up to 25 years in prison for receipt of foreign funding to undertake activities deemed detrimental to national security by the government. The International Center for Not-for-Profit Law (ICNL) reports that:

> From 2016 through 2019, a number of Egypt's most prominent civil society leaders have been banned from travel in connection with the amended law, and several had their personal and organisational assets frozen under court order. Others have been detained and interrogated.
> (ICNL 2020)

Egyptian authorities initiated a wave of raids, interrogations, asset freezes, and travel bans. Brechenmacher (2017: 45) reports, for example, that:

> In September 2016, a criminal court issued an order to freeze the personal assets of five prominent human rights advocates and three NGOs: the Cairo Institute for Human Rights Studies, the Hisham Mubarak Law Center, and the Egyptian Center for the Right to Education. Four months later, women's rights advocate Azza Soliman became the first to be arrested in connection to the case – a few weeks after authorities had frozen her personal and organizational assets and prevented

 DOI: 10.19088/IDS.2021.014

her from traveling abroad. In 2017, the government approved a new draconian law to govern CSOs, 'Law 70 of 2017 on Associations and Other Foundations Working in the Field of Civil Work' which replaced Law 84 of 2002. Domestic and international CSOs, governments, and UN entities roundly condemned the restrictive new law, which created egregious constraints on CSOs' formation, funding, activities, contact with international entities, internal governance, and imposed severe criminal penalties on CSOs for violations. Despite its ratification, the law was never fully enforced—the government never issued implementing regulations to guide its application—and in November of 2018, President el-Sisi publicly indicated that he supported amendment of the law.

In 2019, the Egyptian parliament (House of Representatives) adopted the new NGO law. Groups most affected included bloggers, trade unionists, students, opposition political activists, lawyers, lesbian, gay, bisexual, transgender, intersex or queer (LGBTIQ) and women's rights activists, doctors and CSOs (Dube *et al.* 2020). The restrictive measures were extended to include non-activist citizens who use their own accounts on social media applications to criticise government policies or share and address topics that might be considered prejudicial to national security, such as the health situation during the Covid-19 pandemic. According to CIVICUS Monitor (CIVICUS 2020), civic space in Egypt is rated as 'closed'.

In the conclusion of this section, a quick comparison between the situation of civic space before and after 2011 shows that domestic civic space has historically been restricted, but to varying degrees. As mentioned earlier, the Mubarak regime enforced red lines for civil society, but never closed civic space completely and the situation could be described as close to being open. However, 'the opening of civic space under Mubarak's regime was not a sign of democratisation but it was a move towards consolidating authoritarianism' (Hassan 2011: 3). Under successive regimes, civic space never totally closed but witnessed an increasing number of red lines and could be described as a closing of civic space. One common feature of the situation of civic space under the different ruling regimes is that it was never fully open.

 DOI: 10.19088/IDS.2021.014

# Table 3.1 Civic space timeline

| Year | Regime | Shift | Implication |
|---|---|---|---|
| **1971** | Anwar Sadat | Adoption of permanent constitution | Explicitly stipulated rights to freedom of assembly and to establish NGOs. |
| **2002** | Hosni Mubarak | NGO law | The new law was restrictive: NGOs could only be established upon approval from the Ministry of Social Affairs. |
| **2012** | Mohamed Morsi/Muslim Brotherhood | New constitution after 2011 uprising | NGOs could in theory be established by notifying the authorities, but this was not the case in practice. |
| **2014** | Abdel Fatah El Sisi | Penal Code | The Penal Code criminalised NGOs that received funds from abroad without prior approval. |
| **2015** | Abdel Fatah El Sisi | Counter-terrorism law | The law was a new tool to close civic space and criminalise NGO activities, especially those which received funds from abroad. |
| **2017** | Abdel Fatah El Sisi | Restrictive new NGO law | The proposed new law was to completely close civic space. It was condemned by domestic and international organisations and activists, which led to its suspension. |
| **2019** | Abdel Fatah El Sisi | New NGO law | The new law seemed to promise an opening up of civic space, but it is still too early to judge its implications. |

*Source:* Author's own.

 DOI: 10.19088/IDS.2021.014

# 4. Technology landscape

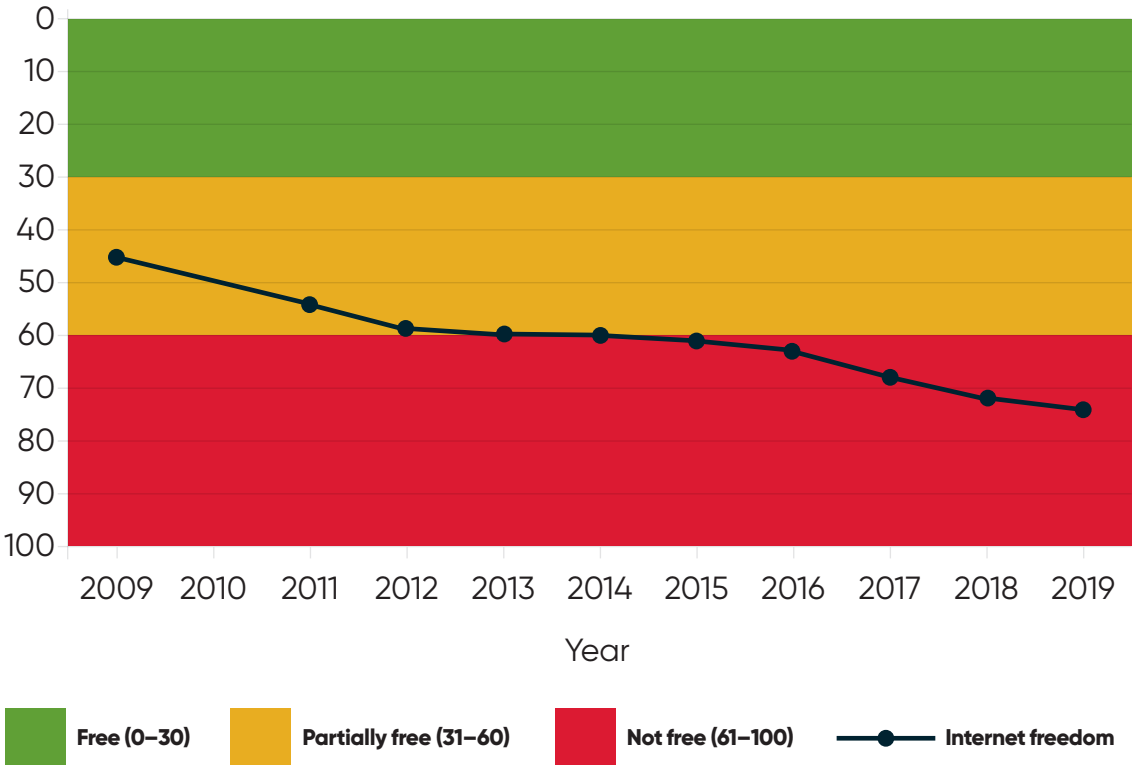
Undoubtedly, the use of technology, the internet, information and communication technology (ICT) tools and applications, social media and digital rights characterised the uprising in 2011, through communicating and 'organising through Facebook, Twitter, blogs, and YouTube' (Bakr 2016: 68). It had a significant role in mobilising for political changes in Egypt, both during the 2011 uprising and second uprising on 30 June 2013:

> Between 11 January and 10 February 2011, there were 34 million participants in the revolution on Facebook across 2,313 pages, where 9,815 participants got 461,000 commentaries. During the period between 10 January and 10 February, 93 million tweets on the revolution were exchanged within Egypt, and between Egypt and the outside world.
> (*Ibid.*)

As a result of political changes and the closing of civic space offline from 2011 up to now, political activists, human right activists, journalists, bloggers and citizens have moved to online platforms as a last resort to exercise their rights to access and share information, criticise government policies and political measures, and engage in public affairs. Therefore, very restrictive measures have been taken to repress and criminalise digital rights and access to information. Due in part to these restrictive measures, Egypt's score on Freedom House's Freedom on the Net Index fell from 'partially free' to 'not free' (see Figure 4.1).

 DOI: 10.19088/IDS.2021.014

## Figure 4.1 Egypt's Freedom on the Net Index score, 2009–19[2]




*Source:* Based on data from Freedom House (2020)

2 Data not available for 2010.

 DOI: 10.19088/IDS.2021.014

## 4.1 Using technology: legal framework

Internet use is governed by the Telecommunications Regulation Law of Egypt No. 10 (2003), which was used as the legal basis to shut down the internet during the Egyptian uprising in 2011. Article 67 of the law allows authorities to shut down telecommunications operator networks for reasons of 'national security' as defined by the authorities.

In 2018, the Egyptian parliament issued Law No.175 of 2018 on Combating Information Technology Crimes (Cybercrimes Law) and Law No. 180 of 2018 on regulating press and media. The new provisions gave authorities the power to block websites if they violated national security. Article 1 of the Cybercrimes Law defines national security as everything related to the independence, stability and security of the homeland, and anything related to the affairs of the Presidency, the Ministry of Defence and General Intelligence and so on. The same definition is also repeated in many laws regulating the internet, without any definition or explanation of the concept of national security or clarification of its determinants (El Asouad 2016).

