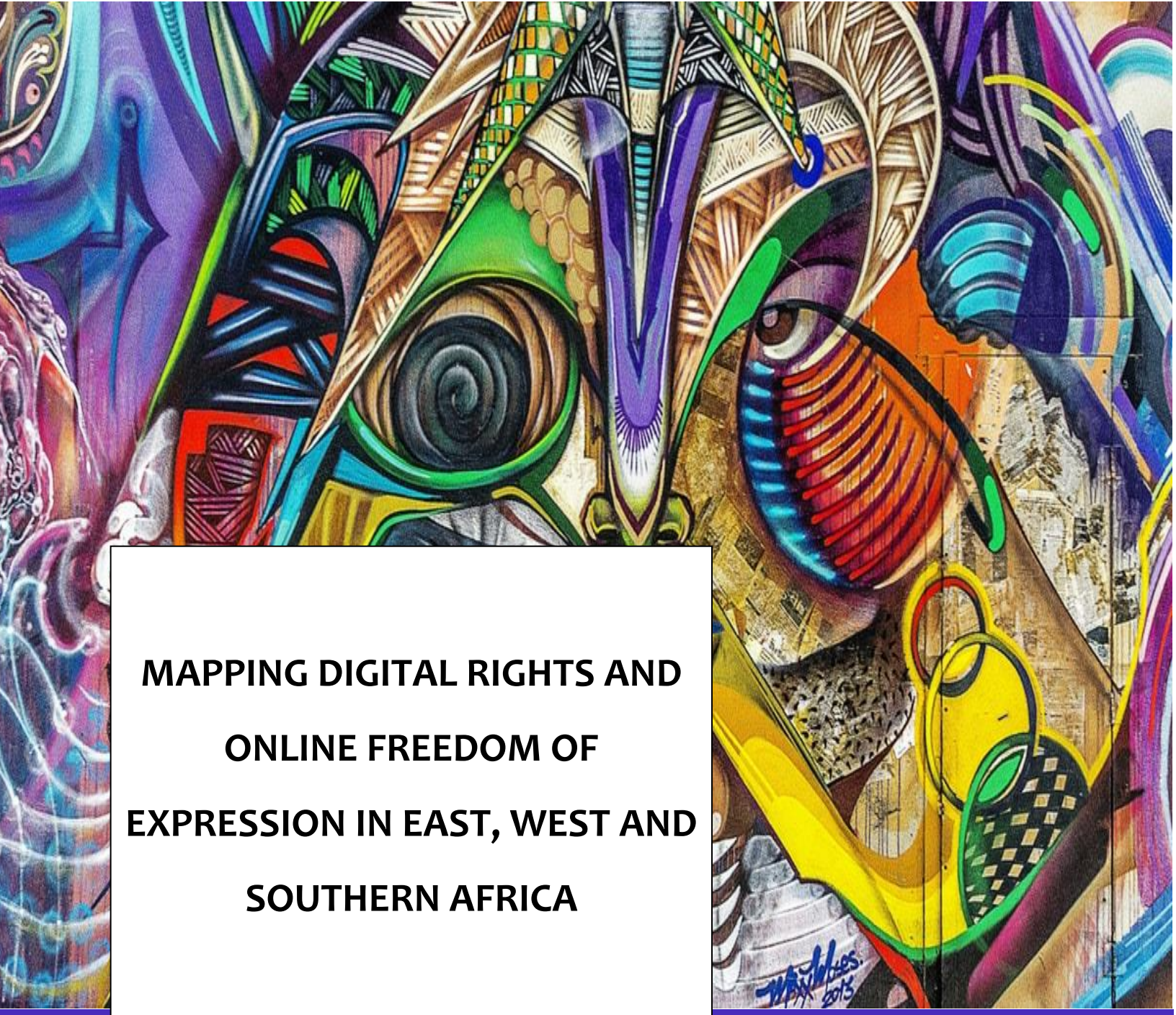

MAPPING DIGITAL RIGHTS AND ONLINE FREEDOM OF EXPRESSION IN EAST, WEST AND SOUTHERN AFRICA

MLDI
Media Legal Defence Initiative

Published by the Media Legal Defence Initiative

•••

2018

www.mediadefence.org

Published by the Media Legal Defence Initiative
https://www.mediadefence.org/

This report was prepared with the assistance of ALT Advisory
https://altadvisory.africa/

TABLE OF CONTENTS

LIST OF ACRONYMS

ACHPR	African Commission on Human and Peoples' Rights
ACRWC	African Charter on the Rights and Welfare of the Child
AFEX	African Freedom of Expression Exchange
APC	Association for Progressive Communications
AU	African Union
CIPESA	Collaboration on International ICT Policy in East and Southern Africa
CSO	Civil society organisation
EAC	East African Community
EACJ	East African Court of Justice
ECOWAS	Economic Community of West African States
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communication technology
IFEX	International Freedom of Expression Exchange
IP	Internet protocol
ISP	Internet service provider
ITU	International Telecommunications Union
MLDI	Media Legal Defence Initiative
MNO	Mobile network operator
NGO	Non-governmental organisation
REC	Regional economic community
SADC	Southern African Development Community
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
VoIP	Voice-over-IP
VPN	Virtual private network

INTRODUCTION

Overview of this report

The right to receive, seek and impart information is well-entrenched under international law – through, for instance, the UDHR, the ICCPR and the African Charter on Human and Peoples' Rights (African Charter) – as well in many domestic laws across the continent. However, the reality on the ground in achieving the realisation of the right gives rise to concern.

The internet has enabled an expansion of civic space and a fuller enjoyment of fundamental rights, although this has not necessarily been welcome in all states. Unfortunately, for many people across the region, access remains a serious challenge. Indeed, internet penetration in Africa is low compared to other continents. According to 2017 ITU data, only 21.8% of African residents have used the internet, compared to 43.7% in the Arab States, 43.9% in the Asia/Pacific region, 65.9% in the Americas, and 79.6% in Europe.[1]

For those who do have access, this access does not come without challenges and restrictions. There are currently various laws and policies in different countries across the region that have been proposed or have been adopted that seek to regulate the internet, and directly encroach – or have the potential to encroach – on the exercise of the right to freedom of expression online. Some countries have also seen a crackdown on human rights defenders and journalists who challenge the state authorities through the institution of criminal and other legal proceedings against them.

While many states appear to see the value of the internet for economic development and education, this is accompanied by a lack of trust in the internet and the concerns for the mobilising power that this can afford to individuals and groups.

In response, civil society organisations and members of the media across the region have taken a firm stand in the face of these challenges. Concerted efforts at policy reform and strategic litigation have served as a bastion into the erosion of the right to freedom of expression. The regional and sub-regional courts have also become an important fora for seeking accountability against African states that unjustifiably infringe the right to freedom of expression.

This report maps the current landscape in respect of digital rights and online freedom of expression in East, West and Southern Africa. It looks at the trends regarding law and policy developments, as well as recent litigation, within these regions. The report focuses on 18 countries – 6 per region – and tracks the recent developments that have taken place in these countries.

[1] Research ICT Africa, 'Policy brief 6: SADC not bridging digital divide', 8 September 2017, accessible at https://researchictafrica.net/polbrf/Research_ICT_Africa_Policy_Briefs/2017_Policy_Brief_6_SADC.pdf.

Part I of the report provides an overview of the litigation before the ACHPR and the African Court on Human and Peoples' Rights (African Court) in respect of freedom of expression. **Parts II, III and IV** of the report look at the trends generally in East, West and Southern Africa respectively, as well as some of the key legal and civil society actors working on digital rights and online freedom of expression, and include a snapshot of some of the notable developments – both positive and negative – that have occurred in the 18 countries under consideration in this report, as well as reflections on opportunities and challenges for vindicating digital rights within each of the countries. Lastly, **Part V** considers what the next possible opportunities will be for digital rights and online freedom of expression litigation in the region.

Defining digital rights

It is by now firmly established by both the ACHPR and the UN that the same rights that people have offline must also be protected online, in particular the right to freedom of expression.[2] Article 19(2) of the ICCPR makes clear that the right to freedom of expression applies regardless of frontiers, through any media of one's choice.

For the purposes of this report, we use the term "digital rights" to refer broadly to human rights in the digital era, and the rights that are implicated in the access and use of the internet and other ICTs. This comprises a wide range of distinct but interrelated topics. As set out below, while this report does not purport to cover the full ambit of digital rights, it seeks to focus on some of the most pertinent trends and developments seen across the region.

In broad terms, some of the key topics explored in this report within the ambit of digital rights and freedom of expression online include digital access, online content regulation, privacy and surveillance, media freedom, the spread of so-called 'fake news' and disinformation on social media platforms, and taxes imposed on access to the internet and platforms. Some countries have also had other noteworthy developments that are unique to the country, and where considered relevant these developments have been included as well.

Approach and methodology

In terms of the temporal scope, the report primarily focuses on developments during the two year period between mid-2016 to mid-2018, although certain of the key laws and policies pre-date this period, and have been included to provide a more holistic picture. We are also cognisant that rapid developments have taken place in some countries between the end of that period and the date of publication. The selection of countries in the report has been informed by various factors. Firstly, it represents a geographic spread, with six countries being selected from each of the sub-regions under consideration. Regard was also had to the social and political influence of the countries, and the role they play in

[2] UN Human Rights Council, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', 27 June 2016, accessible at https://www.article19.org/data/files/Internet_Statement_Adopted.pdf; ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', 4 November 2016, accessible at http://www.achpr.org/sessions/59th/resolutions/362/.

swaying policy development in other countries on the continent. Furthermore, a key consideration was the recent trends in the countries, including new or proposed laws and policies, recent or ongoing litigation, and ICT-infrastructure development, levels of access to the internet and the prevalence of use of ICTs and social media that would likely impact on digital rights.

The availability of country-specific information was another important factor, and related to this, the existence of civil society, media and other organisations that are active in the country and have documented developments. We also took into account countries in which we have previously worked. Finally, we also had regard to where ongoing or future work in respect of digital rights would be likely to achieve positive outcomes. Importantly, we recognise that every country in the region has a unique context that presents its own opportunities and challenges, and although it was not possible for present purposes to map all the countries, we recognise the important and much-needed work that is being undertaken in respect of freedom of expression and digital rights across the continent, including those that fall beyond the scope of this report.

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

A further source of information has been through questionnaires sent to legal and civil society organisations working in the region. A copy of the questionnaire has been included as an appendix at the end of this report, and sought input from the respondents on their work on digital rights, the current context, and their views on the opportunities and challenges in the region. The questionnaire was sent to legal, media and civil society organisations that we are aware of working across all three sub-regions, and 12 responses were received. Of these, 11 were received as completed questionnaires, with the remaining one done via a telephone call. We are deeply grateful for the input received from the respondents acknowledged below. In terms of the methodology for future iterations of this report, we will continue to strive to include as many respondents' views as possible in order to understand the situational positioning from a diverse range of viewpoints.

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

We are also cognisant of certain limitations to this report. Local context is always an important factor. As such, while we have drawn on the experience of various role-players – including MLDI's own experience and that of our partner organisations – and sought to place reliance on credible sources and the reports of actors working on digital rights directly in the countries under consideration, this report does not purport to present a first-hand account of the in-country situation in the 18 selected countries.

We also note that up-to-date information regarding laws, policies and court decisions are not readily accessible in respect of all countries, in which case secondary sources provide the only available information. Furthermore, the process of information-gathering is also made better and more accessible in countries where there are a number of active civil society organisations, strong press freedom and high levels of access to the internet and ICTs, which in turn result in a greater exercise of freedom of expression. The converse is that information-gathering is significantly more challenging in respect of those counties that are currently under repressive regimes, lack judicial independence and accountable state institutions, or where the barriers to accessing the internet and ICTs inhibit the availability of content online.

Lastly, we note that while we have endeavoured to ensure the accuracy of the content contained in the report at the time of publication for the period under consideration, the field of digital rights is dynamic and constantly evolving with new laws, judicial pronouncements and other developments occurring frequently. Changes in leadership, legislative changes and other developments occur rapidly, and can drastically affect the landscape at any time. As mentioned above, it is intended that this report will ultimately form part of a series, with these changes reflected in future editions covering that particular time period.

Acknowledgements

MLDI would like to thank the following individuals and organisations for providing their input that has assisted in the development of this report:

- Association for Progressive Communications, *Anriette Esterhuysen (Senior Advisor)*
- fesmedia, *Sekoetlane Phamodi (Programme Coordinator)*
- Gambian Press Union, *Bai Emil Touray (President)*
- Kenya Union of Journalists, *Erick Uduor (Secretary-General)*
- Legal Resources Centre, *Tsangadzaome Mukumba (Researcher)*
- Media Foundation for West Africa, *Vivian Affoah (Senior Programme Officer: Freedom of Expression)*
- Media Monitoring Africa, *William Bird (Director)*
- PEN Nigeria, *Folu Agoi (President)*
- Protège QV, *Avis Momeni (Secretary-General)*
- Research ICT Africa, *Anri van der Spuy (Manager: Africa Digital Policy Project)*
- Right2Know, *Murray Hunter (Secrecy Organiser)*
- Southern Africa Litigation Centre, *Kaajal Ramjathan-Keogh (Executive Director)*

We note that the respondents have consented to being acknowledged in this report. As indicated above, 11 of the 12 respondents provided their responses through submitted questionnaires, with one having been conducted via a telephonic discussion.