It is clear from the text that the term 'national security' is a loose phrase that cannot be defined. Just as the authorities define what is considered as security, some believe that through the Cybercrimes Law the state aims to fully control the internet, suppress its users and to legalise state practices in censoring this space, including blocking websites and using mass surveillance of communications. Some would add that the Cybercrime Law and the press and media regulation law are two laws that clearly establish the practice of blocking websites and monitoring communications in Egypt. Before the adoption of these controversial laws, the Egyptian legal environment lacked the legal cover and legal justification for the practice of blocking online content. Egyptian authorities scaled up their online content-blocking efforts in May 2017, resulting in the blocking of nearly 500 websites. According to Article (19) of Law No. 180 of 2018 on regulating press and media (Press and Media Regulation Law), the authorities have the right to block websites and electronic news that they characterise as fake news.

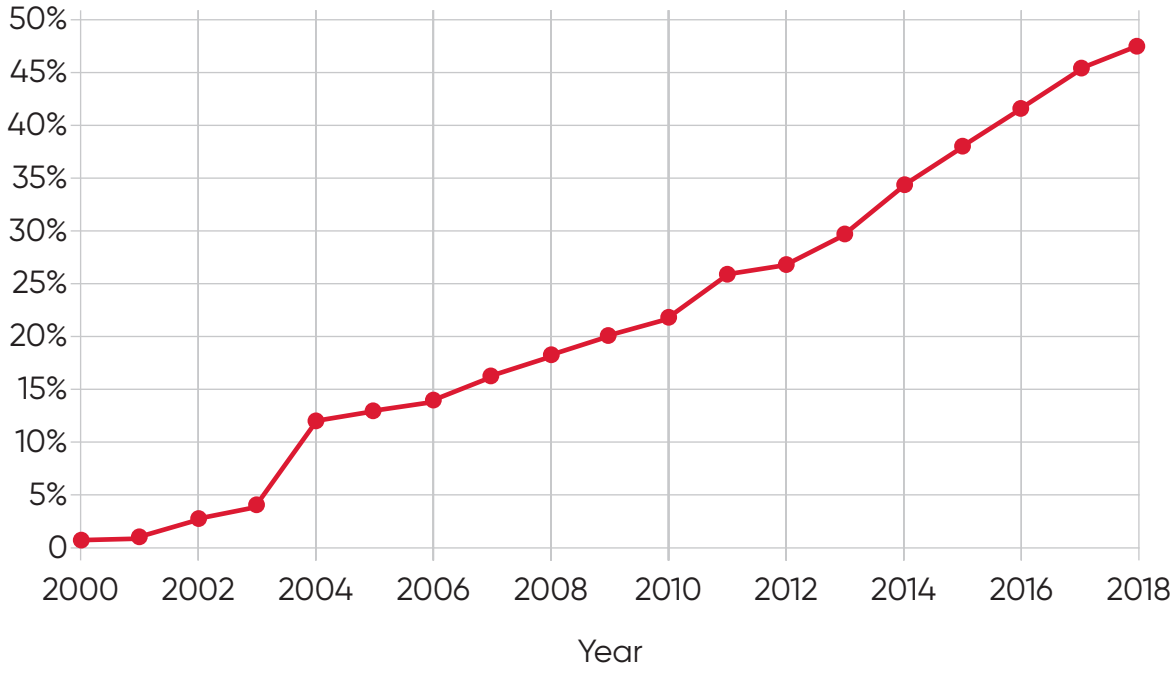
## 4.2 Using technology: background and practices

Prior to January 2011, Egypt witnessed an IT revolution. Egypt was classified as one of the emerging powers in IT regionally. The number of internet users rose from 450,000 at the end of 2000 to 20 million – mostly youths – by 2011 (Bakr 2016: 59) and reaching 29 million during 2011. Internet penetration increased from 0.83 per cent in 2000 to 25.6 per cent in 2011 (see Figure 4.2). By the end of 2019, there were 49,231,493 internet users and internet penetration had increased to 48.1 per cent (Internet World Stats 2020). According to a report for the BBC, 'Egypt was the primary market for BBC

 DOI: 10.19088/IDS.2021.014

Arabic online in 2010, through both its regular and mobile websites, with roughly 2 million page views per month' (SecDev 2011). The number of Facebook users increased from 4.2 million in 2010 to 9.4 million in 2011 (MCIT 2013). By the end of 2019, Egypt had reached 42,400,000 Facebook users (Internet World Stats 2020).

## Figure 4.2 Percentage of the population with internet access in Egypt




*Source:* Based on data from ITU (2020)

Social indicators – such as, but not limited to, rate of literacy, fixed mobile contracts and number of internet users – before 2011 showed that, 'Egyptians enjoyed the freedom to be exposed to the internet and express their views in the press, media, and blogs' (Bakr 2016: 60) with no evidence of internet filtering, despite Egypt being under emergency law and perennial restrictions on freedom of the press. The report for the BBC (SecDev 2011) emphasises that civic space was more open before 2011 than under the current political regime. However, levels of internet surveillance were also high under the Mubarak regime. Since August 2008, internet cafe customers have had to provide their names, email addresses and phone numbers before they can access the internet. But this has not necessarily translated to measures to close civic space. According to Freedom House (2014), the Egyptian government showed a relaxed attitude towards access to ICTs and did not

censor websites or use high-end technologies to block online discussions until 2010. Instead, the Mubarak regime mainly attempted to track members of terrorist groups: 'surveillance and control were targeted at specific individuals' (Hassanin 2014).

Internet and mobile application shutdowns continued after 2011. Some reports showed that in 2016:

> Internet shutdowns [were] frequent in heavily militarized areas of North Sinai and [were] claimed to be carried out to deter communications between insurgent groups in the area. In September 2016, one such shutdown lasted for eight hours before the services were restored. (Grewal 2016: 5)

Signal, a messaging app, was reportedly shut down for a week in December 2016. Media reports said the shutdown aimed to stifle political dissent (*ibid.*). In general, Egypt has not witnessed an entire internet shutdown similar to what happened during the 2011 uprising, but blocking of websites and media platforms are frequently reported.

In May 2017, there was a significant increase in the number of blocked websites: 496 sites were blocked; the blocking of websites has become a frequent phenomenon in Egypt (Paradigm Initiative 2019: 14). The further legitimisation of website censorship and blocking under the Egyptian Cybercrime Law issued in 2018 is evidence that internet censorship in Egypt has now become pervasive (AFTE and OONI 2018). The Egyptian government continues to refrain from clarifying its decision to block websites in spite of a guarantee in Article 68 of the Constitution that 'all information, data and official documents are the property of the people; disclosure of it from its various sources is a right guaranteed by the state' (Arab Republic of Egypt 2014).

The deterioration of the political and security situation since 2011, and the closing of civic space in Egypt have forced human rights and political activists to move their activities to online spaces, and increasingly use technology and social media to exercise their right to freedom of expression. The Cybercrime Law of 2018 legalised the targeting of journalists, human rights activists, bloggers or any persons accused of misusing social media to spread fake news. The above-mentioned legal framework is used to criminalise online activities and close the online civic space in Egypt. For example:

> In 2016, online journalists Amr Badr and Mahmoud Sakka were held in detention for attempting to overthrow the regime and incitement on social media while a news website photographer was jailed for 2 years. Hamdy Mokhtar, a photographer for an opposition news website was also

 DOI: 10.19088/IDS.2021.014

sentenced to 2 years imprisonment. Khaled Elbashy, the Chief Editor of Al Bedaiah online newspaper and board member of Egypt's Press Syndicate was detained on May 29, 2016, for 'disseminating false news and rumours' and 'sheltering criminals'. Egyptian authorities have also been accused of abusing the 2-step verification process for the surveillance of bloggers and shut down telephone and Internet services in the North Sinai region during the weekend of September 17, 2016.
(Paradigm Initiative Nigeria 2016: 13)

## Table 4.1 Technology regulation timeline

| Year | Shift | Implication |
|---|---|---|
| **2003** | Telecommunications Regulation Law | Legal basis for communications shutdown during the 2011 Egyptian uprising. |
| **2011** | Internet shutdown | Entire internet shut down in Egypt for first time. |
| **2014** | Establishment of Egyptian Supreme Cybersecurity Council | The council was formed of intelligence and military personnel, prioritising a military perspective over a human rights perspective. |
| **2018** | Cybercrime Law | Used to legalise blocking of websites and targeting of activists. |
| **2018** | Press and Media Regulation Law | The law gave the authorities the right to block online media platforms and target journalists. |

*Source:* Author's own.

 DOI: 10.19088/IDS.2021.014

# 5. Digital rights landscape

The roots of the current legal framework on digital rights in general can be found in the International Bill of Human Rights, especially the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. It is worth mentioning that Egypt is party to most of the international human rights instruments used as the initial basis for digital rights, such as the African Charter on Human and Peoples' Rights, the International Covenant on Civil and Political Rights, the Convention against Torture and Other Cruel Inhuman or Degrading Treatment or Punishment, the Convention on the Elimination of All Forms of Discrimination against Women, and the International Covenant on Economic, Social and Cultural Rights.

Article 31 of the Constitution stipulates that: 'The security of information space is an integral part of national economy and security. The state commits to taking the necessary measures to preserve it in the manner organized by law'. In the field of digital rights, which is one of the pillars of Internet governance, Article 57 stipulates that:

> Telegraph, postal, and electronic correspondence, telephone calls, and other forms of communication are inviolable, their confidentiality is guaranteed and they may only be confiscated, examined or monitored by causal judicial order, for a limited period of time, and in cases specified by the law. 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.

Article 65 adds that: 'Freedom of thought and opinion is guaranteed. All individuals have the right to express their opinion through speech, writing, imagery, or any other means of expression and publication'. Article 68 stipulates the right to access information, as well. It is prohibited to withhold information or intentionally give false information.

 DOI: 10.19088/IDS.2021.014

# 6. Digital rights in times of Covid-19

Egypt's government has dealt with Covid-19 as a national security issue. The government took restrictive legal measures to prevent information circulating about the outbreak of Covid-19 in Egypt (AFTE 2020b). Social media is surveilled by the government to track and ban any information about the number of infected people in the country that contradicts government information or data: 'The Egyptian authorities took a legal measures (*sic*) against the individuals who broadcasts (*sic*) fake news, statements, or rumors on Covid-19. Furthermore, the General Attorney stated that it would deal with such fake news and stories according to the Law' (*ibid.*). According to the Association of Freedom of Thought and Expression (AFTE):

> Most likely, the security services' move came within the framework of a broader plan or approach in order to prevent citizens from expressing their opinions regarding the policies of state institutions in the face of the Covid-19 pandemic, as the Corona issue – now open to include more activists and users of social media (*sic*).
> (*ibid.*: 5)

Many journalists and citizens have been prosecuted, interrogated and sentenced for criticising the government response to the Covid-19 crisis or citing numbers of infected people that contradict figures announced by the government, as well as people accused of spreading fake news and misinformation about the health situation (*ibid.*).

The Egyptian government's attempts to restrict digital rights during the Covid-19 pandemic are attributed to three main reasons, which have led to the majority of arrests of activists and users of social media: (1) criticising the Ministry of Health's policies in dealing with the Covid-19 pandemic; (2) spreading information about the presence of unannounced cases of Covid-19; and (3) requesting the release of prisoners for fear of spreading infection in prisons, in particular political prisoners and pre-trial detainees (*ibid.*).

In addition, in its report about how the Egyptian government dealt with the internet during the pandemic outbreak, AFTE emphasised that:

> the aim of arrest the activists and social media users is to restrict the public debate about Covid-19 and prevent the Egyptian citizens from using the only reaming (*sic*) means to interact with public affairs, which is using the Internet and Social Media to circulate information and express

 DOI: 10.19088/IDS.2021.014

> opinion on public policies In this regard, the Egyptian authorities use their security services, which surveillance (*sic*) the accounts of social media users. Furthermore Egypt has witnessed the banning of many websites that provided contents related to Covid-19 during the pandemic. (*ibid.*: 6)

## 6.1 Digital rights of vulnerable groups

Since it started, the Covid-19 pandemic has dramatically transformed most daily activities such as work, learning, communication and access to information that is only accessible through the internet. Therefore, access to the internet during Covid-19 is an essential issue, and governments are under an obligation to provide and secure affordable devices and access to the internet for vulnerable groups.

According to the United Nations High Commissioner for Refugees (UNHCR)-Egypt:

> The majority of refugees and asylum-seekers in Egypt were already highly vulnerable prior to the outbreak of COVID-19 and has been directly impacted by the evolving circumstances. Many have lost their source of income and cannot afford to buy sufficient basic supplies or pay their rent. (UNHCR-Egypt 2020)

According to Farahat (2020), obstacles that contribute to denying refugees their right to access the internet include their limited financial capacity, mainly because they cannot afford to buy appropriate equipment that has features to connect to the internet and operate the different applications and digital platforms used for e-learning and communication. In addition, lack of official recognition of refugee documents such as personal ID prevents them from registering with different internet service providers to have access to the internet or to purchase SIM cards under their own names, which means they are unable to access portable financial wallets, online cash payments and various other mobile financial services and smartphone applications.

In summary, digital rights for some vulnerable groups such as refugees have been ignored by UNHCR and the Egyptian government during the Covid-19 pandemic. So, the Egyptian government and UNHCR-Egypt have to work together to ensure refugees' – and, in particular, students' – access to the internet and other digital rights.

 DOI: 10.19088/IDS.2021.014

# 7. Conclusion and recommendations

There is a direct relationship between the political environment, civic space and digital rights. Digital rights could be described as human rights in '**virtual civic space**'. The political environment in Egypt has negatively affected civic space both offline and online. Social media technologies were used by civic activists in 2010 and 2011 to open civic space. The government has since used a range of technologies to close civic space, shutting it down, monitoring messages and manipulating discourse. Legislation has been used to mitigate the effectiveness of civil society institutions as well as individual activists.

The role of social media during the events of 2011 and afterwards encouraged the government to use new tools to monitor, control and surveil online activities and adopt very restrictive laws that deprive people of their rights to peaceful assembly and freedom of expression using the internet; also, the right to privacy has been affected by surveillance.

For reasons of counterterrorism and national security, civic space is restricted and seems closed. The new political environment does not seem like it will change in the near future. Moreover, parliament is upholding the trend of government and plays a negative role, particularly regarding laws linked to digital rights.

The above conclusion leads to the necessity to:

- Adopt advocacy campaigns at national, regional and international levels that call to change existing laws, producing policy papers and briefs related to digital rights. One of the strong points is that there are a lot of NGOs focused on human rights, but not specialised in digital rights. Capacity building for civil society on digital rights is urgently needed.
- Build the capacity of political party members and parliament on digital rights issues, to be able to change or adopt legislation in line with international human rights law – this is urgently required.
- Adopt 'strategic litigation' as a mechanism to change the government's policies that negatively affect civic space and digital rights.
- Design capacity-building programmes for lawyers, especially on strategic litigation, digital rights and using international human rights instruments before national courts.
- Raise the awareness of human rights activists and civil society about digital rights.
- Increase the number of organisations that focus on digital rights. This is essential: the shortage of organisations that work on digital rights and related issues creates a gap. Only a few organisations specialise in this field.

 DOI: 10.19088/IDS.2021.014

# References

AFTE (2020a) ***Freedom of Expression in the Time of Social Distancing Quarterly Report on the State of Freedom of Expression in Egypt (January–March 2020)***, Cairo: Association of Freedom of Thought and Expression (AFTE) (accessed 10 November 2020)

AFTE (2020b) ***The Pandemic Hasn't Stopped Repression: An Outlook on how the Egyptian State has Controlled the Internet under COVID-19***, Cairo: Association of Freedom of Thought and Expression (AFTE) (accessed 10 November 2020)

AFTE and OONI (2018) ***The State of Internet Censorship in Egypt***, Cairo: Association for Freedom of Thought and Expression (AFTE) and the Open Observatory of Network Interference (OONI)

ANND (2020) ***National Report About the Egyptian Civic Space***, Arab NGO Network for Development (ANND) (accessed 18 December 2020)

ANND (2019) *CIVIC Space in Arab Region, The Regional Report*, Arab NGO Network for Development (ANND)

Arab Republic of Egypt (2014) Constitution of the Arab Republic of Egypt (2014), Cairo: Government of Egypt

Arab Republic of Egypt (2013) 'The Statement of the General Command of the Armed Forces on 3 July 2013', *Official Gazette* issue (26) Bis (H) 3 July, Cairo: Government Egypt

Bakr, N. (2016) **'The Egyptian Revolution'**, in S. Calleya and M. Wohlfeld (eds), *Change and Opportunities in the Emerging Mediterranean*, Mediterranean Academy of Diplomatic Studies, University of Malta (accessed 18 December 2020)

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

CIVICUS (2020) **Monitor Tracking Civic Space: Egypt** (accessed 17 September2020)

Dube, H.; Simiyu, M.A. and Ilori, T. (2020) ***Civil Society in the Digital Age in Africa 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)

El Asouad, M. (2016) ***Right to Information and the National Security in Egypt***, Cairo: Association of Freedom of Thought and Expression (AFTE)

Farahat, M. (2020) ***Refugees' Digital Rights: The Vitality of the Right to Internet Access During the Covid-19 Pandemic***, Visto for Rights and Development, 14 June (accessed 10 November 2020)

Freedom House (2020) ***Freedom on the Net*** (accessed 4 December 2020)

Freedom House (2019) ***Freedom in the World*** (accessed 4 December 2020)

Freedom House (2014) ***Freedom on the Net 2014 – Egypt*** (accessed 4 December 2020)

Grewal, J. (2016) ***Internet Shutdowns in 2016***, The Centre for Internet and Society, India

Hassan, H.A. (2011) 'Civil Society in Egypt under the Mubarak Regime', *Afro Asian Journal of Social Sciences* 2.2.2

Hassanin, L. (2014) 'Egypt', in ***Global Information Society Watch 2014: Communications Surveillance in the Digital Age***, Association for Progressive Communications (APC) and Hivos

International Center for Not-For-Profit Law (ICNL) (2020) ***Egypt*** (accessed 10 November 2020)

Internet World Stats (2020) ***Internet Users Statistics for Africa*** (accessed 18 September 2020)

ITU (2020) ***Internet Access Statistics***, International Telecommunication Union (accessed 4 December 2020)

Ministry of Communication and Information Technology (MCIT) (2013) *The Future of the Internet Economy in Egypt. A Statistical Profile 2013*, Cairo: Government of Egypt

Paradigm Initiative (2020) ***Digital Rights in Africa Report 2019. Violations Reloaded: Government Overreach Persists Despite Increased Civil Society Advocacy***, Accra: Paradigm Initiative

Paradigm Initiative Nigeria (2016) *Digital Rights in Africa Report 2016. Choking The Pipe: How Governments Hurt Internet Freedom on a Continent that Needs More Access*, Lagos: Paradigm Initiative Nigeria

Rastegari, B. (2012) 'The Egypt's Revolution: Causes and Developments from Legal Perspective', Aceh Development International Conference 2012, 26–28 March, International Islamic University Malaysia

SecDev (2011) ***Censorship and Social Activism in the Middle East and North Africa: A Report for the BBC***, Ottawa: The SecDev Group

United Nations High Commissioner for Refugees (UNHCR) (2020) ***Egypt: Fact Sheet***, July

# Cameroon Digital Rights Landscape Report

Kathleen Ndongmo



This report is part of 'Digital Rights in Closing Civic Space: Lessons from Ten African Countries'; the Introduction is also recommended reading.