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

PART I: AFRICAN REGIONAL HUMAN RIGHTS MECHANISMS

The AU is the overarching regional body across the African continent, with a vision of "an integrated, prosperous and peaceful Africa, driven by its own citizens and representing a dynamic force in the global arena". As set out in Article 3 of the Constitutive Act of the AU, the objectives of the AU include, among others, to promote and protect human and peoples' rights in accordance with the African Charter and other relevant human rights instruments; to promote democratic principles and institutions, popular participation and good governance; and to promote peace, security and stability on the continent.

The African Charter is the primary human rights instrument in the region. The right to freedom of expression is contained in Article 9 thereof, and provides as follows:

> "(1) Every individual shall have the right to receive information.
> (2) Every individual shall have the right to express and disseminate his opinions within the law."

Notably, it is not the only legal instrument that contains protections for information rights. The ACRWC, for instance, provides express protections for the rights of freedom of expression and privacy of children. In this regard, Article 7 of the ACRWC provides that: "Every child who is capable of communicating his or her own views shall be assured the rights to express his opinions freely in all matters and to disseminate his opinions subject to such restrictions as are prescribed by laws"; and Article 10 provides that: "No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks".

At a policy level, the AU has also had developed policies and guidelines that have an impact on digital rights. This has focused primarily on data protection and cybersecurity, most notably through the 2014 AU Convention on Cyber Security and Personal Data Protection[3] and the 2018 Personal Data Protection Guidelines.[4]

The ACHPR is the primary human rights organ of the AU. Established in terms of Article 30 of the African Charter and inaugurated in November 1987, it is charged with the functions of protecting and promoting human and peoples' rights, and interpreting the African Charter. It has contributed to the protection and promotion of the right to freedom of expression in several important ways. Firstly, the ACHPR is a quasi-judicial body, empowered to make recommendations to states on receipt of a complaint. Through this function, the ACHPR has provided important guidance on the interpretation of the right to freedom of expression.

[3] Accessible at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

[4] Accessible at https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/.

For instance, in *Media Rights Agenda / Nigeria*, the ACHPR made clear that the reference to "within the law" in Article 9(2) of the African Charter must be interpreted as referring to "within international law", explaining that to do otherwise would "defeat the purpose of the rights and freedoms enshrined in the Charter", and that "international human rights standards must always prevail over contrary national law".[5] Through this ruling, the ACHPR made clear that states could not rely on their domestic laws to justify non-compliance with their international obligations in respect of freedom of expression under Article 9 of the African Charter.

Another important function served by the ACHPR is through its monitoring of states' compliance with the African Charter. In this regard, states are required to submit periodic reports to the ACHPR, with national human rights institutions and civil society organisations also able to provide input to the ACHPR in respect of the sate review. Representatives of the state party are also required to make oral representations to the ACHPR and respond to questions posed.

The ACHPR has made important recommendations to states parties regarding freedom of expression, including digital rights. For instance, in respect of South Africa, the ACHPR recommended as follows:[6]

> "The [ACHPR] recommends that South Africa should:
> (i) accelerate the enactment of the Protection of State Information Bill and ensure that the Bill is in line with regional and international standards;
> (ii) expedite the establishment of the Information Regulator;
> (iii) amend the Cybercrimes and Cybersecurity Bill in line with international best practices on access to information; and
> (iv) accelerate the enactment of the Judicial Matters Amendment Bill decriminalizing the common law crime of defamation."

In a similar vein, the ACHPR made the following recommendations to Kenya regarding freedom of expression and access to information:

> "Kenya should:
> (i) decriminalize defamation by repealing relevant provisions in the Penal Code;
> (ii) expedite the finalization and enactment of the draft Freedom of Information Bill; and
> (iii) take appropriate measures to effectively guarantee the right to freedom of expression, in particular for journalists and human rights defenders."

[5] Media Rights Agenda / Nigeria, Application No. 224/98, accessible at http://www.achpr.org/communications/decision/224.98/.

[6] ACHPR, 'Concluding observations and recommendations on the combined second periodic report under the African Charter on Human and Peoples' Rights and the Initial Report under the Protocol to the African Charter on the Rights of Women in Africa of the Republic of South Africa', 9-18 June 2016, accessible at http://www.achpr.org/files/sessions/20th-eo/conc-obs/2nd-2003-2014/co_combined_2nd_periodic_republic_of_south_africa.pdf.

These recommendations can be important advocacy tools domestically, particularly as the state should be required in subsequent reports to indicate whether there has been compliance with the previous recommendations.

The third important role that the ACHPR has played is in the development of soft law instruments regarding freedom of expression. The 2002 Declaration of Principles on Freedom of Expression in Africa[7] has been seminal in the development of the right to freedom of expression across the region. Other guidelines, such as the Guidelines on Freedom of Association and Assembly in Africa[8] and the Guidelines on Access to Information and Elections in Africa,[9] have also served to further the interpretation and understanding of the right, and to facilitate an understanding by states and other actors of how the right to freedom of expression should be applied in a manner that complies with international norms and standards. Notably, the Guidelines on Access to Information and Elections in Africa in particular have sought to grapple with the application of rights online, and includes provisions in respect of internet regulatory bodies (paragraphs 25 to 28) and the online media platform providers (paragraph 29).

The ACHPR's Special Rapporteur on Freedom of Expression and Access to Information has been a key role-player in furthering the right to freedom of expression, both online and offline. In addition to leading the development of these instruments, proposing resolutions and undertaking fact-finding missions, the Special Rapporteur has been particularly active in recent months in publishing statements on current affairs that are of topical importance. For instance, in July 2018 the Special Rapporteur issued a press release on the acquittal of journalists in Angola on charges of insult and defamation,[10] and in August 2018 issued press releases on the trend of attacks on journalists in Uganda[11] and on the high fees imposed by decree on journalists and media outlets in Mozambique.[12] These statements, which are quick and responsive in nature, serve to put pressure on states and guide state-action on matters that impact the enjoyment of freedom of expression.

The ACHPR Special Rapporteur on Freedom of Expression and Access to Information has also worked with other special procedure mechanisms from regional and international bodies on matters directly relevant to digital rights. This has included, for instance, the Joint Declaration on Freedom of Expression, 'Fake News', Disinformation and Propaganda, published jointly by the special rapporteurs from the ACHPR, UN, the Organization for Security and Co-operation in Europe and the Organization of American States.[13] The ACHPR Special Rapporteur on Freedom of Expression and Access to Information is currently engaged in an important project, supported by CSOs from around the continent,

[7] Accessible at http://hrlibrary.umn.edu/achpr/expressionfreedomdec.html.

[8] Accessible at http://www.achpr.org/files/instruments/freedom-association-assembly/guidelines_on_freedom_of_association_and_assembly_in_africa_eng.pdf.

[9] Accessible at http://www.achpr.org/files/instruments/freedom-association-assembly/guidelines_on_freedom_of_association_and_assembly_in_africa_eng.pdf.

[10] Accessible at http://www.achpr.org/press/2018/07/d415/.

[11] Accessible at http://www.achpr.org/press/2018/08/d417/.

[12] Accessible at http://www.achpr.org/press/2018/08/d420/.

[13] Accessible at https://www.osce.org/fom/302796.

to update the 2002 Declaration of Principles on Freedom of Expression in Africa, which are expected to include a section on digital rights in the updated version.

The African Court, too, has a crucial role to play as the highest decision-making body in the region. Article 2 of the Protocol to the African Charter on Human and Peoples' Rights on the Establishment of the African Court on Human and Peoples' Rights[14] (African Court Protocol) provides that the African Court shall complement the protective mandate of the African Commission. Judgments of the African Court are binding on the states against whom the judgment is delivered.

The African Court has, to date, delivered two landmark decisions in respect of freedom of expression. In *Zongo v Burkina Faso*,[15] a case involving the murder of members of the media in Burkina Faso, the African Court found that Burkina Faso had violated Articles 1 and 7 of the African Charter by failing to act with due diligence in seeking, trying and judging the assassins of Norbert Zongo and his companions, and therefore had violated the rights of the applicants to be heard by competent national courts. The African Court also held that Burkina Faso had violated Article 9 of the African Charter protecting freedom of expression because of its failure in the investigation and prosecution of the murderers of Norbert Zongo, which caused fear and worry in media circles.

Thereafter, in *Konaté v Burkina Faso*,[16] a case involving the conviction of a journalist on a charge of criminal defamation, the African Court held that aspects of criminal defamation laws, particularly those imposing the sanction of imprisonment, violated Article 9 of the African Charter and other international human rights provisions recognising the right to freedom of expression. *Konaté* has been particularly influential in other countries in the region, having been cited and followed in domestic court decisions regarding challenges to the offence of criminal defamation.[17]

Through its judgments, the African Court has been willing to order, for instance, that the respondent state amend impugned legislation to make it compliant with Article 9 of the African Charter and other international law instruments; that reparations be paid, including for moral damage suffered; and that the state be required to report to the African Court on the status of implementation of the judgment.[18]

While there is potentially an even more significant role that the African Court can play – particularly given its power to hand down binding judgments – a limitation with the jurisdiction of the African Court is that, as set in Article 5(3) of the African Court Protocol, individuals and NGOs can only approach the

[14] Accessible at http://www.achpr.org/instruments/court-establishment/.

[15] Zongo v Burkina Faso, Application No. 013/2011, accessible at: http://en.african-court.org/images/Cases/Ruling%20on%20Reparation/Application%20No%20013-2011%20-%20Beneficiaries%20of%20late%20Norbert%20%20Zongo-Ruling%20on%20Reparation.PDF.

[16] Konaté v Burkina Faso, Application No. 004/2013, accessible at http://en.african-court.org/index.php/55-finalised-cases-details/857-app-no-004-2013-lohe-issa-konate-v-burkina-faso-details.

[17] See, for instance, Misa-Zimbabwe et al v Minister of Justice et al, Case No. CCZ/07/15, accessible at https://globalfreedomofexpression.columbia.edu/cases/misa-zimbabwe-et-al-v-minister-justice-et-al/; Okuta v Attorney-General, Petition No. 397 of 2016, accessible at: https://globalfreedomofexpression.columbia.edu/cases/okuta-v-attorney-general/.

[18] See, for instance, Konaté v Burkina Faso: Judgment on reparations, Application No. 004/2013, accessible at http://en.african-court.org/images/Cases/Judgment/Konate%20Judgement%20on%20Reparation%20(English).pdf.

African Court directly if the affected state party has made a declaration in terms of Article 34(6) of the African Court Protocol recognising such jurisdiction of the African Court. In 2016, Rwanda withdrew its declaration; as such, at the time of writing, the applicable states are Benin, Burkina Faso, Côte d'Ivoire, Ghana, Malawi, Mali, Tanzania, The Gambia and Tunisia.

Despite the different limitations experienced by the ACHPR and the African Court, both have generally been receptive fora for litigants seeking to vindicate the right to freedom of expression, and have played important roles in developing jurisprudence on the right that have furthered its enjoyment. Although the decisions delivered thus far have been more focused on traditional forms of offline media, they undoubtedly have important positive implications for freedom of expression online as well. However, the next frontier for freedom of expression litigation before the ACHPR and the African Court will be digital rights. In a positive development, in August 2018, the African Court and UNESCO signed a memorandum of understanding to formalise their cooperation to promote freedom of expression and freedom of the press, including online.[19] Both the ACHPR and the African Court are well-poised to assist litigants to respond to the challenges being faced and inculcate a rights-based approach to laws and practices impacting freedom of expression online.

[19] UNESCO, 'UNESCO and African Court on Human and Peoples' Rights agree to strengthen their cooperation', 16 August 2018, accessible at https://en.unesco.org/news/unesco-and-african-court-human-and-people-s-rights-agree-strengthen-their-cooperation.

PART II: EAST AFRICA

Selected Countries:
Burundi • Ethiopia • Kenya • Rwanda •Tanzania • Uganda

Overview and background

There have been a number of concerning trends in East Africa in recent years. Certain key countries, such as Tanzania and Uganda, have seen a serious crackdown on the media and civil society, with a number of instances of threats, harassment and new laws that severely curtail the enjoyment of the right to freedom of expression. One trend of particular concern has been in respect of new tax and licensing rules for social media. In this regard, during the course of 2018, the national parliament of Uganda passed a law imposing a tax on the use of social media platforms; Tanzania and Kenya issued rules that require bloggers and other content producers to obtain a licence before posting their content on online platforms; and Zambia, Rwanda and the Democratic Republic of Congo are discussing similar proposals.[20]

There appears to be a clear trend of key influential states influencing the laws and policies of other states in the region. The countries selected below represent a cross-section both of those influencing trends and those following suit.

At the sub-regional level, the EAC has also had sought to play a policy role, although this does not appear to have influenced policy in the REC in a significant way. A notable development was the 2008 Draft EAC Legal Framework for Cyberlaws,[21] prepared by the EAC Taskforce on Cyberlaws with the support of UNCTAD. However, data protection and privacy rights are only dealt with briefly, and only identifies the following minimum obligations for the lawful processing of personal information:

> "To comply with certain 'principles of good practice' in respect of their processing activities, including accountability, transparency, fair and lawful processing, processing limitation, data accuracy and data security;
> To supply the individual with a copy of any personal data being held and processed and provide an opportunity for incorrect data to be amended."

[20] ARTICLE19, 'Eastern Africa: New tax and licensing rules for social media threaten freedom of expression', 26 June 2018.

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

Although coordinated policy development on digital rights at the sub-regional level has not been significant, the EACJ as the sub-regional judicial authority in East Africa has played an important role in safeguarding fundamental rights, including the right to freedom of expression. The EACJ is one of the organs of the EAC, and is established under Article 9 of the Treaty for the Establishment of the East African Community (EAC Treaty). Following the revival of the EAC in November 1999, the EACJ replaced the defunct East African Court of Appeal, and became operational in November 2001. The seat of the EACJ is currently in Arusha, although this remains the temporary seat until the permanent seat is decided.

Unlike the other regional and sub-regional courts, the EACJ does not have express human rights jurisdiction. However, in *Burundi Journalists' Union v The Attorney General of the Republic of Burundi*, the EACJ accepted that it had jurisdiction to hear cases relating to freedom of expression and the press as this links to principles of accountability, democracy and good governance that the member states are obliged to uphold.[22]

The EACJ is developing an important body of jurisprudence upholding the right to freedom of expression. In June 2018, for instance the EACJ declared that an order issued by the by the Tanzanian Minister for Information, Culture, Arts and Sports restricted freedom of expression and press freedom, and thereby constituted a violation of the respondent's obligation under the EAC Treaty to uphold and protect the principles of democracy, rule of law, accountability, transparency and good governance.[23] The order stated that: "The newspaper title 'MSETO' shall cease publication including any electronic communication as per the Electronic and Postal Communications Act for the duration of thirty-six months with effect from 10 August, 2016." The EACJ concluded in its ruling that the Minister's order contained "obvious unreasonable, unlawful and disproportionate anomalies", and ordered the Minister to annul the order and allow the applicants to resume publication.

As with the other regional and sub-regional fora, the EACJ has not yet had cause to deal directly with digital rights and freedom of expression online. However, the EACJ has thus far been a receptive forum for freedom of expression litigation generally, and there is therefore no reason to think that this will not continue to be the case in respect of digital rights litigation going forward. One aspect to note regarding the EACJ, however, is that it applies a strict time bar for the lodging of cases, and does not recognise the concept of continuing violations.[24] As such, prospective litigants must ensure that cases are filed timeously within the prescribed time period.

There are a number of well-established and effective legal and civil society organisations working on digital rights and freedom of expression online in East Africa. For litigation specifically, some of the key organisations in the sub-region that have developed experience in these issues include ARTICLE 19:

[22] Burundi Journalists' Union v The Attorney General of the Republic of Burundi, Reference No. 7 of 2013, para 15, accessible at: http://eacj.org/?cases=burundi-journalists-union-vs-the-attorney-general-of-the-republic-of-burundi.

[23] Accessible at https://www.mediadefence.org/news/east-african-court-overturns-tanzania%E2%80%99s-newspaper-ban.

[24] Attorney General of Uganda and Another v Awadh and Others, Appeal No. 2 of 2012, para 31, accessible at http://eacj.org/?cases=omar-awadh-and-6-others-vs-attorney-general-of-uganda); Attorney General of Kenya v Independent Medical Legal Unit, Appeal No. 1 of 2011, accessible at http://eacj.org/?cases=attorney-general-of-the-republic-of-kenya-vs-independent-medical-legal-unit-arising-from-appeal.

East Africa, the Kenya Human Rights Commission in Kenya and Unwanted Witness in Uganda. These organisations have played a pivotal role in developing the digital rights landscape through the courts in East Africa.

Country snapshot

(i) Burundi

The right to freedom of expression is guaranteed in Article 31 of the Constitution of Burundi. However, despite this protection, Burundi has experienced a number of challenges to the full enjoyment of the right to freedom of expression. This is seen both at the hands of the stand and through online users. With regard to the latter, as noted in a 2017 report:[25]

> "Burundi is grappling with hate speech, amidst widespread violence, torture and disappearances and restrictions of liberties. Facebook posts and comments, some using pseudonyms others by people apparently using their real names, have been reported to routinely contain blatant incitement to violence. In the run-up to the June 2015 election, hate speech was used as a key tool to whip up support in a campaign marred by harassment, intimidation and violence. During the period, the use of words such as "zirye" meaning "to eat"; "kumesa" meaning "kill him" or "to wash"; "inyezi zirye" meaning "eat the insects"; "savoner" meaning "cleaned up"; and "gukorerako" meanings include to beat, punish and even kill, in statements online and offline, continued to provoke, incite and stir tension in the country."

Law No. 100/97 on Electronic Telecommunications is a key law governing the ICT sector. It imposes a number of obligations on ISPs. For instance, Article 30 provides that operators of electronic communications are fully responsible for fighting fraud on their domains.

Law No. 1/15 on Regulating the Media has given rise to particular concern. In terms of Article 1, it covers all types of communications, including on the internet. Although an improvement in some respects on its predecessor,[26] there are still a number of concerning provisions. For instance, Article 18 obliges journalists to refrain from publishing any information that infringes on national unity, order and public safety, morality and good morals, honour and human dignity, national sovereignty, privacy and presumption of innocence; and Article 19 provides that the National Communication Council has powers to refuse to accredit or withdraw journalists' accreditation.[27] Although Article 16 provides for the protection of journalistic sources, this is at odds with Article 250 of the Penal Code that empowers a court to compel journalists to reveal their sources.[28]

[25] CIPESA, 'State of internet freedom in Africa 2017', September 2017, p 17.

[26] CIPESA, 'State of internet freedom in Burundi 2016', December 2016, accessible at https://cipesa.org/?wpfb_dl=230.

[27] ARTICLE 19, CIPESA, the East Africa Law Society, Pan African Lawyers Union & East and Horn of Africa Human Rights Defenders Project, 'Joint submission to the Universal Periodic Review of Burundi', 29 June 2017, accessible at https://www.article19.org/data/files/medialibrary/38816/Joint-submission-to-the-Universal-Periodic-Review-of-Burundi-by-ARTICLE-19-and-others.pdf.

[28] ARTICLE 19, CIPESA, the East Africa Law Society, Pan African Lawyers Union & East and Horn of Africa Human Rights Defenders Project, n 27.

SIM card registration has become a mandatory requirement since 2015, in terms of which personal information, such as names and addresses, have to be supplied.[29] Article 3 of Burundi's Ministerial Law No 540/356 of 2016 obliges mobile operators to "take all the necessary measures" to verify if the SIM card users are the real subscribers, and if they detect an anomaly, to block the SIM card. In terms of Article 1, possession of two SIM cards from the same telecommunications provider is prohibited, and any person who requires a dual SIM card must seek authorisation. In terms of article 29 of the Decree Law 100/97 of 2014, telecommunications companies in Burundi are liable to a fine of BIF 5,000,000 for every unregistered SIM card in use. Article 29 further provides that in addition to registering subscribers, service providers also have an obligation to disclose those details to the regulator upon request. In addition to the freedom of expression concerns, it has also given rise to privacy concerns regarding the data that is being collected and stored through SIM card registration, and the ability of authorities to access that information.[30]

The most recent law to raise concern is Law No. 1/09 of 11 May 2018, which amended the Code of Criminal Procedure, 2013, and was assented to by the president on 11 May 2018.[31] Articles 47, 69, 70, 71 and 72 grant wide-ranging powers to government agencies and the prosecution authorities to order the interception of communications and instruct ISPs to install any device to facilitate interception. The view has been expressed that this law is in contravention of the Constitution, and "clearly a wish to legalise the illegal and arbitrary practices that the forces of law and order have already resorted to for the last three years".[32]

According to reports, Burundian civil society actors – particularly human rights defenders and journalists – have been the primary targets of systematic oppression by authorities, and face heightened risks of threats, intimidation and violent attacks.[33] Most recently, in August 2018, a Burundian activist was reportedly jailed for five years accused of preparing reports on human rights abuses for a banned organisation.[34] Furthermore, it was reported in October 2016 that over 100 journalists fled Burundi since

[29] ARTICLE 19, CIPESA, the East Africa Law Society, Pan African Lawyers Union & East and Horn of Africa Human Rights Defenders Project, n 27.

[30] ARTICLE 19, CIPESA, the East Africa Law Society, Pan African Lawyers Union & East and Horn of Africa Human Rights Defenders Project, n 27.

[31] Accessible at http://www.assemblee.bi/IMG/pdf/9%20du%2011%20mai%202018.pdf.

[32] CIPESA, 'A new interception law and blocked websites: The deteriorating state of internet freedom in Burundi', 11 July 2018, accessible at https://cipesa.org/2018/07/a-new-interception-law-and-blocked-websites-the-deteriorating-state-of-internet-freedom-in-burundi/.

[33] International Service for Human Rights, 'Burundi | Stop the harassment, intimidation, arbitrary arrest and criminalization of human rights defenders', 18 January 2018, accessible at https://www.ishr.ch/news/burundi-stop-harassment-intimidation-arbitrary-arrest-and-criminalisation-human-rights.

[34] News24, 'Burundi rights activist handed five-year term', 14 August 2018, accessible at https://www.news24.com/Africa/News/burundi-rights-activist-handed-five-year-term-20180814.

the previous year's crackdown on the media began, with those remaining facing threats from the police and other authorities.[35] Several independent media houses have also been shut down.[36]

With the increase in internet users in Burundi, there has also been an increase in government efforts to control online information flows.[37] Burundi had a partial ten-day internet shutdown during the election period of 2015, which affected mobile access to social media platforms.[38] The shutdown was ordered by the Agence de Régulation et de Contrôle des Télécommunications after protests opposed to what opponents considered as a third-term for the President, despite a two-term constitutional limit.[39] A report of a discussion with a telecommunications provider revealed that the regulator simply telephoned and ordered that access to the social media platforms be unlocked, without there being any official documentation available regarding this blockage.[40]

From 29 April 2015 to 13 May 2016, the government ordered telecommunications companies and ISPs to block access to specific social media applications, including Twitter, Facebook and WhatsApp, on the grounds that "people were using those social media to spread dangerous rumours and helping protesters to organise their movements, which could endanger national security."[41] ISPs were also reportedly tasked to monitor users who were considered to be fuelling the protests."[42]

In August 2016, 56 individuals who were members of a WhatsApp political discussion group were arrested by police for allegedly spreading defamatory and abusive statements on WhatsApp and other social media.[43] This reinforced suspicion of government surveillance capability.[44] Ultimately, 46 were released, but eight members of the group were detained and were accused of "sending out libellous and insulting writings against institutions and authorities on the social media networks".[45]

[35] International Service for Human Rights, 'Briefing paper for the Universal Periodic Review: The situation of human rights defenders in the Republic of Burundi', June 2017, accessible at https://www.ishr.ch/sites/default/files/documents/172806_upr_briefing_paper_burundi_june2017_final_0.pdf.

[36] Freedom House, 'Freedom of the press 2017: Burundi', accessible at https://freedomhouse.org/report/freedom-press/2017/burundi; ARTICLE 19, CIPESA, the East Africa Law Society, Pan African Lawyers Union & East and Horn of Africa Human Rights Defenders Project, n 27.

[37] ARTICLE 19, CIPESA, the East Africa Law Society, Pan African Lawyers Union & East and Horn of Africa Human Rights Defenders Project, n 27.

[38] CIPESA, n 25, p 21.

[39] CIPESA, n 25, p 21.

[40] CIPESA, n 26.

[41] ARTICLE 19, CIPESA, the East Africa Law Society, Pan African Lawyers Union & East and Horn of Africa Human Rights Defenders Project, n 27.

[42] ARTICLE 19, CIPESA, the East Africa Law Society, Pan African Lawyers Union & East and Horn of Africa Human Rights Defenders Project, n 27.

[43] ARTICLE 19, CIPESA, the East Africa Law Society, Pan African Lawyers Union & East and Horn of Africa Human Rights Defenders Project, n 27.