© 2021 Kathleen Ndongmo © Institute of Development Studies. DOI: 10.19088/IDS.2021.015

# 1. Introduction

Internet users in Cameroon face many challenges when it comes to accessing civic space, and particularly digital civic space – not least the notorious months-long internet shutdowns. Economic, social, cultural, and political factors all play a part in the landscape of the digital rights of this badly divided country. This report aims to briefly sketch the relevant political, civic, and technological landscape. It examines the various barriers to accessing digital civic space faced by journalists, minorities, and ordinary citizens, and identifies gaps in knowledge and capacity that must be addressed in order to allow the citizens of Cameroon to monitor their civic space and exercise their digital rights. The report suggests that some of the essential steps are securing internet access and educating citizens in identifying fake news, and concludes that internal security and international scrutiny are the necessary foundation for protecting civic space.

 DOI: 10.19088/IDS.2021.015

# 2. The political landscape

## 2.1 Background

Cameroon is a lower-middle-income country in West Africa with a population of around 25 million (World Bank 2019), comprising more than 200 ethnic groups (Tchouteu 2017). Around half of the population live in an urban setting (Benneh and DeLancey 2020). Economic development is held back by economic and political corruption: Cameroon scores only 25 out of 100 on the Corruption Perceptions Index, where 100 indicates the absence of corruption (Transparency International 2019). The country suffers from high unemployment as well as ongoing ethnic and regional tensions, which have escalated to the point of being almost a civil war – notably in the Northwest and Southwest regions of the country. Since 2008, it has consistently been rated in the 'alert' category for state fragility (Fund for Peace 2020).

Cameroon is divided into majority francophone (French-speaking) and minority anglophone (English-speaking) regions. Many anglophone Cameroonians feel sidelined by the francophone regime, which has led to protests and even separatist movements in recent years.

Cameroon is officially a democracy with universal suffrage, but the effectiveness of the democracy is undermined by an autocratic regime. Paul Biya has been president of Cameroon since the 1980s, and is entitled to appoint ministers, vice-ministers, and regional functionaries. He is also the head of the armed forces (Nations Encyclopedia 2020a). Although there has been a multi-party system since the 1990s, and despite major anti-Biya protests in 2008, Biya's party, the Cameroon People's Democratic Movement (CPDM), has retained power at every election.

Contested elections have been a recurring theme of Paul Biya's premiership. The CPDM has convincingly won every election since the introduction of democratic elections, but there have frequently been accusations of irregularities, fraud, and voter intimidation. In 2006, Elections Cameroon (ELECAM) was created as an independent body to monitor elections, although it did not begin work until 2010. The fact that 11 of its 12 members were members of the CPDM and appointed by the president made its true independence questionable (*Cameroon Today* n.d.).

Despite the oversight of ELECAM, there were accusations in the 2011 presidential election that the opposition had colluded with the government. At that point, all of the leaders of the opposition were still former members of the Cameroonian National Union, the party (headed by Biya) that ruled

 DOI: 10.19088/IDS.2021.015

Cameroon when it was a single-party state, until 1985 (Tchouteu 2017). Likewise, in the first senatorial elections in 2013, there were reports that the main opposition party, the Social Democratic Front (SDF), had cooperated with Biya for personal reward to ensure that the CPDM established control of the senate (*ibid.*).

Biometric voter registration was introduced in 2013 but allegations of serious electoral irregularities have not gone away (Reuters 2018). The president has abused his political power to remove restrictions to presidential terms and to ensure that the new senate was full of his supporters, avoiding genuine political scrutiny (Tchouteu 2017).

## 2.2 Recent political developments

Since 2016, there have been protests and political unrest in the anglophone regions, which led to these regions being badly underrepresented in the 2018 elections. Separatist groups have been involved in conflict with government forces, and both sides have been accused of atrocities against civilians (Human Rights Watch 2019).

Since the unrest began in 2016, separatists have imposed 'ghost town days' in the anglophone regions every Monday, when all social and economic activity is suppressed. 'Ghost town' protests were originally used in the 1990s as part of a strike by transportation workers, but the idea has been revived and imposed by threat of force. Separatist factions in the western (anglophone) regions of Cameroon seek to create the state of 'Ambazonia'. A symbolic Independence Day was celebrated in the anglophone regions in October 2018, which provoked a government backlash. However, separatist groups remain divided, reducing their effectiveness (Foute 2019b). Other activists in anglophone regions simply want more representation for English speakers within Cameroon. There was considerable unrest in 2016 when proposals were released for French to replace English in the education and judicial systems within the anglophone regions (Atabong 2016).

Paul Tasong, Economic Minister Delegate in charge of Planning, was appointed as National Coordinator of the Presidential Plan for the Reconstruction and Development of the Northwest and Southwest regions in April 2020. This ten-year plan aims to promote social cohesion, revitalise social infrastructure, and revive the economy of the region, but time will tell whether these measures will end the conflict in the area (Cameroon Tribune 2020).

 DOI: 10.19088/IDS.2021.015

# 3. The civic space landscape

The term 'civic space' refers to an open and democratic society. An open civic space allows citizens and civil society organisations to organise, participate, and communicate without hindrance. In doing so, they are able to claim their rights and influence the political and social structures around them. This can only happen when a state holds by its duty to protect its citizens, and respects and facilitates their fundamental rights to associate, assemble peacefully, and freely express views and opinions (see CIVICUS 2020). These rights are not available in Cameroon, with the country being classed as 'not free' every year since 1977 (Freedom House 2019, 2020; see Figure 3.1).

## Figure 3.1 Freedom House ranking for ADRN countries, 2000–19[1]


*Note:* ADRN – African Digital Rights Network.

*Source:* Adapted from Freedom House (2019)

Flashpoints over civic space have generally occurred around the time of elections, which are widely regarded as fraudulent and corrupt. Biometric voter registration was mandated in 2012 and rolled out from 2013, using German technology. The permanent biometric register of voters is now

1 Data not available for 2010 and 2012.

 DOI: 10.19088/IDS.2021.015

updated each year (Azonga 2014). Despite this attempt to regularise voting practices, suspicions and allegations of fraud and disenfranchisement still accompany elections in Cameroon.

Cameroon is a member of the United Nations (UN) and the African Union, and as such has ratified many UN human rights conventions such as the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (National Commissions for UNESCO of France and Germany 2010). However, in practice, Cameroon has been accused of many human rights abuses during the last 20 years, particularly since the beginning of the anglophone crisis in 2016. Accusations include unlawful or arbitrary killings, forced disappearances, torture, and arbitrary detention (US Bureau of Democracy, Human Rights and Labour 2019). Civic space is closed down by restrictions on political participation, peaceful assembly, and freedom of association, while the media is controlled by violence, threats, and unjustified arrests (*ibid.*).

## 3.1 The civic space and the media

Cameroon is currently ranked 134 out of 180 in the World Press Freedom Index (Reporters without Borders 2020). Much of its media is controlled by the state. While there are dozens of private newspapers, none of them is as regularly produced or as widely read as the government newspaper, the *Cameroon Tribune*. Cameroon's radio and TV network is controlled by the Office de Radiodiffusion–Télévision Camerounaise (CRTV), which is under the authority of the Ministry of Information and Culture (Nations Encyclopedia 2020b). The government is willing to use its power to shut down criticism or scrutiny by the private media. In 2008, Equinox TV was forcibly suspended. The reason given by the government was that it had failed to pay a broadcast licence fee, but it was generally believed that it was actually because of Equinox's coverage of the 2008 protests against the removal of limits on presidential terms.

Abuses against the media and journalists followed the contested 2018 election (CPJ 2020). In November 2018, Equinoxe presenter and prominent anglophone journalist, Mimi Mefo Takambou, was detained and charged with disseminating fake news, endangering state security, and terrorism (BBC Monitoring 2018). Then in 2019, pidgin journalist Samuel Wazizi died in military custody, allegedly from torture (CPJ 2020). In August 2019, the USA excluded Cameroon from a regional trade pact because of its human rights abuses (Ekonde and Adebayo 2019).