[44] CIPESA, n 25, p 31.

[45] CIPESA, n 25, p 31.

In April 2017, concerns were also raised about the editor of Radio Isanganiro, Joseph Nsabiyabandi, being interrogated by the National Intelligence Service about his alleged collaboration with two Burundian exile radio stations based in neighbouring Rwanda.[46]

Certain independent news websites have also been blocked in Burundi. Since October 2017, the websites of independent local news publishers http://www.iwacu-burundi.org, http://www.isanganiro.org and http://www.ikiriho.org cannot be accessed from Burundi, and tests indicate that the websites are blocked from access within Burundi.[47] The conduct by the state in restricting access to the internet has led to many users having adopted VPNs to bypass such blockages.[48]

There has been no notable digital rights litigation in the period under review, despite a number of concerns regarding laws and practices underway in the country. The reprisals against civil society organisations and human rights defenders and difficulties experienced in operating within the country – which has consequently caused various actors to leave the country and operate from outside – have contributed to the dearth of jurisprudence in this regard.

(ii) ***Ethiopia***

The Constitution of Ethiopia, 1995 provides for freedom of expression, freedom of the press and access to information, and prohibits censorship. The constitutional guarantees were subsequently affirmed in the Mass Media and Freedom of Information Proclamation, 2008. However, there have been various violations to the right to freedom of expression, particularly during periods of states of emergency.

On 2 March 2018, the Ethiopian parliament approved a six-month state of emergency declared by Ethiopia's Council of Ministers, following the resignation of the country's prime minister the previous month. This has seen a crackdown by security agents against protesters and other critics, including seven protesters having been shot and killed by security agents and others arrested.[49] Concerns were raised that the state of emergency would facilitate other violations of the right to freedom of expression in the country,[50] particularly in the aftermath of the previous state of emergency that was declared from October 2016 and lasting for ten months.[51]

However, the resignation of the former prime minister has seen the appointment of a new prime minister, to whom positive reforms in the country have been attributed.[52] As such, although the challenges to

[46] Reporters Without Borders, 'Interrogation of Radio Isanganiro editor latest attack on free speech in Burundi', 6 April 2017, accessible at https://www.ifex.org/burundi/2017/04/06/radio_isanganiro/.

[47] CIPESA, n 32.

[48] CIPESA, n 26.

[49] IFEX, 'AFEX calls on Ethiopian government to uphold freedom of expression rights', 12 March 2018, accessible at https://www.ifex.org/ethiopia/2018/03/12/freedom-expression/.

[50] IFEX, n 49.

[51] Human Rights Watch, 'Ethiopia: Events of 2017', 2017, accessible at https://www.hrw.org/world-report/2018/country-chapters/ethiopia.

[52] CIPESA, 'The reforms Ethiopia needs to advance internet freedom', 6 August 2018, https://cipesa.org/2018/08/the-reforms-ethiopia-needs-to-advance-internet-freedom/.

freedom of expression that have been seen over the past several years are referred to below, there is a sense of optimism and the new prime minister and cabinet have promised to open up the democratic space in the country and expand freedom of expression online and offline.[53]

The government has historically tightly controlled the media landscape, which has been exacerbated during states of emergency.[54] Ethiopia has a powerful state-owned monopoly over telecommunications and internet services through EthioTelecom.[55] This has enabled the government to restrict information flows and access to internet and mobile phone services.[56] All connections to international internet are centralised through EthioTelecom, which enables the government to cut off the internet at will.[57] This monopoly has also caused access to telecommunications also remains prohibitively expensive for most users in the country, although it was announced in June 2018 that EthioTelecom would be privatised and the telecommunications market would be opened to other players.[58] For now, however, Ethiopia remains one of the least connected countries in the world, with low penetration rates stemming from underdeveloped telecommunications infrastructure, which is almost entirely absent from rural areas.[59]

The Ethiopian Telecommunications Agency is the primary regulatory body overseeing the telecommunications sector. In practice, government executives have complete control over ICT policy and sector regulation, and the Information Network Security Agency has significant power to regulate the internet under its mandate to protect communications infrastructure and prevent cybercrime.[60]

In the absence of independent domestic media, social media and diaspora television play key roles in disseminating information.[61] This has led the government to seek to restrict access to social media and diaspora television.[62]

In 2016, Twitter and WhatsApp services were shut down in the Oromia region of Ethiopia in response to protests by citizens seeking greater socio-political inclusion in the country, as well as in a bid to prevent examination papers being leaked.[63] Further shutdowns were reported in 2017, with disruptions reported during the national school leaving examinations for over 1 million high school learners.[64] In April 2017, two of the main diaspora television stations – Ethiopian Satellite Television and the Oromia Media Network – were charged under the anti-terrorism law, and the executive director of Oromia Media

[53] CIPESA, n 52.

[54] Human Rights Watch, n 51.

[55] Paradigm Initiative, 'Digital rights in Africa 2017 report', May 2018, p 23.

[56] Freedom House, 'Freedom on the net 2017: Ethiopia', accessible at https://freedomhouse.org/report/freedom-net/2017/ethiopia.

[57] Freedom House, n 56.

[58] Freedom House, 'Freedom on the net 2018: Ethiopia', accessible at https://freedomhouse.org/report/freedom-net/2018/ethiopia.

[59] Freedom House, n 58.

[60] Freedom House, n 56.

[61] Human Rights Watch, n 51.

[62] Human Rights Watch, n 51.

[63] Paradigm Initiative, n 55, p 23.

[64] Paradigm Initiative, n 55, p 23.

Network was charged under the criminal code.[65] However, access was restored in April 2018 under the new prime minister, and hundreds of previously blocked websites became accessible between May and June 2018.[66] Of concern, however, in August 2018 the new government reportedly shut off broadband and mobile internet in the Somali region of the country, following tension between the national and regional governments.[67]

On 25 May 2017, opposition politician Yonatan Tesfaye was sentenced to six years' imprisonment after being found guilty of "encouraging terrorism" for comments made on Facebook criticising the government for their handling of the Oromia protests.[68] Also in May 2017, Getachew Shiferaw, the former editor-in-chief of the opposition newspaper, *Negere Ethiopia*, was sentenced to 18 months in prison for making what was held to be "inciting comments" in a private message he sent to his colleagues using Facebook Messenger in which he criticised the government.[69]

In June 2017, musician Seena Solomon was arrested with her producers and performers for uploading so-called resistance music to YouTube, which the government categorised as incitement.[70] Similarly, musician Temeri Mekonen was also arrested for incitement through music.[71]

In March 2018, Seyoum Teshome, publisher of a popular blog known as the Ethiothinktank, was arrested at his residence, with reportedly no reason given for his arrest and no information provided regarding his whereabouts.[72] This followed Teshome's criticism of the government's six-month state of emergency. Teshome was also arrested and detained for two months during the previous state of emergency last year.[73]

Also in March 2018, William Davison, a reporter for *The Guardian*, was deported after being detained for a day at a police station, on the basis that Davison was not affiliated to any foreign media and, therefore, cannot cover happenings within the country.[74]

There have, however, been positive developments under the new regime and the appointment of the new Prime Minister. In this regard, in February 2018, after six years of facing charges that included terrorism and inciting violence, prosecutors announced that they would be dropping all remaining

[65] Human Rights Watch, n 51.

[66] Freedom House, n 58.

[67] NetBlocks, '#KeepItOn: Joint letter on keeping the internet open and secure in Ethiopia', 9 August 2018, accessible at https://netblocks.org/news/keepiton-joint-letter-on-ethiopia-qr8VJP85.

[68] Freedom House, n 56; Paradigm Initiative, n 55, p 23.

[69] Paradigm Initiative, n 55, p 23.

[70] Paradigm Initiative, n 55, p 24.

[71] Paradigm Initiative, n 55, p 24.

[72] IFEX, n 49.

[73] IFEX, n 49.

[74] IFEX, n 49.

charges.[75] The nine bloggers who make up Zone 9 comprise three journalists, a human rights lawyer and professionals working in business, government and academia, and called their blog Zone 9 after the term said to be used by political prisoners in Addis Ababa's Kaliti jail to refer to an outside world they viewed as equally shackled by the lack of civil liberties.[76] In April 2017, the Supreme Court held that two members of the Zone 9 Bloggers, who blog about human rights, good governance and social justice – and who had been acquitted of terrorism charges[77] – should instead face charges of inciting violence through their writing.[78] The new charges were based on Article 257 of the Criminal Code, and arise from the bloggers' possession of digital security manuals such as tutorials on communication encryption, that were alleged to be evidence of involvement in terrorism activities; had the charges not been dropped, a conviction carried a penalty of up to ten years in prison.[79]

This was not the only positive development following the regime change:[80]

> "In just the past few months, positive reforms have swept through Ethiopia. One of the notable changes has been the rapid expansion of internet freedom and digital rights in the country. Over the past decade, the Ethiopian government has relentlessly blocked news websites, blogs, and TV stations, jammed radio stations, and arrested those with dissenting voices. Now Ethiopia has dropped the charges against many bloggers, journalists, and opposition groups, freed thousands of prisoners, and most recently unblocked more than 250 websites."

There does remain cause to be vigilant. There also remain a number of laws of concern to the exercise of freedom of expression online that remain on the statute books.[81] Notably, this includes the Computer Crime Proclamation, enacted in June 2016, which criminalises an array of online activities.[82] In terms of the law, content that incites fear, violence, chaos or conflict among people can be punished with up to three years in prison; disseminating defamatory content can be penalised with up to 10 years in prison; the distribution of unsolicited messages to multiple emails (spam) carries up to five years in prison; and the government's surveillance capabilities are strengthened by enabling real-time monitoring or interception of communications.[83] In general, government surveillance of communications

[75] CIPESA, 'Zone 9 bloggers to speak on censorship, repression and surveillance at the Forum on Internet Freedom in Africa 2018', 17 September 2018, accessible at https://cipesa.org/2018/09/zone-9-bloggers-to-speak-on-censorship-repression-and-surveillance-at-the-forum-on-internet-freedom-in-africa-2018-fifafrica18/.

[76] The Guardian, 'Ethiopia's jailing of Zone 9 bloggers has a chilling effect on freedom of expression', 27 April 2015, accessible at https://www.theguardian.com/world/2015/apr/27/ethiopia-zone-9-bloggers-jailed-freedom-expression.

[77] Committee to Protect Journalists, 'In Ethiopia, Zone 9 bloggers acquitted of terrorism charges', 16 October 2015, accessible at https://cpj.org/2015/10/in-ethiopia-zone-9-bloggers-acquitted-of-terrorism.php.

[78] Committee to Protect Journalists, 'Ethiopia Supreme Court says two Zone 9 bloggers should face incitement charges', 6 April 2017, accessible at https://cpj.org/2017/04/ethiopia-supreme-court-says-two-zone-9-bloggers-sh.php.

[79] ARTICLE 19, 'Ethiopia: Free expression and online anonymity must be respected', 13 April 2017, accessible at https://www.article19.org/resources/ethiopia-free-expression-and-online-anonymity-must-be-respected/; Committee to Protect Journalists, n 78.

[80] Access Now, 'Ethiopia: Verifying the unblocking of websites', 3 July 2018, accessible at https://www.accessnow.org/ethiopia-verifying-the-unblocking-of-websites/.

[81] CIPESA, n 52.

[82] Accessible at http://www.addisinsight.com/2016/05/09/ethiopia-computer-crime-proclamation-text-draft/; Freedom House, n 56.

[83] Freedom House, n 56.

has been pervasive in the country, and has not been reformed under the new prime minister.[84] However, the new prime minister did reportedly force the resignations of officials of the Information Network Security Agency who were accused of monitoring and hacking activists.[85]

The Criminal Code also penalises defamation with a fine or up to one year imprisonment.[86] Moreover, in terms of the Anti-Terrorism Proclamation No. 652/2009, sentences of up to 20 years imprisonment for the publication of statements that directly or indirectly encourage terrorism. The law also bans VoIP services, and requires all individuals to register their telecommunications equipment – including smartphones – with the government.[87] Cybercafés are subject to burdensome operating requirements under the Telecom Fraud Offences Proclamation of 2012, which prohibit them from providing VoIP services, and mandate that owners obtain a licence from EthioTelecom via an opaque process that can take months.[88]

Digital rights litigation in the country has generally taken the form of defensive litigation that has been necessitated by criminal charges being brought against bloggers and other individuals for activities online, some of which have resulted in hefty penalties. In the instance of the Zone 9 bloggers, although they had been acquitted of terrorism charges and the prosecutors ultimately dropped all charges, it remains noteworthy that the court in the matter had ruled that certain members should still face charges of inciting violence through their writing prior to the charges being dropped. Despite the positive developments in the country following the new Prime Minister, it remains to be seen whether trust in the public institutions has yet been fully restored.

(iii) Kenya

Kenya has a competitive ICT sector that has seen access to the internet being widespread in the country, with an internet penetration rate of approximately 90%.[89] Although access has grown due to increasing affordability and improved speeds, there remains a digital divide between urban and rural areas, as well as a digital divide based on gender.[90] The National Optic Fibre Backbone Infrastructure aims to improve telecommunications across the country's governance structures and increase delivery of e-government services, such as applications for national identity cards or passports and registration of births and deaths.[91] As such, Kenya has a vibrant online culture, and has readily adopted online services such as mobile money platforms.

[84] Freedom House, n 58.
[85] Freedom House, n 58.
[86] Accessible at http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/70993/75092/F1429731028/ETH70993.pdf.
[87] Freedom House, n 58.
[88] Freedom House, n 58.
[89] Freedom House, n 92.
[90] Freedom House, n 92.
[91] Freedom House, n 92.

In the run-up to the presidential elections in 2017, Kenya faced various issues regarding hate speech, disinformation and surveillance that threatened to undermine freedom of expression online.[92] Notably, Kenya has a particularly well-organised civil society, who coordinated various efforts during the election period to monitor and challenge rights violations. In a positive development, the Communications Authority of Kenya provided a commitment that the internet would not be shut during the election period.[93]

A number of fake news websites were reportedly registered during the election period to disseminate false information, and different political camps reportedly set up teams of paid bloggers, social media influencers and bots to shape public opinion online.[94] Propaganda, hate speech and social media campaigns targeting individuals or organisations affiliated with the opposing side became common, including via paid Google Ads and Facebook sponsored posts.[95] Research analysing social media trends during elections indicated that bots had a significant influence in the Kenyan elections, at a rate of 24.8% during the August 2017 election and 27.6% during the October 2017 re-run of the election.[96]

Furthermore, in the run-up to the presidential election, the Communications Authority of Kenya sought powers to monitor calls and text messages of Kenyans, and the authorities announced that they had purchased $9.3 million to monitor social media and mobile phones.[97] Furthermore, in August 2017, the National Cohesion and Integration Committee monitored social media sites, identified 21 WhatsApp groups for spreading hate speech and arrested an administrator of another group for spreading false information.[98]

Concerns were raised as such provisions may unjustifiably limit permissible online expression.[99] In terms of the guidelines, administrators of social media pages were required to moderate and control the content and discussions generated on their platform; mobile network operators were given the power to refuse at their discretion the transmission of political messages that do not comply with the guidelines; and bulk political messages required prior approval from the National Cohesion and Integrated Commission under the guidelines.

The Communications Authority of Kenya is established as the regulatory authority of the communication sector in terms of the Kenya Information and Communications Act, 1998, as amended.[100] Concerns

[92] Freedom House, 'Freedom on the net 2017: Kenya', accessible at https://freedomhouse.org/report/freedom-net/2017/kenya.

[93] Freedom House, n 92.

[94] Freedom House, n 92.

[95] Freedom House, n 92.

[96] Quartz Africa, 'How social media bots became an influential force in Africa's elections', 18 July 2018, accessible at https://qz.com/africa/1330494/twitter-bots-in-kenya-lesotho-senegal-equatorial-guinea-elections/.

[97] Paradigm Initiative, n 55, p 27.

[98] CIPESA, n 25, p 16.

[99] Freedom House, n 92.

[100] Accessible at http://www.kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2013/THEKENYAINFORMATIONANDCOMMUNICATIONSAMENDMENTBILL2013.pdf.

have been raised that the independence of the Communications Authority of Kenya has been undermined through amendments to the legislation that enable the executive branch of government to appoint the chairperson and board members.[101] However, in June 2017, the High Court quashed certain amendments that sought to, among other things, transfer regulatory authority to the cabinet secretary.[102]

Recently, a matter of particular concern has been the notice placed by the Kenya Film and Classification Board in local newspapers, indicating that licences would be required for anyone filming with the intent to exhibit a film publicly, including videos recorded on mobile devices and posted on social media.[103] According to the notice, failure to comply could result in a fine of up to Ksh100,000 or imprisonment of up to five years.

There are also other examples of the government seeking to restrict online content. For instance, following public outcry over the public funds spent on foreign trips by the president, a popular website tracking these trips was taken down by the Kenya Network Information Centre in December 2015 following government order.[104] In a separate incident in June 2016, Kenya's Safaricom reportedly declined to provide unrestricted access to the Kenya Revenue Authority of user information and records relating to Mpesa, its mobile money platform.[105]

Kenyan law does not provide for the limitation of liability of intermediaries for hosting, caching, linking, or mere conduits. Intermediaries can be held legally responsible for content carried on or through their networks, which amounts to libel under the Defamation Act, copyright infringement under the Copyright Act, infringement of privacy, child pornography under the Sexual Offences Act, 2006, hate speech under the National Cohesion and Integration Act, or prohibited publication or inciting material under the Penal Code.[106] Under the 2017 Guidelines for the Prevention of Dissemination of Undesirable Bulk Political SMS and Social Media Content via Electronic Communications Networks, intermediaries can be held liable for spreading falsehoods, hate speech and insults, but there are no penalties are prescribed in these guidelines.[107]

Hate speech has been of particular concern in Kenya following the post-election violence in 2007. Hate speech is penalised under the National Cohesion and Integration Act, 2008, and individuals found guilty of spreading hate speech can be fined up to KES1 million, sentenced up to three years in prison, or both. Concerns have been raised that the hate speech provisions are used to silence opposition parties, and are open to abuse given the broad and vague definitions.[108]

[101] Freedom House, n 92.

[102] Freedom House, n 92.

[103] ARTICLE 19, 'Kenya: Censorship by film classification board limiting free expression', 17 May 2018, accessible at https://www.article19.org/resources/kenya-censorship-by-film-classification-board-limiting-free-expression/.

[104] CIPESA, n 25, p 20.

[105] CIPESA, n 25, p 34.

[106] CIPESA, n 25, p 25.

[107] CIPESA, n 25, p 25.

[108] ACCORD, 'South Africa and Kenya's legislative measures to prevent hate speech', 21 July 2017, accessible at http://www.accord.org.za/conflict-trends/south-africa-kenyas-legislative-measures-prevent-hate-speech/.

In Kenya, the Data Protection Bill has not yet been enacted, although this is gaining traction in recent months.[109] The Data Protection Bill has had a protracted history: in 2014, the Cabinet Secretary for for Information Communication and Technology announced that a Data Protection Bill would be tabled in Parliament to provide a single overarching regulatory framework for the processing of personal data; this was tabled a year later in 2015, and remained pending in parliament until it was reintroduced by the Senate's ICT Committee in 2018.[110] In May 2018, the Cabinet Secretary for the Ministry of Information, Communications and Technology constituted a task force to develop the policy and regulatory framework for privacy and data protection in Kenya, and to facilitate public consultation.[111] This is particularly timely, given that the country has been described as being in a "biometric craze", with both public and private bodies piloting and implementing voice, fingerprint, face and iris recognition systems.[112]

Furthermore, the right to privacy and anonymity has been compromised through the mandatory SIM card registrations imposed in terms of the Information and Communications (Registration of SIM Cards) Regulations, 2015. The regulations grant the communications regulator access to service providers' offices and records without a court order, which raises concerns about the lack of judicial oversight.[113] Furthermore, in April 2017, the Kenya Film Classification Board proposed a real-name registration policy on social media to curb the spread of fake news,[114] but the proposal was never made it to the floor of parliament.

Concerns have also been raised above the government's disproportionate surveillance capabilities. Although the Information and Communications Act prohibits unlawful monitoring and interception of communications, the Prevention of Terrorism Act, 2012 allows the authorities to limit constitutional freedoms – such as the right to privacy – during terrorist investigations. According to reports, national security agencies in Kenya, particularly the National Intelligence Service, have unlawful direct access to communication systems in Kenya that allow for the interception of both data and content.[115]

Notwithstanding these concerns, Kenya has a well-established constitutional framework and the courts have a strong record of upholding fundamental rights, including freedom of expression and privacy. Article 33 of the Constitution of Kenya, 2010 enshrines the right to freedom of expression, and Article 31 enshrines the right to privacy. The courts in Kenya also have a strong record of upholding fundamental

[109] CIPESA, n 25, p 12.

[110] Global Partners Digital, 'Data protection on the ground: Kenya's draft bill', 12 July 2018, accessible at https://www.gp-digital.org/data-protection-on-the-ground-1-kenyas-draft-bill/.

[111] Ministry of Information, Communications and Technology, 'Request for comments on the proposed Privacy and Data Protection Policy and Bill, 2018', undated, accessible at http://www.ict.go.ke/request-for-comments-on-the-proposed-privacy-and-data-protection-policy-and-bill-2018/.

[112] Kenya ICT Action Network, 'Policy brief: Data protection in Kenya', 2018, accessible at https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf.

[113] Freedom House, n 92.

[114] Quartz Africa, 'Kenya will propose a law to force people to use their real names on social media', 28 April 2018, accessible at https://qz.com/africa/971316/kenya-will-propose-a-law-to-force-people-to-use-their-real-names-on-social-media/.

[115] Privacy International, 'Trace, capture, kill: Inside communications surveillance and counter-terrorism in Kenya', March 2017, accessible at https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf.

rights, including online. In *Andare v Attorney General and Another*, the court found section 29 of the Information and Communications Act on improper use of licensed telecommunication system vague and beyond the scope of limitations in the constitution.[116] In February 2017, in *Okuta v Attorney General and Another*, the High Court held that the criminal defamation provisions under section 36 and 194 of the Penal Code laws were unconstitutional.[117] In *Alai v Attorney General*, in respect of a story featuring pictures of members of the President's family and criticising the President, the court found the offence of undermining the authority of a public officer under section 132 of the Penal Code unconstitutional.[118] The section had been used to prosecute both online and offline speech.[119] In August 2016, a court awarded Roshana Ebrahim, a former Miss World Kenya, Kshs 1 million in damages for breach of privacy after nude photographs were leaked of her by a former partner.[120] In a landmark decision in February 2017, a Kenyan court declared section 194 of the Penal Code which creates the offence of criminal defamation to be illegal.[121]

In an important victory in April 2018, in *Okiya Omtatah Okoiti v Communications Authority of Kenya and Others*,[122] the High Court found that installation of a device management system to access information on the international mobile equipment identity, international mobile subscriber identity, mobile station integrated subscriber directory number and call data records of subscribers would unjustifiably limit the right to privacy, notwithstanding with the objective of weeding out counterfeit phones. The court held that there were less restrictive means available to achieve the stated purpose, and fells outside of the legislative mandate of the Communication Authority of Kenya. The court held further that the decision was taken before undertaking meaningful stakeholder consultation, and was therefore incapable of being read in a manner that is constitutionally compliant.

Furthermore, in May 2018, in *Bloggers Association of Kenya v Attorney General and Others*, the High Court issued a conservatory order suspending the entry into force of 26 sections of the contentious Computer Misuse and Cybercrimes Act, 2018, just two weeks after it received presidential assent.[123] As set out in the petition, the law is challenged for contravening the constitutional provisions on freedom of opinion, freedom of expression, freedom of the media, freedom and security of the person, right to privacy, right to property and the right to a fair hearing.[124] Concerns had been raised regarding the Computer Misuse and Cybercrimes Act which, although aimed at combatting abuse and the spread of

[116] Andare v Attorney General, Petition No. 149 of 2015, accessible at https://globalfreedomofexpression.columbia.edu/cases/andare-v-attorney-general/.

[117] Okuta v Attorney General and Others, Petition No. 397 of 2016, accessible at https://globalfreedomofexpression.columbia.edu/cases/okuta-v-attorney-general/.

[118] Alai v Attorney General, Petition No. 147 of 2016, accessible at https://globalfreedomofexpression.columbia.edu/cases/alai-v-attorney-general/.

[119] Freedom House, n 92.

[120] Ebrahim v Ashleys Kenya Limited and Others, Petition No. 361 of 2016, accessible at http://kenyalaw.org/caselaw/cases/view/129282/.

[121] Paradigm Initiative, n 55, p 28.

[122] Constitutional Petition No. 53 of 2017, accessible at http://kenyalaw.org/caselaw/cases/view/151117/.

[123] CIPESA, 'Sections of Kenya's Computer Misuse and Cybercrimes Act, 2018 temporarily suspended', 30 May 2018, accessible at https://cipesa.org/2018/05/sections-of-kenyas-computer-misuse-and-cybercrimes-act-2018-temporarily-suspended/.