 DOI: 10.19088/IDS.2021.015

The latest example of intimidation of the media is the arrest in July 2020 of Ojong Joseph, a human rights reporter. On 14 February 2020, there was a massacre in Ngarbuh, a village in the anglophone Northwest region, allegedly by government troops. The government initially denied the massacre and denigrated international human rights observers, saying civilian deaths were an unfortunate accident during a clash with separatist terrorists. However, they later carried out an inquiry and arrested three soldiers for the outrage (Finnan 2020). This provides a glimmer of hope about Cameroon's future attitude both to civil rights and to disinformation.

## 3.2 The civic space and minorities

The key minority in Cameroon is the English-speaking population, who make up about 20 per cent of the country. The recent anglophone crisis was precipitated by the neglect of English as a medium, and the prioritising of French systems, in the anglophone education and judicial systems (Atabong 2016). Since the beginning of the crisis in 2016, it is estimated that 3,000 people have been killed and half a million have had to flee their homes (Human Rights Watch 2020b).

Both the government and anglophone separatists have been accused of violence, including sexual violence. This means that women and girls are especially vulnerable to being targeted in the conflict. In addition, the Cameroon government is poor at tackling crimes of violence against women (US Bureau of Democracy, Human Rights and Labour 2019). Girls are entitled to access education on the same basis as boys, but female literacy continues to lag behind that of males (UNESCO Institute of Statistics 2020). Women are also less likely to have access to the internet (Toussi 2019).

Same-sex sexual activity is against the law in Cameroon, and there is widespread discrimination against lesbian, gay, bisexual, and transgender (LGBT) people. The lack of legal protection from discrimination makes it harder for members of this community to access education, health care, and employment (Acodevo *et al.* 2017). The 2010 law on cybercrime and cyberterrorism explicitly criminalises using electronic communications to sexually proposition a member of the same sex, a prohibition that does not extend to opposite-sex propositions. Blackmail and extortion against people who have (or are perceived to have) a homosexual orientation are common, and there is very little redress. Organisations that support LGBT rights find it difficult to register in Cameroon, and lawyers who defend people accused of LGBT crimes can be subject to intimidation (*ibid.*).

 DOI: 10.19088/IDS.2021.015

All of these restrictions and difficulties mean that the severely limited civic space in Cameroon is even more limited for people other than heterosexual, francophone males.

## 3.3 The civic space timeline

The first major disturbance of the last 20 years in Cameroon began in February 2008. President Paul Biya proposed a constitutional amendment that would remove limits upon presidential terms, which would enable him to continue as president even though he had already held office for 25 years. The major opposition party organised a demonstration but the presence of *gendarmes* (military security forces) forced this to be called off. *Gendarmes* and police used tear gas and water cannons, but this only inflamed the situation, leading to the deaths of two young men. A TV channel that focused on the protests was shut down on a pretext (Global Security n.d.).

Protests continued in February 2008 over the death of the two youths, the extension of presidential terms, and worsening economic conditions, including high food prices. Rather than engaging with criticism, the government of Cameroon responded with high levels of violence, leaving at least 16 people dead (Global Security n.d.).

In 2010 and 2014, the government of Cameroon responded to new threats with new laws. The 2010 law on cybercrime and cyberterrorism was intended to stop the spread of harmful false information and the promotion of terrorism, but the terms of the law mean that it partly criminalises free speech online, as there are possible fines and jail terms for those who disseminate information that they cannot verify. Cameroon is troubled by genuine terrorists connected to Boko Haram and ISIS in Africa, but the law on terrorism that was passed in 2014 was later abused to hold journalists in detention. One problem with these laws is that the government of Cameroon may define 'terrorism' very differently from those posting content online – content that they believe to be legitimate criticism. This was illustrated in 2016 when there was a serious train derailment. Reports circulated on social media while the government was still officially denying knowledge of the accident, and later individual statements and videos of the accident on social media contradicted official government accounts about the cause and the number of casualties. The government of Cameroon and the state-run media reacted with strong criticism of social media use in general, with Cavaye Djibril, Speaker of the National Assembly, calling it a 'social malaise' and even 'a new form of terrorism' (Tande 2016).

 DOI: 10.19088/IDS.2021.015

The year 2017 was that of the long internet shutdowns, which were used as a tactic to shut down civic space, especially for anglophones. The first shutdown began in 2017 and lasted for 93 days. It seems to have been in response to anglophone protests about the sidelining of English in education and the justiciary. English and French officially have equal status in Cameroon, but in practice, French has priority and English is often neglected by the francophone regime (Atabong 2016). The first shutdown originally affected the whole of Cameroon but was later restricted to the anglophone regions. After international pressure from the UN, internet access was restored, but a further, longer shutdown followed in October 2017. Money transfers, online businesses, certain kinds of health care (e.g. coordinating malaria treatment), and education all relied on internet access. Tech entrepreneurs, without access to the internet, were forced to move to other parts of Cameroon or to leave the country (Ritzen 2018).

In 2018, Paul Biya won a seventh term as president in an election that was marred by low turnout, especially in anglophone regions, where intimidation of anglophone voters kept voter turnout in single figures (Reuters 2018). In an effort at public relations, CRTV featured an interview with a person claiming to be a Transparency International observer who said the elections were 'extremely good' (O'Donnell and Gramer 2018). This person was later exposed as a fraud with no links whatsoever to Transparency International (Transparency International 2018).

 DOI: 10.19088/IDS.2021.015

# Table 3.1 Civic space timeline table – key events

| Year | Shift | Implication |
|---|---|---|
| **2006** | ELECAM created to monitor elections, starts to function in 2010. | Shows government intention that elections be seen as free and fair, despite no actual improvement. |
| **2008** | Riots over food prices harshly suppressed. | Increasing government authoritarianism. |
| **2010** | New law on cybersecurity and cybercriminality. | Limits freedom of speech online. |
| **2011** | Paul Biya stands for re-election.<br>Mobile access to Twitter stopped for ten days because of protests. | The first major incident of internet censorship in Cameroon, demonstrates growing importance of online activism. |
| **2012–13** | Introduction of biometric voter registration. | Aimed at reducing electoral irregularities. |
| **2014** | Journalists arrested for defamation. | Chilling effect on freedom of the press. |
| **2015** | New law requires registration for all SIM card owners to target criminal and terrorist activity. | Increases government control over telecoms companies and citizens' access to communications. |
| **2016** | Journalists arrested for failing to disclose information and sources. | Restriction on press freedom. |
| **2017** | Anglophone journalists, opposition politicians, and civil society figures imprisoned. | Anglophone voices silenced, power reserved for francophone administration. |
| **2017** | Writer Patrice Nganang arrested after criticising government on Facebook. | Chilling effect on freedom of speech and online dialogue. |
| **2018** | Paul Biya re-elected in contested election. Abuses against media and journalists follow. | Criticism of the government and electoral process becomes more dangerous. |
| **2019** | Journalist Samuel Wazizi dies in military custody. | Chilling effect on freedom of the press. |
| **2019** | New law passed criminalising hate speech and tribalism. | Gives the government new powers over freedom of speech, can be used in partisan manner. |
| **2020** | Human rights reporter Ojong Joseph is arrested. | Sends a message about lack of respect for human rights. |

*Source:* Author's own.

 DOI: 10.19088/IDS.2021.015

# 4. The technology landscape

Although privately owned television stations have been allowed in Cameroon since 2001, the government still maintains a high degree of control over the media.

Fixed-line telephones are comparatively rare, but there is high uptake of mobile telephone services. In 2000, there were 95,000 landline telephones in use whereas in 2002 there were already 300,000 mobile phones in use (Nations Encyclopedia 2020b). The use of mobile phones has increased steadily over the last 20 years, especially as costs for fixed lines continue to be prohibitive. Recent data show that mobile phone penetration has reached 90 per cent of the population, or 23.6 million people.[2]

Fixed telephone lines are provided by the Cameroon Telecommunications Corp (CAMTEL), which is owned by the state. In 2020, there are four private mobile telecoms providers, but telecoms are still controlled by CAMTEL, the state-owned mobile provider that holds the monopoly of optical fibre management (African Telecoms News n.d.). CAMTEL can suspend the access of other internet providers, something that happened in October 2017, when Orange Cameroon's use of the networks was unlawfully suspended as the result of a payment dispute that Orange strongly denied, cutting off service for its users (Medou Badang 2017).