[124] Accessible at https://www.blog.bake.co.ke/wp-content/uploads/2018/05/BAKE-petition-Cybercrimes-act.pdf.

disinformation on social media, could be used to silence critical and dissenting voices in light of the hefty fines and long prison sentences.[125] Despite attempts by the Attorney General seeking to have the suspension lifted pending the hearing and determination of the case, the High Court held that the suspension would remain until November 2018 when a determination would be made on directions and the continuity of the case.[126]

However, despite the positive legal developments, there have also been incidents of concern. Numerous bloggers and social media users were arrested or summoned for questioning, many on the basis of their criticisms of government officials online before section 132 of the Penal Code was declared unconstitutional. For instance, in 2017, two WhatsApp administrators were arrested for allegedly sharing hate messages.[127] As summarised by Freedom House, this includes the following:[128]

- Jackson Njeru, an administrator for the Facebook page, "Buyer Beware," was arrested and jailed for three months in November 2016. He was charged with contempt of court for posting on Facebook about a case in progress against court orders. The post had requested page subscribers to contribute funds to provide bail for a defendant in the case.
- In October 2016, Deputy President William Ruto sued activist Boniface Mwangi for defamation on Twitter. Ruto withdrew the case in November.
- Authorities detained blogger Dennis Owino on 17 October 17 2016. Known for blogging on corruption issues, Owino was held for six hours before being released without charge.
- In October 2016, Kenya deported a South Sudanese rebel spokesperson, James Gatdet Dak, allegedly for comments he posted on his Facebook page that were seen as celebrating the firing of a Kenyan general by the UN Secretary General attached to the South Sudan peacekeeping mission.
- In July 2017, blogger Paul Odhiambo was arrested for spreading alleged hate speech on Facebook and WhatsApp.
- In August 2017, Robert Alai, a popular blogger and social media influencer, was arrested in connection with information he published about the health of a family member of President Kenyatta. Content posted on his Facebook page in relation to the story was removed without explanation. Alai has been arrested numerous times for online speech.
- Shortly after the August 2017 elections, Japeth Mulewa was arrested for being an administrator of a WhatsApp group that was allegedly spreading hate.
- In September 2017, Oliver Nyabwazi Moraira was arrested for allegedly posting hate speech on her Facebook page.

[125] Internet Sans Frontières, 'Kenya adds to the legislative inflation on 'fake news'', 24 May 2018, accessible at https://internetwithoutborders.org/kenya-adds-to-the-legislative-inflation-on-fake-news/; ARTICLE 19, 'Kenya: Passage of flawed Computer and Cybercrimes Act threatens free expression', 18 May 2018, accessible at https://www.article19.org/resources/kenya-passage-of-flawed-computer-and-cybercrimes-act-threatens-free-expression/.

[126] IT Web Africa, 'Bloggers gain upper hand in dispute over Kenya's cybercrime law', 4 October 2018, accessible at http://www.itwebafrica.com/security/515-kenya/244939-bloggers-gain-upper-hand-in-dispute-over-kenyas-cybercrime-law?o=eaan&E.

[127] Paradigm Initiative, n 55, p 28.

[128] Freedom House, n 92.

There have also been a number of incidents of bloggers and internet users being intimidated and subjected to violence; in this regard, there have reportedly been 94 incidents of violations against individual journalists and media workers, including bloggers, between May 2017 and April 2018.[129] Furthermore, content is periodically restricted for violating Kenyan social mores.[130] This also includes the example mentioned above regarding the restrictions on the distribution and exhibition of the 'Rafiki' film borne out of concerns by the Kenya Film and Classification Board that the film promoted homosexuality.[131]

From the examples set out above, Kenya can be seen as a leader in the region in respect of its digital rights litigation. The two recent decisions in particular in *Okoiti* and *Bloggers Association of Kenya* are landmark rulings that lay a positive foundation for similar challenges pertaining to surveillance and cybercrimes laws in Africa. The courts in Kenya has a strong record of upholding rights, including freedom of expression, which is further complimented by the existence of a number of well-established legal and civil society organisations that work on freedom of expression and digital rights. There are also further opportunities for future digital rights litigation in order to safeguard the rights of users, bloggers and others who have been targeted for their online activities.

(iv) Rwanda

Article 38 of the Constitution of Rwanda lays the foundation for the right to freedom of expression and access to information. The media is largely controlled by the government.[132] Other relevant laws include Law No 02/2013 of 2013 regulating the media; Law No 04/2013 of 2013 relating to access to information, which provides for the right to freedom of opinion and expression; and law No. 09/2013 of 2013 establishing Rwanda Utilities Regulatory Authority that is responsible for regulating the licensing of media houses, audio, audio-visual media and internet. Law No 02/2013 of 2013 also established a media self-regulatory body for journalists to ensure compliance with media principles.

Access to ICTs has improved notably over the past few years, supported by the government's strategy to transform the country into an information economy.[133] Following the liberalisation of the mobile telecommunications market in 2006, Rwanda's ICT market is generally vibrant and competitive, with there being three main mobile operators – MTN, TIGO and Airtel – and nine licensed ISPs as of June 2017.[134] Rwanda has been noted to be one of the fastest growing African countries in ICTs, and

[129] ARTICLE 19, 'Kenya: Violations of media freedom', 2018, accessible at https://www.article19.org/wp-content/uploads/2018/05/Kenya-Report-1.pdf.

[130] Freedom House, 'Freedom on the net 2018: Kenya', accessible at https://freedomhouse.org/report/freedom-net/2018/kenya.

[131] Freedom House, n 130.

[132] Jambonews, 'Rwanda: The right to freedom of expression and of free media remains in jeopardy', 4 December 2017, accessible at http://www.jambonews.net/en/news/20171204-rwanda-the-right-of-freedom-of-expression-and-of-free-media-remains-in-jeopardy/.

[133] Freedom House, 'Freedom on the net 2017: Rwanda, 2017, accessible at https://freedomhouse.org/report/freedom-net/2017/rwanda.

[134] Freedom House, n 133; Research ICT Africa, 'Disentangling the broadband divide in Rwanda: Supply-side v demand-side', May 2017, p 2, accessible at https://researchictafrica.net/polbrf/Research_ICT_Africa_Policy_Briefs/2017%20Policy%20Brief%202_Rwanda.pdf.

has strived to become a regional training centre for quality ICT professions and research.[135] However, despite measures to reduce costs, poverty remains the primary impediment to ICT uptake.[136]

Although there have not been any reports of restrictions on connectivity in Rwanda, Article 52 of the Law Governing Telecommunications, 2001 gives the government powers over telecommunications networks, including the power to suspend a telecommunications service for an indeterminate period, either generally or for certain communications.[137] Furthermore, the Rwandan government does restrict the types of online content that users can access, including news outlets and opposition blogs that have been blocked for years.[138]

The concerns regarding the government's efforts to block or interfere with the use of social media and other online platforms have been particularly heightened during election periods. In May 2017 – in the run-up to President Kagame's run for the presidency for a third time – the government published regulations to govern the manner in which campaign messages leading up to the presidential election should be posted on social media. In particular, it provided that any such content should first be submitted to the National Election Commission for approval or disapproval 24 hours before the post would be published.[139] Following significant public outrage, and a statement published by the Rwanda Utilities Regulatory Authority indicating that the elections body had no mandate to regulate social media use,[140] the elections body opted to back-track on the law.[141]

However, according to CIPESA, despite Rwanda's steady progress to economy through ICT innovations, there is an obstructive regime for the enjoyment of freedom of expression online, with restrictive laws governing media, arbitrary surveillance and interception of private communication and control of online platforms.[142] This view is echoed by Freedom House, which states that: "While Rwanda continued to make remarkable progress in its economic and ICT development in the past year, the country's tight restrictions on freedom of speech and political activity are among the world's worst, imposed under the pretext of maintaining stability in the aftermath of the 1994 genocide that claimed over 100 000 lives".[143]

In this regard, various laws and state practices contravene the constitutional guarantees of freedom of expression, access to information and privacy under Article 38 of the Constitution.

[135] Freedom House, 'Freedom on the net 2018: Rwanda', accessible at https://freedomhouse.org/report/freedom-net/2018/rwanda.

[136] Freedom House, n 133.

[137] Law No. 44/2001 of November 2001 Governing Telecommunications, accessible at http://www.rura.rw/fileadmin/laws/TelecomLaw.pdf.

[138] Freedom House, n 133.

[139] Freedom House, n 133.

[140] Accessible at http://www.rura.rw/index.php?id=104&tx_ttnews%5Btt_news%5D=156&cHash=d2f215ca024a96d0db5016ae8f8cc4f.

[141] CIPESA, 'Shadow report on the state of freedom of expression online in Rwanda', Shadow report to the ACHPR, 31 October 2017, accessible at https://cipesa.org/?wpfb_dl=257.

[142] CIPESA, n 141.

[143] Freedom House, n 133.

A law that has been the cause of particular concern is the Information and Communications Technologies Law No. 24/2016 of 2016. For instance, in terms of section 123, all electronic communications network or service providers are required to install technical instruments and features that allow and facilitate the lawful interception of electronic communications and monitoring, and to notify any authorised entity that carries out interception activities of any electronic network upgrades. In terms of section 126, the ICT Minister is empowered to interrupt any private communication that appears detrimental to national sovereignty, contrary to any existing law, public order or good morals, and to suspend wholly or in part any electronic communications service or network operations for a specified or undetermined period. Furthermore, in terms of section 127, all electronic communications service providers are obliged – "irrespective of professional secrecy" – to urgently and without monetary charges, collect and provide to the ICT Minister and the Regulatory Authority any information sought for the guidance and supervision of activity relating to the ICT sector.

At a more general level, concerns have also been raised that the law provides for unfettered powers to the minister and contains vaguely-defined terms.[144] The government has been urged to review the law and bring it in compliance with international human rights standards, out of concern for the impact that the law will have on the right to freedom of expression.[145]

Concern has also been raised regarding the Code of Criminal Procedure, under law No. 30/2013,[146] which empowers security organs in section 72 to seek written authority from any prosecutor appointed by the Justice Minister during investigations to intercept private audio and video recordings, email or online communications on grounds of national security, which is defined as measures taken by the country to ensure its security. The written permission may, however, be waived on grounds of urgency for national security purposes. Such interception orders are valid for three months, renewable once. The concern raised is that this provision fundamentally undermines the independence of the courts and bars them from using their discretionary powers to halt any such impugned interceptions pending the hearing of the petition.[147] Article 451 of the Penal Code further creates the criminal offence of spreading false information with the intent to create a hostile international opinion.

There are also concerns with the surveillance provisions contained in Law No. 60/2013[148] regulating the Interception of Communications. In this regard, it is required in terms of section 7 that communication service providers support interceptions by ensuring that their systems are capable of interception. Section 10 further provides that security organs requiring interception may request direct interception without resorting to service providers. In July 2018, the government passed a law that extends the powers of interception to a civilian institution – the Office of the Ombudsman – to investigate

[144] CIPESA, n 141.

[145] ARTICLE 19, 'Rwanda: Law governing information and communication technologies', 18 May 2018, accessible at https://www.article19.org/resources/rwanda-law-governing-information-and-communication-technologies/.

[146] Accessible at http://itegeko.com/en/codes-lois/code-of-criminalprocedure-2/.

[147] CIPESA, n 141.

[148] Accessible at http://rema.gov.rw/rema_doc/Laws/Itegeko%20rishya%20rya%20REMA.pdf.

corruption-related crimes.[149] Furthermore, the Rwanda Utilities Regulatory Authority is permitted unrestricted access to the SIM card databases, and may be required to facilitate access of authorised persons in certain circumstances.[150]

Criminal defamation, insult and genocide ideology offences provided for under articles 288 and 289 of the Penal Code No. 01/2012 of 2012 and the Genocide Ideology Law, 2008 prescribe hefty penalties for speech, ranging from fines to prison sentences of up to nine years for the latter offence and two years for the former.[151] In August 2018, revisions to the Penal Code were signed into law increasing the penalties for criminal defamation, including a prison sentence of five to seven years for defamation against the president.[152] It also penalises the "humiliation of national authorities", including through cartoons, with one to two years in prison and fines.[153] Furthermore, the spread of "false information or harmful propaganda with the intent to cause a hostile international opinion against [the] Rwanda government" carries penalties of between seven and ten years in prison in peacetime, and life imprisonment during wartime.[154] Although the law does not expressly state so, the offences likely apply to both online and offline content.

It has been reported that there have been a few arrests for online activities. In October 2016, Joseph Nkusi, a blogger, was arrested on his return to Rwanda from Norway and questioned about his political activities and online writings that were known for being critical of the government. According to reports, Nkusi had founded a radical opposition group while living in Norway and made false claims about the 1994 genocide, which is illegal under Rwanda's law against "genocide ideology". In March 2018, Nkusi was sentenced to ten years in prison for incitement to civil disobedience and the spread of rumours.[155]

Arrests for online activities encouraged increased self-censorship in the country. For instance, in March 2017, Violette Uwamahoro, a Rwandan native, was charged with revealing state secrets and other offences, reportedly based on email exchanges and WhatsApp messages that the prosecutor had presented before the court as evidence.[156] She remained on trial as of mid-2017.[157]

There has not been any notable digital rights litigation in the country, despite laws pertaining to surveillance and online content restrictions giving rise to serious concerns. As ICT adoption and

[149] Freedom House, n 135.