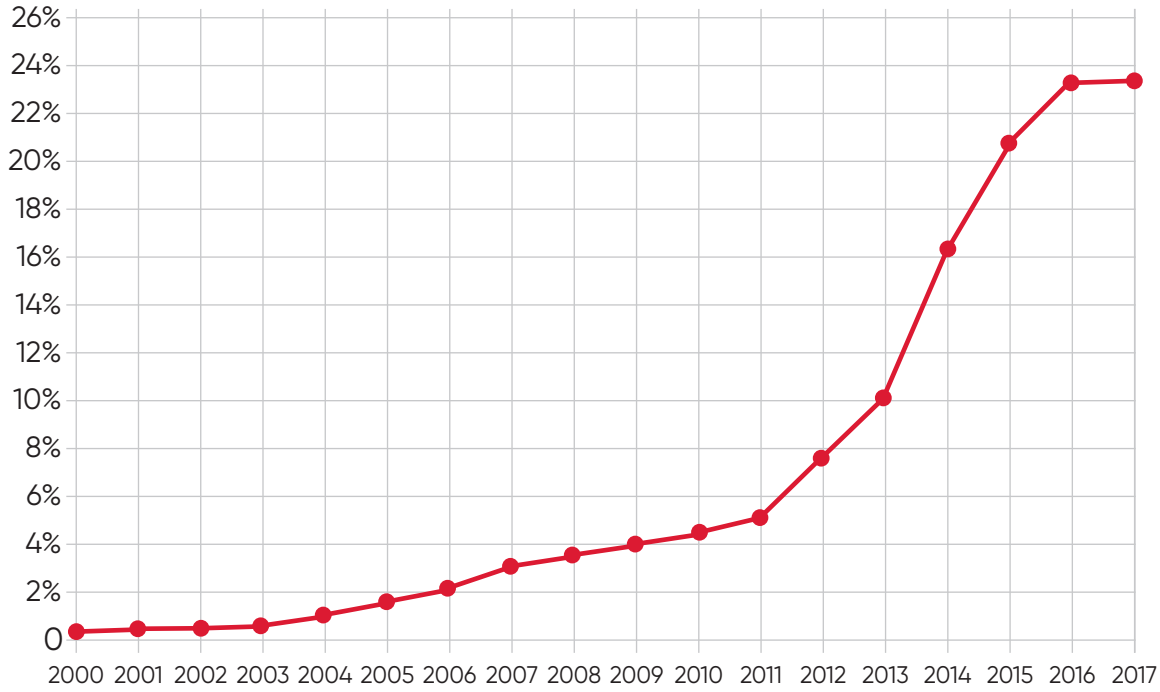
The introduction of 3G and 4G mobile internet took place in 2015–16. This allowed wider use of the internet, as people had previously had to rely on internet cafes. Unfortunately, lack of real competition between mobile providers has kept mobile internet expensive and therefore either inaccessible or severely limited for most people in the country (Owono and Blanc 2014). Neither mobile telephones nor fixed-line telephones are an affordable internet solution for most Cameroonians.

Internet penetration has grown hugely in Cameroon over the last 20 years, from 0.25 per cent in 2000 up to 23.1 per cent in 2020 (see Figure 4.1). However, this total remains low compared to the African average of 39.3 per cent and the world average of 58.8 per cent (Statista 2020). Internet services are notoriously slow in Cameroon, with bandwidths of 340 gigabytes in 2014, compared to 12 terabytes in nearby Ghana (Owono and Blanc 2014).

2 See **Mobile Connections in Cameroon**.

 DOI: 10.19088/IDS.2021.015

## Figure 4.1 Percentage of the population with internet access in Cameroon




*Source:* Based on data from ITU (2020)

In 2010, the government took its first major step in trying to control cyberspace. It passed a new law relating to cybersecurity and cybercriminality. While many countries have laws aimed at preventing online crime and terrorism, what was significant about this law was that users of social media could be punished with fines and imprisonment if they shared information that could not be verified:

> Whoever uses electronic communications or an information system to design, to publish or propagate a piece of information without being able to attest its veracity or prove that the said piece of information was true shall be punished with imprisonment for from 06 (six) months to 02 (two) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both of such fine and imprisonment.[3]

This naturally places ordinary citizens at a disadvantage, as they may be forced either to accept government accounts of events or to face legal punishments for disseminating information from other sources. This law also discriminates against LGBT people by criminalising 'sexual propositions to another person of the same sex' (Acodevo *et al.* 2017: 6).

Although the government set up a bilingual web portal as early as 2001, its use remains limited, partly due to citizens lacking access to the internet,

3 Section 78(1), Law n° 2010/012 of 21 December 2010 Relating to Cybersecurity and Cybercriminality in Cameroon.

 DOI: 10.19088/IDS.2021.015

and partly due to a failure of government to engage with the potential of the new medium. The train derailment incident in 2016 (see section 3.3) clearly demonstrated the government's distrust and suspicion of social media and instant internet communication.

This hostile attitude is also shown in the internet shutdowns that have been a notorious government tactic in Cameroon within the last five years. Despite difficulties of access due to high expense, the internet has been used in recent years for education, health care (e.g. access to malaria treatment), and for entrepreneurial, web-based businesses. Government shutdowns in 2017 into 2018 had a catastrophic effect on all web-based commerce and amenities, driving some entrepreneurs out of the country (Ritzen 2018). These shutdowns have often been contained to just the anglophone regions, highlighting their political nature. The justification given by the government for shutdowns (when one is offered) is to prevent the dissemination of misleading and harmful information. The government has also 'throttled' internet access at times by deliberately reducing bandwidth. Sometimes this throttling is targeted, as with the slowdown of social media before the announcement of the 2018 election results (Netblocks 2018).

There is also evidence that the Cameroon state engages in surveillance of emails and social media, although this is not highly developed, given Cameroon's low level of internet usage (APC and Hivos 2014).

Despite a low level of Twitter use, hashtag campaigns have been used to express discontent about the political and economic situation in Cameroon, and to garner international attention (Nganji and Cockburn 2020). This method was used successfully in 2017 with the #BringBackOurInternet hashtag. The prominent whistle-blower Edward Snowdon **tweeted his support**. International attention may have contributed to the decision of the Cameroon government to restore internet access. However, it did not stop them from imposing a second, even longer shutdown after the protests in the anglophone regions following a symbolic anglophone 'Independence Day' on 1 October 2017.

The Cameroonian diaspora helped with the #BringBackOurInternet campaign. Emigrants often use web-based technology to take part in the civic space of Cameroon, using platforms such as Facebook, Twitter, and WhatsApp (Okwuosa 2017). Their internet access tends to be much better, especially when they are living in Western countries such as Germany or the USA, but government restrictions on internet access within Cameroon have the power to limit the effectiveness of diaspora interventions, if the resident population cannot receive communications.

The government imposed higher transfer charges on wire transfer agencies such as MoneyGram and Western Union in January 2019. Later in 2019, there were allegations that funds transfers to anglophone regions of the country were being deliberately blocked (Mimi Mefo Info 2019). During the Covid-19 pandemic, they also requested telecoms companies to shut down

 DOI: 10.19088/IDS.2021.015

electronic money transfers to a relief fund for needy families because it was coordinated by the opposition party Cameroon Resistance Movement (CRM) (Paradigm Initiative 2020).

## Table 4.1 Technology timeline table

| Year | Shift | Implication |
|---|---|---|
| **2001** | E-government web portal set up: Services du Premier Ministre | Groundwork for e-governance and open government data |
| **2010** | Universal Telecom Service Law | Opens phone and internet access to badly-served regions, increasing civic space |
| **2010** | Cybercrime and Cybersecurity Law | Fines and imprisonment for anyone unable to prove the veracity of online posts |
| **2011** | Mobile access to Twitter blocked for ten days because of protests | Demonstrates that online protest was impacting government |
| **2013** | Compulsory biometric ID | To address election irregularities |
| **2014** | Third mobile phone provider introduced | Potential for service improvement through competition (not realised yet) |
| **2015** | Mandatory SIM registration | Reduces privacy. Aids surveillance |
| **2015–16** | Introduction of 3G and 4G | Open access to online info and communications |
| **2016** | Digital Cameroon strategic plan launched | Positive intention to increase digital access, but this did not last |
| **2016** | #AnglophoneCrisis campaign goes viral internationally | Opens international space to issues and puts pressure on government |
| **2017** | Two major internet shutdowns:<br>1st: 93 days, whole country<br>2nd: 250 days, anglophone region only | Dramatic closing of civic space and increase in government control |
| **2017** | Use of VPNs to evade shutdowns | Keeps space open for those able to afford access to VPN software |
| **2017** | #bringbackourinternet campaign gains international traction | External pressure forces reopening of online civic space |
| **2018** | Throttling of bandwidth to slow social media before announcement of election results | Closes space for citizen voices in commentary on events |
| **2019** | Tax imposed on international app downloads | Expense restricts access and creates class divide in digital access |
| **2019** | Higher transfer charges imposed on wire transfer agencies | Restricts financial options of Cameroonians |
| **2020** | Government requests shutdown of opposition fundraising for pandemic relief<br>#BringBackOurRice hashtag started | Citizens attempt to hold government accountable |

*Source:* Author's own.

 DOI: 10.19088/IDS.2021.015

# 5. The digital rights landscape

Digital proficiency in Cameroon is still at a low level. Citizens face particular challenges to using the internet in general, and to effectively using it as a medium of civic space. The government launched a *Strategic Plan for a Digital Cameroon by 2020* in 2016 which aimed to improve infrastructure and increase cybersecurity and digital literacy, but these laudable aims were undermined by shutting off the internet the following year (Digital Cameroon 2016).

The high cost of internet on both mobiles and landlines leaves many Cameroonians unable to access the internet. Cameroon has lower internet penetration than average for Africa, at 23.1 per cent. Only 10.2 per cent of citizens have a Facebook account (Statista 2020). This problem is compounded by the limitations of the electricity network, which does not extend to most rural areas (Ndongsok and Ruppel 2018).