[150] 001/ICT/RURA /2013, 16 January 2013, accessible at http://www.rura.rw/uploads/media/FINAL_SIM_CARD_REGISTRATION_REGULATIONS_03.pdf.

[151] AllAfrica, 'Rwanda: Jail term for insulting Rwandan President', 28 October 2017, accessible at https://allafrica.com/stories/201710290050.html; CIPESA, CIPESA, n 141.

[152] Freedom House, n 135.

[153] Freedom House, n 135.

[154] Freedom House, n 135.

[155] Freedom House, n 135.

[156] BBC News, 'British Rwanda 'plot' woman Violette Uwamahoro back in UK', 12 April 2017, accessible at https://www.bbc.com/news/world-africa-39579013; BBC News, 'Violette Uwamahoro: Rwanda court releases UK woman', 27 March 2017, accessible at https://www.bbc.co.uk/news/world-africa-39410708; Freedom House, n 133.

[157] Freedom House, n 133.

development in the country continues to grow, it is likely that future opportunities for digital rights litigation will arise in order to ensure that users' rights are safeguarded.

(v) Tanzania

The situation in Tanzania has been described as an "unprecedented human rights crisis", with there being at least eight media houses banned, at least 27 journalists arbitrarily arrested and detained, and 32 citizens having been charged for publicly or privately criticising the president or the government.[158] Since taking office in October 2015, the president has restricted basic freedoms through repressive laws and decrees, and critical journalists, politicians, human rights defenders, civil society activists and senior UN officials have faced various threats, intimidation and arbitrary detention by government authorities.[159] In May 2018, 65 CSOs wrote to the Tanzanian government raising their concerns about the rapidly deteriorating environment for the media, human rights defenders and opposition party members in the country.[160]

A significant development has been the decision by the government to sign the Electronic and Postal Communications (Online Content) Regulations, 2018 into law with effect from April 2018.[161] This requires the registration of all online publishers with the state communication authorities In terms of Regulation 2, the regulations apply to all online content, including application services, bloggers, internet cafés, online content hosts, online forums, online radio or television, social media, subscribers and users of online content, and any other related online content. Concern has been expressed that the regulations "seek to further constrain an already dwindling space for freedom of expression in Tanzania".[162] Various concerns have been raised with the regulations, including concerns that the definitions are vague and overbroad, that the powers afforded to the Communications Regulatory Authority seriously interfere with the right to freedom of expression, and that it imposes a wide range of obligations on different users, ISPs and others.[163]

Part III of the Regulations sets out the general obligations for online content, which include requiring online content providers to "ensure that online content is safe, secure and does not contravene the provisions of any written law" and, in terms of Regulation 5, to "use moderating tools to filter prohibited content" and "put in place mechanisms to identify source of content". Online content providers are also required to remove content within 12 hours of being notified, and are obliged in terms of Regulation 5(3) to cooperate with law enforcement officers. Regulation 5(2) requires subscribers and users of online content to be responsible and accountable for information they post in online forums, social media, blogs and other related media. Bloggers and online forums will also be required to register with the

[158] International Federation for Human Rights & Legal and Human Rights Centre, 'Tanzania: Freedom of expression in peril', August 2017, p 2.

[159] Human Rights Watch, 'Tanzania: Events of 2017', accessible at https://www.hrw.org/world-report/2018/country-chapters/tanzania-and-zanzibar.

[160] ARTICLE 19, n 179.

[161] ARTICLE 19, 'Tanzania: Restrictive regulations on online content signed into law', 23 April 2018, accessible at https://www.article19.org/resources/tanzania-restrictive-regulations-online-content-signed-law/.

[162] ARTICLE 19, n 161.

[163] ARTICLE 19, n 161.

Tanzania Communications Regulatory Authority, and where the blog or online forum allows the public to post content, they are required to set mechanisms so that content will not be published prior to their review. Regulation 7(1) provides that bloggers are also required to use moderating tools to filter content and set mechanisms to identify the source of such content. In terms of regulation 7(2), these requirements apply to Tanzanian residents, Tanzanian citizens outside the country or non-citizens residing in the country blogging or running online forums with content for consumption by Tanzanians.

In terms of regulation 16, the regulations impose a TShs. 5 million fine for social media users and online content producers found with materials deemed "indecent, obscene, hate speech, extreme violence or material that will offend or incite others, cause annoyance, threaten harm or evil, encourage or incite crime, or lead to public disorder".[164] The regulations were opened for public consultation in September 2017, and will come into force once signed by the Minister of Information, Culture, Arts and Sports. The Regulations have been severely criticised for overly restricting freedom of expression and media freedom through unnecessary censorship, prohibition of anonymity, registration requirements for bloggers and online forums, the wide scope of prohibited content, and the power afforded to intermediaries to interfere with users' freedom of expression.[165]

These measures appear to be targeted specifically at bloggers, citizen journalists and digital-first media publications reporting on and providing critical opinion and commentary against State actors through formerly less-regulated, more accessible and increasingly influential online publishing platforms than legacy media which is otherwise highly regulated, cost prohibitive, and losing trust and traction.

Prior to this, the Tanzanian government introduced four laws that impact freedom of expression and the press: the Cybercrimes Act, 2015; the Statistics Act, 2015; the Media Services Act, 2016; and the Access to Information Act, 2016.[166] The Cybercrimes Act has given rise to particular concern. In terms of section 16, it is an offence to publish information, data or facts presented in a picture, text, symbol or any other form in a computer system, where such information, data or fact is false, deceptive, misleading or inaccurate.[167] Furthermore, the government has been described as using the Cybercrimes Act to legally harass private citizens who criticise the government on online platforms.[168]

Jamii Media has previously sought to challenge sections 32 and 38 of the Cybercrimes Act, seeking to declare it unconstitutional. In March 2017, the High Court of Tanzania concluded that the impugned provisions were not unconstitutional, and that Tanzania's police have unfettered powers in investigating cybercrimes.[169] The judgment has been criticised for violating the right to privacy as contained in the

[164] CIPESA, n 25, p 14.

[165] Media Council of Tanzania, 'Online Content Regulation will strangle freedom of expression', The Guardian, 4 October 2017, accessible at https://www.ippmedia.com/en/columnist/online-content-regulations-will-strangle-freedom-expression-1.

[166] International Federation for Human Rights & Legal and Human Rights Centre, n 158.

[167] CIPESA, n 25, p 19.

[168] International Federation for Human Rights & Legal and Human Rights Centre, n 158.

[169] ARTICLE 19, 'Tanzania: Cybercrimes Act upheld in further blow to free expression', 15 March 2017, accessible at https://www.article19.org/resources/tanzania-cybercrimes-act-upheld-in-further-blow-to-free-expression/.

Constitution of Tanzania and the ICCPR in allowing the state to infringe on citizens' rights to privacy without judicial oversight.[170]

There is also an important challenge to the legality of the Media Services Act, the Legal and Human Rights Centre, the Media Council of Tanzania and Tanzania Human Rights Defender's Coalition filed an application before the EACJ on 11 January 2017.[171] The three organisations highlighted several sections of the Media Services Act, arguing that they were a threat to the freedoms of expression and of information, thus violating Tanzania's obligations under the East African Treaty. As mentioned above, the EACJ has already ruled against the government of Tanzania in the *Mseto* matter, and upheld the right to freedom of expression on that occasion.[172]

The government has also shut down or threatened privately owned radio stations and newspapers, and ended live transmissions of parliamentary debates.[173] In respect of the banning of newspapers: in June 2017, authorities banned the independent newspaper *Mawio* for two years over articles linking former presidents to alleged mismanagement of mining deals; thereafter, in September, the government banned *Mwanahalisi*, a weekly newspaper, for two years on claims of unethical reporting and endangering national security for an article calling for people to pray for an opposition party member; in October, authorities banned *Raia Mwema*, a weekly newspaper, for 90 days for publishing an article deemed critical of Magufuli's presidency.[174]

The situation for critics of the government has been dire. In 2016, at least ten people were arrested and charged for online offences, including six being charged under the Cybercrime Act, 2015 for insulting or criticising the leadership style of the President through posts on Facebook or WhatsApp.[175] Furthermore, in December 2016, police arrested Maxence Melo, a prominent human rights defender and the owner of Jamii Forums, an independent whistleblower and reporting website, and Mike William, a shareholder of Jamii media which hosts the site.[176] The site hosted articles and debates exposing public sector corruption and criticising government actions. Police searched the offices of Jamii Forums and Melo's home without warrants, and reportedly made copies of several documents.[177] On 16 December 2016, the Resident Magistrate Court of Dar es Salaam brought charges against Melo in terms of the Cyber Crimes Act, including obstruction of investigations for refusing to reveal the names of anonymous contributors to Jamii Forums, and managing a domain not registered in Tanzania.[178] Although the court began hearing the case in August 2018, there have been over 40 adjournments.[179]

[170] ARTICLE 19, n 169.

[171] International Federation for Human Rights & Legal and Human Rights Centre, n 158.

[172] Accessible at https://www.mediadefence.org/news/east-african-court-overturns-tanzania%E2%80%99s-newspaper-ban.

[173] Human Rights Watch, n 159.

[174] Human Rights Watch, n 159.

[175] CIPESA, n 25, p 14.

[176] Human Rights Watch, n 159.

[177] Human Rights Watch, n 159.

[178] Human Rights Watch, n 159.

[179] ARTICLE 19, 'Tanzania: Civil society groups express concern over rapid decline in human rights', 10 May 2018, accessible at https://www.article19.org/resources/tanzania-civil-society-groups-express-concern-over-rapid-decline-in-human-rights/.

In 2017, outspoken opposition MPs Tundu Lissu and Halima Mdee were arrested and detained for abusing the President, as well as for sedition and incitement respectively.[180] In December 2016, Godbless Lema, another member of Parliament, was detained for four months and was charged with sedition for insulting the President in a video and audio clips that were widely shared on social medial.[181] In March 2017, Tanzanian rapper Nay wa Mitego was arrested and detained for a day in relation to the lyrics of the song, "WAPO", which were deemed insulting to the government and the President.[182]

Digital rights litigation within the country has been limited, and notably the important challenge to the Cybercrimes Act was unsuccessful. Furthermore, other cases have suffered from lengthy delays. Legal and civil society organisations, as well as members of the media, have suffered serious reprisals from state actors for challenging the government and seeking to exercise their freedom of expression and press freedom, which have placed constraints on the ability of these organisations to conduct their work freely. The EACJ has presented an important opportunity for freedom of expression litigation, and may continue to be an avenue to be pursued in respect of digital rights litigation as well.

(vi) Uganda

The Constitution of Uganda guarantees freedom of the press and expression. As at 2016, Uganda had an internet penetration rate of approximately 19%.[183] Although internet access has become more affordable, particularly on mobile phones, costs are expensive, and limited access to electricity further impedes access in rural areas.[184] Uganda's communication sector is amongst the fastest growing in Africa due to the rapid growth of mobile telephony, with 22 ISPs in the country.[185]

There have been some significant – and concerning – developments during the course of 2018 that affect freedom of expression online. In March 2018, the Ugandan Communications Commission issued a notice calling for online publishers, news platforms, radio and television operators to "apply and obtain authorization" for the provision of services.[186] Without specifying the requirements necessary for application, the Ugandan Communications Commission indicated that, within a month of issuance of the notice, measures will be enforced against non-compliant service providers and this "may entail directing Internet Service Providers (ISP) to block access to such websites and/or streams."[187] The Ugandan Communications Commissions is mandated under section 5 of the Communications Act, 2013

[180] CIPESA, n 25, p 14.

[181] CIPESA, n 25, p 14.

[182] CIPESA, n 25, p 14.

[183] Internet Live Stats, 'Internet users by country (2016)', 2016.

[184] Freedom House, 'Freedom on the net 2017: Uganda', accessible at https://freedomhouse.org/report/freedom-net/2017/uganda.

[185] AFEX, 'Internet freedom in Africa: Baseline report of eight countries', 2017, p 55.

[186] Accessible at https://www.www.ucc.co.ug/wp-content/uploads/2018/03/UCC_ONLINE-DATA-COMMUNICATIONS-SERVICES.pdf.

[187] CIPESA, 'Uganda moves to register online content providers', 25 March 2018, accessible at https://cipesa.org/2018/03/uganda-moves-to-register-online-content-providers/.

to monitor, inspect, license, supervise, control and regulate all communications services, including internet-based platforms.