The state has strong control over both telecoms and the media which it uses to the disadvantage of its citizens, for example by bandwidth throttling, internet shutdowns, and sanctioning private telecoms providers and TV channels. These tactics are particularly focused on anglophone regions. Digital advances in Cameroon have usually been located in these regions (for example at 'Silicon Mountain' in Buea) so this antipathy to anglophone culture holds the whole of Cameroon back digitally (Atabong 2019).

There are major restrictions on free speech online. Laws on terrorism and cybercrime make it a serious offence to share information that the sharer cannot prove to be true, which places a high burden on netizens. Using electronic communications for same-sex relationships is also illegal.

Cameroon is one of several African countries implicated in recent Russian disinformation campaigns, apparently recruiting local people with genuine social media accounts (Ilyushina 2019). It is too early to know what the effects will be on Cameroonian online civic space, but it seems unlikely that the Cameroonian government has the technical knowledge to deal with this new and sophisticated threat, given its acknowledged weaknesses in the area of ICT (Digital Cameroon 2016).

Cybersecurity remains poor for institutions and individual users in Cameroon. The country scored only 0.432 (out of 1) in the latest Global Cybersecurity Index (ITU 2018).

The government of Cameroon clearly views digital space as more of a threat than an opportunity, which is in line with its authoritarian view on civil rights in general, particularly in relation to minorities. The government deliberately restricts citizens' access to the internet, as well as carrying out surveillance

 DOI: 10.19088/IDS.2021.015

of social media. A lack of transparency means that, as yet, not very much is known about where the government is sourcing its surveillance technology from, although CAMTEL's telecommunications equipment is sourced from its principal Chinese partners (APC and Hivos 2014). In 2019, Cameroon's government launched a video-surveillance command centre built and implemented by Chinese technology company Huawei. The centre runs off Huawei equipment and provides connectivity for the transmission of footage (itweb.africa 2019).

Despite these difficulties, Cameroonians who are active online, and Cameroonian emigrants, have made use of social media to challenge the status quo and hold the government to account, using Twitter hashtags such as #BringBackOurInternet and #KeepItOn (#KeepItOn 2018) to highlight internet outages, and #anglophonecrisis to report the ongoing tensions and violence in the anglophone regions. Some net-savvy citizens have been able to maintain their internet access using virtual private networks (VPNs) but these are expensive and must be downloaded before shutdowns occur in order to be effective.

Deliberate disinformation is a new threat that is not yet fully understood, by the government or by citizens. Social media, and Facebook in particular, have been a means of spreading 'fake news', hate speech, and inflammatory posts, worsening the situation between separatist or federalist anglophones and the francophone regime, security services, and supporters (McAllister 2018). The government has responded by passing a law criminalising hate speech, with higher penalties for hate speech spread via media (#defyhatenow 2020), but they fail to implement this consistently. Human rights lawyer, Felix Agbor Balla, said: 'The problem with government is that they politicise it – they use it when it is convenient for them. When people use [hate speech] against people who are against the government – nobody cares' (Ekonde 2020).

The Cameroon government itself has recently made use of a number of USA-based PR companies in an attempt to garner political support for the regime in Washington, but they do not appear to be targeting citizens within Cameroon so far (Foute 2019a). In 2018, it also tried to persuade Facebook to remove anti-government 'fake news' even when that news had been verified by international organisations such as Amnesty International (Atabong 2018).

In this environment, citizens need education in assessing and using information that is disseminated online in order to judge its veracity, and education about what constitutes hate speech. Facebook has so far failed in its duty of care in this area, but government censorship is not a viable alternative.

 DOI: 10.19088/IDS.2021.015

# 6. Digital rights during Covid-19

Cameroon is the country in central Africa that has been worst affected by Covid-19, despite implementing typical restrictions on freedom of movement and association such as prohibiting gatherings of more than 50 people, encouraging e-meetings, and closing ports and airports to passengers (Republic of Cameroon Prime Minister's Office 2020). Whether any extra restrictions on liberty will continue once the pandemic is over remains to be seen.

The government's handling of the crisis has been marred by a double scandal. In June, Human Rights Watch called on Cameroon's government to disclose why funds for tackling the virus had not been released from the Health Solidarity Fund. Since 1993, public primary care facilities have been obliged to pay 10 per cent of their monthly revenues to the fund (Human Rights Watch 2020a). Then in July 2020, human rights groups warned that the US$40m solidarity fund raised by civilians had been embezzled, including 4,000 bags of rice that were illegally sold (Kindzeka 2020). Citizens placed pressure upon the government by starting a Twitter campaign using the hashtag **#BringBackOurRice**, along the lines of #BringBackOurInternet. The government initially denied all allegations but has since ordered an investigation.

The effect of the pandemic on digital rights has been mixed. CAMTEL, Orange, and MTN have all offered reduced prices for internet data to help people stay connected during lockdown, keeping online space open. On the other hand, personal data are under threat, with information being shared online about people who arrived in the country and were suspected of having the virus. The government also abused its power to try to get telecoms companies to block payments to a relief fund coordinated by an opposition party (Paradigm Initiative 2020).

Tracking and tracing infection is likely to be an important part in the next phase of controlling the virus. So far, the Cameroon government has not implemented any form of digital track-and-trace, relying instead on public awareness messages. However, should the government start collecting data about citizens for virus control purposes, the level of corruption in Cameroon means that there is a danger it would be retained after the crisis passes and/or used for other purposes, to the detriment of its citizens.

 DOI: 10.19088/IDS.2021.015

# 7. Conclusion

The major challenges to both civic space and digital rights in Cameroon come from the autocratic government's tight grip on discourse, both online and in the press. International observers have noted major infractions of freedom of speech, freedom of association, and the freedom of the press, despite Cameroon being a signatory of many human rights treaties. Abuses against ordinary citizens, and especially against writers and journalists, create an environment where using electronic or traditional media to voice dissenting opinions can come with a high cost. It is not reasonable to expect people to risk their freedom or their lives to enter civic space in Cameroon. Therefore, international pressure on the Cameroonian government to deal with its record of human rights abuses is essential to digital rights in Cameroon. The government has softened its stance lately, launching investigations into both abuses by soldiers and embezzlement of funds. This may be an indication that it is prepared to take action to be welcomed back into the international fold.

Lack of access to the internet is also a huge problem for Cameroonians when it comes to exercising their digital rights. Again, the root of the problem is government control. Although the Cameroon government does not have a monopoly on telecoms, its high level of control over all providers restricts meaningful competition that might bring down prices. The government has failed miserably to achieve the aspirations in its 2016 *Strategic Plan for a Digital Cameroon by 2020* (Digital Cameroon 2016) and has in fact taken backwards steps by bandwidth throttling and shutdowns. National and international pressure must be placed upon the government to prioritise citizens' access to fast, affordable internet. In 2020, this is an essential requirement for taking part in civic space and being part of the international community. Better use of digital resources could also be an advantage to the functioning of the government, if it could manage to see the internet as not merely a threat but also an opportunity.

For netizens in Cameroon, current priorities are education about, and access to, VPNs. These are essential to circumvent government shutdowns of the internet or of particular web-based services such as Twitter and WhatsApp. Cameroonians who are online should be encouraged to select and download a VPN before any shutdown occurs, so that they can continue to occupy the civic space and draw international attention to the situation. VPNs can be expensive to use (although often free to download) so it would be useful to develop an affordable VPN targeted at netizens of countries at risk from shutdowns.

 DOI: 10.19088/IDS.2021.015

Disinformation or 'fake news' has become a serious problem worldwide in recent years, particularly from malicious state actors. While there is as yet no evidence that the Cameroon government is targeting its citizens in this way, the fact that Cameroonian social media users have been implicated in Russian disinformation campaigns is a signal that Cameroonian citizens, and all netizens, need to be educated about this threat: what it is, how to spot it, what to do about it. Often the solution is as simple as checking the source of a news item or article via a basic online search. However, as 'fake news' becomes more complex, education from experts in this field will be more valuable. Attempts to get the social networks themselves to stem the problem have failed, so education on the ground will be essential, ideally both by digital means (to reach a digitally active audience) and also through in-school education, to reach the upcoming generation of internet users.

All of these suggestions would be valuable for Cameroon, but the uncomfortable truth is that not much progress is likely to be made while the anglophone crisis rages on. Efforts to build capacity within civic society, whether the educational or the private sector, are too precarious in what is effectively a one-party state with the ability, and the will, to shut off internet access overnight. With a highly corrupt government that is paranoid about terrorism, real and imagined, and prepared to use draconian laws against not only hostile militants but also impartial journalists, the civic space will not be a safe place for Cameroonians, and especially not for anglophones during the current crisis. Therefore, urgent diplomatic action is needed to bring about an end to the conflict and restore relations within Cameroon. Establishing internal security is the essential foundation for building an effective, accessible civic space in Cameroon.

 DOI: 10.19088/IDS.2021.015

# References

Acodevo *et al.* (2017) ***The Violations of the Rights of Lesbian, Gay, Bisexual, and Transgender (LGBT) Individuals in Cameroon*** (accessed 4 August 2020)

African Telecoms News (n.d.) Cameroon Mobile and Fixed Network Operators List

APC and Hivos (2014) ***Global Information Society Watch 2014: Communications Surveillance in the Digital Age***, Johannesburg and The Hague: Association for Progressive Communications and Humanist Institute for Cooperation with Developing Countries (accessed 7 August 2020)

Atabong, A.B. (2019) **'Cameroon's Plan for a Francophone-Led Tech Hub isn't Being Welcomed in its Anglophone Region'**, *Quartz Africa*, 23 January (accessed 7 August 2020)

Atabong, A.B. (2018) **'Cameroon Has Been Asking Facebook for Help with Fake News Ahead of a Contentious Election'**, *Quartz Africa*, 14 September (accessed 29 August 2020)

Atabong, A.B. (2016) **'Mass Protests in Cameroon are Exposing the Fragility of its Dual French-English System'**, *Quartz Africa*, 24 November (accessed 7 August 2020)

Azonga, T. (2014) **'Biometric Voting in Cameroon'**, *CamerounWeb*, 16 October (accessed 8 August 2020)

BBC Monitoring (2018) **'Name in the News: Equinoxe TV, Cameroon's Activist Television Channel'**, 9 November (accessed 6 August 2020)

Benneh, G. and DeLancey, M.W. (2020) **'Cameroon'**, *Encyclopædia Britannica* online (accessed 31 July 2020)

Cameroon Today (n.d.) ***Elections Cameroon, ELECAM: An Overview of the Cameroon's Election Body*** (accessed 7 August 2020)

*Cameroon Tribune* (2020) **'Cameroon: NW/SW Reconstruction, Development: Paul Tasong Wants All Hands On Deck'**, *allAfrica*, 30 June (accessed 28 August 2020)

CIVICUS (2020) ***Civic Space*** (accessed 23 October 2020)

CPJ (2020) **'Samuel Wazizi'**, *Committee to Protect Journalists* (accessed 7 August 2020)

#defyhatenow (2020) **'Social Media and Conflict'**, in *Field Guide Cameroon 2020* (accessed 10 August 2020)

Digital Cameroon (2016) ***Strategic Plan for a Digital Cameroon by 2020*** (accessed 28 August 2020)

Ekonde, D. (2020) **'Cameroon's 3-Year Separatist Crisis: Online Threats, Attacks on Identity and Freedom of Expression'**, *Global Voices Advox*, 18 May (accessed 10 August 2020)

Ekonde, D. and Adebayo, B. (2019) **'US Removes Cameroon From Trade Pact Over Alleged "Persistent" Human Rights Violations'**, *CNN*, 1 November (accessed 10 August 2020)

Finnan, D. (2020) **'Cameroon Government Makes U-Turn on Anglophone Massacre in Ngarbuh'**, *Radio France Internationale*, 22 April (accessed 7 August 2020)

Foute, F. (2019a) **'Anglophone Crisis in Cameroon: The Lobbyists' War Rages in Washington'**, *The Africa Report*, 5 August (accessed 28 August 2020)

Foute, F. (2019b) **'Cameroon: Anglophone Secessionists Split on Swiss Mediation'**, *The Africa Report*, 15 July (accessed 6 August 2020)

Freedom House (2020) ***Country and Territory Ratings and Statuses FIW 1973–2020*** (accessed 28 August 2020)

Freedom House (2019) ***Freedom in the World*** (accessed 4 December 2020)

Fund for Peace (2020) ***Fragile States Index 2019*** (accessed 29 October 2020)

Global Security (n.d.) ***Cameroon: 2004 Election*** (accessed 6 August 2020)

Human Rights Watch (2020a) **'Cameroon: Investigate, Distribute Health Fund'**, 12 June (accessed 7 August 2020)

 DOI: 10.19088/IDS.2021.015

Human Rights Watch (2020b) ***Cameroon: Events of 2019*** (accessed 10 August 2020)

Human Rights Watch (2019) ***Cameroon: Events of 2018*** (accessed 8 August 2020)

Ilyushina, M. (2019) **'Russia's "Troll Factory" is Alive and Well in Africa'**, *CNN*, 1 November (accessed 7 August 2020)

ITU (2020) ***Internet Access Statistics***, International Telecommunication Union (accessed 4 December 2020)

ITU (2018) ***Global Cybersecurity Index (GCI) 2018***, Geneva: International Telecommunication Union Publications (accessed 29 August 2020)

Itweb.Africa (2019) **'Cameroon Unveils Huawei-Built Video Surveillance Centre'**, *itweb.Africa*, 26 August (accessed 11 November 2020)

#KeepItOn (2018) ***The State of Internet Shutdowns Around the World: The 2018 #KeepItOn Report*** (accessed 5 August 2020)

Kindzeda, M.E. (2020) **'Cameroon Citizens Raised $40M for COVID Relief, But Where is It?'**, *VOA News*, 27 July (accessed 29 October 2020)

McAllister, E. (2018) **'Facebook's Cameroon Problem: Stop Online Hate Stoking Conflict'**, *Reuters*, 5 November (accessed 10 August 2020)

Medou Badang, E. (2017) **'Announcement: Customer's Best Interests First'**, *Orange*, 18 October (accessed 10 August 2020)

Mimi Mefo Info (2019) ***Diaspora: Problems of Money Transfer to Anglophones Regions***, 15 April (accessed 6 August 2020)

National Commissions for UNESCO of France and Germany (2010) ***Claiming Human Rights: Cameroon*** (accessed 7 August 2020)

Nations Encyclopedia (2020a) ***Cameroon: Government*** (accessed 4 August 2020)

Nations Encyclopedia (2020b) ***Cameroon: Media*** (accessed 5 August 2020)

Ndongsok, D. and Ruppel, O. (2018) 'The State of Electricity Production and Distribution in Cameroon', in O. Ruppel and E. Yogo (eds), *Environmental Law and Policy in Cameroon: Towards Making Africa the Tree of Life*, Baden-Baden: Nomos Verlagsgesellschaft

Netblocks (2018) **'Facebook and WhatsApp Restricted in Cameroon on Eve of Election Results'**, 21 October (accessed 29 August 2020)

Nganji, J.T. and Cockburn, L. (2020) **'Use of Twitter in the Cameroon Anglophone Crisis'**, *Behaviour & Information Technology* 39.3: 267–87 (accessed 6 August 2020)

O'Donnell, J. and Gramer, R. (2018) **'Cameroon's Paul Biya Gives a Master Class in Fake Democracy'**, *Foreign Policy*, 22 October (accessed 23 October 2020)

Okwuosa, A. (2017) **'The Diaspora Groups in American Suburbia Backing a Breakaway African Nation'**, *Quartz Africa*, 7 November (accessed 6 August 2020)

Owono, J. and Blanc, F. (2014) ***Internet and Broadband in Cameroon: Barriers to Affordable Access***, Washington DC: Alliance for Affordable Internet (accessed 8 August 2020)

Paradigm Initiative (2020) **'Digital Rights: How Francophone Africa is Bracing for COVID-19's Impact?'**, 2 June (accessed 10 August 2020)

Reporters without Borders (2020) ***2020 World Press Freedom Index*** (accessed 29 October 2020)

Republic of Cameroon Prime Minister's Office (2020) ***Government Response Strategy to the Coronavirus Pandemic (Covid-19)*** (accessed 5 August 2020)

Reuters (2018) **'Cameroon Court Hears Calls for "Irregular" Election to be Annulled'**, 16 October (accessed 23 October 2020)

Ritzen, Y. (2018) **'Cameroon Internet Shutdowns Cost Anglophones Millions'**, *Al Jazeera News*, 26 January (accessed 7 August 2020)

Statista (2020) ***Percentage of Population Using the Internet in Cameroon from 2000 to 2017*** (accessed 5 August 2020)

Tande, D. (2016) **'Cameroonian Government Launches Campaign Against Social Media, Calls It "A New Form of Terrorism" '**, *Global Voices*, 16 November (accessed 6 August 2020)

Tchouteu, J. (2017) *Cameroon: The Haunted Heart of Africa*, New York NY: Tisi Books

Toussi, S. (2019) **'Overview of Cameroon's Digital Landscape'**, CIPESA, 12 September (accessed 29 August 2020)

Transparency International (2019) ***Corruption Perceptions Index*** (accessed 28 August 2020)

Transparency International (2018) **'International Election Observers in Cameroon are Not Affiliated with Transparency International'**, 9 October (accessed 7 August 2020)

UNESCO Institute of Statistics (2020) ***Cameroon*** (accessed 6 August 2020)

US Bureau of Democracy, Human Rights and Labour (2019) **'Cameroon'**, in *Country Reports on Human Rights Practices for 2019* (accessed 7 August 2020)

World Bank (2019) ***Cameroon Country Overview*** (accessed 4 August 2020)

 DOI: 10.19088/IDS.2021.015

institute of development studies

Delivering world-class research, learning and teaching that transforms the knowledge, action and leadership needed for more equitable and sustainable development globally.

Institute of Development Studies
Library Road
Brighton, BN1 9RE
United Kingdom
+44 (0)1273 606261
**ids.ac.uk**

Charity Registration Number 306371
Charitable Company Number 877338