Uganda has also begun charging a tax on using social media, focused on over-the-top services such as Facebook, Twitter, Tinder and Grinder.[188] On 30 May 2018, the Ugandan parliament passed the Excise Duty (Amendment) Bill 2018, which, among other things, provides that: "A telecommunication service operator providing data used for accessing over the top services is liable to account and pay excise duty on the access to over the top services."[189] At the time of announcing it in March 2018, the president stated that the tax was aimed at platforms such as WhatsApp, Facebook, Twitter, Skype and Viber, in order to curtail "gossip".[190] This came into effect on 1 July 2018, and has been described as a "clear attempt to undermine the right to freedom of expression".[191] According to this law, over the top services – including WhatsApp, Facebook or Twitter – will be subject to a tax duty of UGX200 per user per day of access.[192] This raises serious concerns that the increased cost will push basic connectivity out of the reach of millions.[193] However, later that month, it was announced in parliament that the government would be reviewing the decision to impose the tax following concerns raised by the public.[194]

The day after the law came into effect, a Ugandan technology company, Cyber Law Initiative (U) Limited, filed a petition before the Constitutional Court seeking to have the government's decision overturned and the law declared illegal, null and void.[195] The case is still pending.

Some of the key laws in Uganda include the following: the Communications Act, 2013 that has the mandate of managing communications operations in the country; the Communications Amendment Bill, 2016 that removed parliamentary approval as a requirement in the approval of regulation by the Ministry; the Computer Misuse Act, 2011 that ensures safety and security of electronic transactions and information systems and forbids the abuse, misuse and unlawful access to information; the Anti-Terrorism Act, 2002 that allows the interception of information in regard to acts of terrorism, including the interception of correspondence and surveillance of persons suspected to be involved or plan acts of terrorism; the National Information Technology Act, 2009 that established the National Information

[188] Global News, 'Uganda is charging a tax on using social media. Free speech advocates are livid', 2 July 2018, accessible at https://globalnews.ca/news/4308191/uganda-social-media-tax/; AFEX, 'Ugandan government taxes social media users, threat to internet rights', 1 June 2018, accessible at http://www.africafex.org/digital-rights/ugandan-government-taxes-social-media-users-threat-to-internet-rights-2.

[189] ARTICLE 19, n 20.

[190] Amnesty International, 'Uganda: Scrap social media tax curtailing freedom of expression', 2 July 2018, accessible at https://www.amnesty.org/en/latest/news/2018/07/uganda-scrap-social-media-tax-curtailing-freedom-of-expression/; Paradigm Initiative, 'Shots fired against digital rights in Uganda and Tanzania', 9 April 2018, accessible at https://paradigmhq.org/shots-fired-against-digital-rights-in-uganda-and-tanzania/.

[191] Amnesty International, n 190.

[192] ARTICLE 19, n 20.

[193] CIPESA, 'Uganda blocks access to social media, VPNs and dating sites as new tax takes effect', 1 July 2018, accessible at https://cipesa.org/2018/07/uganda-blocks-access-to-social-media-vpns-and-dating-sites-as-new-tax-takes-effect/.

[194] Mail & Guardian, 'Uganda reviewing social media taxes after outcry', 12 July 2018, accessible at https://mg.co.za/article/2018-07-12-uganda-reviewing-social-media-taxes-after-outcry.

[195] CNN, 'Uganda government sued over social media tax', 2 July 2018, accessible at https://edition.cnn.com/2018/06/01/africa/uganda-social-media-tax/index.html.

Technology Authority to oversee information technology; the Regulation of Interception of Communications Act, 2010 that provides that a warrant to intercept communications can be issued by a designated judge; the Anti-Pornography Act, 2014 that punishes all forms of pornography and allows for the creation of a registry of all persons found guilty under the act.[196] The country's draft Data Protection and Privacy Bill, 2014 has not yet been passed.[197]

In terms of section 9 of Uganda's Anti-Terrorism Act, 2002, any person who runs or supports any institution for publishing and disseminating news or materials that promote terrorism" guilty of an offence. Concern has been raised that this provision can construe any content passing through an ISP or intermediary as information promoting terrorism and therefore in contravention of the law.[198] Further, in terms of section 20, any person who knowingly obstructs an authorised officer in carrying out interception and surveillance commits an offence. On a related note, in terms of the Anti-Pornography Act, 2014, ISPs are liable if they do not use or enforce the procedure recommended by the Pornography Control Committee to control pornography and thus permit its download or upload through their service; section 7 empowers the Committee to expedite the development, acquisition and installation of software to detect and suppress pornography.

Section 79 of the Communications Act prohibits the unlawful interception and disclosure of communications of persons by an operator or employee of an operator of a communication service or system. Also, section 80 makes it an offence for an operator or an employee to intentionally intercept, disrupt, deny accessibility to or to divert government communication. Service providers who fail to provide services that render real time and full time monitoring facilities for the interception of communication are liable to punishment with a fine of UGX 2,040,000 or imprisonment for a period not exceeding five years or both, as well as a possible cancellation of their licence.

In April 2017, parliament passed the Communications (Amendment) Bill, 2016, which amended section 93(1) of the Communications Act to eliminate the system of checks and balances on the minister's supervision of the communications sector.[199] The strengthened power of the minister was witnessed when he ignored parliament's motion to extend SIM card re-registration and instead directed the Ugandan Communications Commission to switch off all unverified cards in 2017.[200]

There have been a number of social media shutdowns in Uganda, typically justified in terms of sections 5 and 6 of the Communication Act that gives the Uganda Communications Commission the mandate to block access to social media and mobile money services.[201] This is rationalised by the government on the basis that the shutdowns are necessary to ensure state security and to decrease cybercrime.[202] For instance, during the presidential election in February 2016, the government shut down Facebook,

[196] AFEX, n 185, pp 55-57.
[197] AFEX, n 185, p 57.
[198] CIPESA, n 25, p 19.
[199] Freedom House, n 184; CIPESA, n 25, p 28.
[200] Freedom House, n 184; CIPESA, n 25, p 28.
[201] AFEX, n 185, p 60.
[202] AFEX, n 185, p 60.

Twitter, WhatsApp, and mobile money services; thereafter, in May 2016, a similar shutdown occurred on the day of the presidential inauguration.[203] These shutdowns were carried out under the guise of curtailing civil unrests.[204] It is estimated that at least 1.5 million VPNs were downloaded during the internet shutdown in February 2016.[205]

In June 2017, the High Court in Kampala heard argument in a matter brought by Unwanted Witness against the Attorney General, the Uganda Communications Commission and the eight telecommunications companies challenging the internet shutdown and social media blockage in February and May 2016.[206] The case remains ongoing.

The Ugandan government is reportedly believed to be working on a proposal to limit the number of internet gateways by requiring that they are routed through the Uganda Internet Exchange Point, as well as other proposals requiring the hosting of content, websites, databases, and any other applications within the country.[207] Concern has been raised that such a move would allow greater government control and monitoring ability of internet traffic and content from an infrastructure level.[208]

There have also been incidents of arbitrary blocking and filtering of social media content.[209] The Anti-Pornography Act, Anti-Terrorism Act and the Computer Misuse Act and the further allow the government to monitor pornography and immoral content, to exercise surveillance of the internet and social media, and for the government to arrest and prosecute persons for such publications on social media or over the internet.[210] This has reportedly also been used by the government to justify the filtering or blocking of publications that criticise the government.[211]

There is currently a constitutionality challenge to the Computer Misuse Act and other cyber-related laws, on the basis that these laws are being used to stifle freedom of expression. This includes a challenge to section 25 of the Computer Misuse Act, which provides that: "Any person who wilfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanour and is liable on conviction to a fine not exceeding twenty-four currency points or imprisonment not exceeding one year or both." It is argued in the petition that the impugned provision

[203] Freedom House, 'Freedom on the net 2016: Uganda', 2016.

[204] Freedom House, n 203.

[205] CIPESA, n 25, p 30.

[206] Unwanted Witness, 'Court adjourns social media shutdown lawsuit', 22 May 2017, accessible at https://unwantedwitness.or.ug/court-adjourns-social-media-shutdown-lawsuit/.

[207] CIPESA, n 25, p 32.

[208] CIPESA, n 25, p 32.

[209] AFEX, n 185, p 62.

[210] AFEX, n 185, p 62.

[211] AFEX, n 185, p 62.

fails to meet regional and international human rights norms and standards.[212] Calls have been made for the hearing of the petitions before the Constitutional Court to be fast-tracked.[213]

A number of Ugandans have faced threats, harassment and lawsuits for exercising their right to freedom of expression. For instance, during 2017 alone, at least 25 Ugandans reportedly faced charges related to freedom of expression online, making this the highest number of Ugandans arrested for their online expression.[214] The Computer Misuse Act has been one of the government's most preferred laws to criminalise users' online activities given its broad provisions that make offences of online communications that disturb the "peace and quiet" of a person or those which may be "obscene, lewd, lascivious, or indecent".[215]

In August 2016, Fred Muwema, a prominent Ugandan lawyer, sought orders to reveal the identity of the blogger who goes under the name Tom Voltaire Okwalinga, and further prohibiting the alleged defamatory publications on his Facebook page, pursuant to section 33 of the Defamation Act, 2009.[216] Muwema sued Facebook in Ireland, where the company is legally registered, after the company refused his request to reveal the identity.[217] In its initial ruling, the High Court of Ireland ruled in favour of Muwema, ordering Facebook to reveal the identity, but later recalled the decision following Facebook's appeal that the order posed a risk to the personal safety of the person(s) behind the page. [218] Facebook also cited a previous case when the Ugandan government had requested Tom Voltaire Okwalinga's administrative identity, which it did not grant.[219] In the court's final decision, made in February 2017, the court agreed that the offending posts were defamatory and instructed Facebook to notify Tom Voltaire Okwalinga to remove the posts within fourteen days.[220]

Later that year, in November 2016, Ugandan police arrested, detained, charged, and later released KTN Kenya news anchor and reporter Joy Doreen Biira, a Ugandan, for abetting terrorism by allegedly taking photos of mass killings in Kasese in Uganda where 55 were killed by the army, and posting them on Facebook.[221] Her laptop and phones were confiscated and she was forced to delete the posts.[222] Her arrest was widely condemned, sparking outrage online through hashtags such as #FreeJoyDoreen and #JournalismIsNotaCrime which trended on Twitter.[223] She was released on bond and the case

[212] Freedom House, n 184.

[213] PML Daily Reporter, 'Digital rights body slams security agencies on harassing online users', 31 August 2018, accessible at http://www.pmldaily.com/news/2018/08/digital-rights-body-slams-security-agencies-on-harassing-online-users.html.

[214] Digital Watch Observatory, 'Internet users in Uganda facing charges for online freedom of expression', 19 January 2018, accessible at https://dig.watch/updates/internet-users-uganda-facing-charges-online-freedom-expression.

[215] Freedom House, n 184.

[216] CIPESA, n 25, p 18.

[217] Freedom House, n 184.

[218] Freedom House, n 184.

[219] Freedom House, n 184.

[220] Freedom House, n 184.

[221] CIPESA, n 25, p 20.

[222] CIPESA, n 25, p 20.

[223] CIPESA, n 25, p 20.

against her is ongoing, despite calls by KTN Kenya for solidarity and her release.[224] In December 2016, Swaibu Nsamba Gwogyolonga, an opposition leader in Uganda, was accused of vilifying President Museveni by posting the President's image in a casket on Facebook.[225] He was arrested and charged with "offensive communication and libel contrary to sections 25 of the Computer Misuse Act and 181(1) of the Penal Code respectively, and he is currently out on bail.[226]

A case that received much attention was that of Stella Nyanzi in April 2017. Dr Nyanzi is a human rights activist, who was charged with cyber harassment against President Museveni based on the Computer Misuse Act.[227] Nyanzi used social media to criticise the President and his wife, who is also the Minister of Education, which was deemed by the state to be offensive and in breach of his right of peace and privacy.[228] In this regard, Dr Nyanzi was abducted by law enforcement, detained and later charged with two counts of cyber harassment and offensive communication under section 24(1)(2)(a) and 25 of the Computer Misuse Act for "repeatedly insulting the person of the President" on her Facebook page, referring to him as "a pair of buttocks" and his wife as "empty-brained".[229] Dr Nyanzi was remanded in prison for 33 days before being freed on bail in May 2017.[230]

The same month, Gertrude Uwitware, a news anchor with NTV Uganda, was abducted by unknown assailants and badly beaten following posts she made on her blog defending academic Stella Nyanzi's criticisms of the current regime.[231] Both Uwitware and Biira were forced to remove their respective posts from social media.[232]

There appear to be important opportunities for digital rights litigation in the country. As mentioned, there are two key cases pending before the courts pertaining to internet shutdowns and to provisions of the Computer Misuse Act. These cases have the potential to set important precedents for the safeguarding of digital rights, both in Uganda and more broadly across the region.

Concluding observations

While each of the countries under review present unique challenges and opportunities that are particular to the domestic context, there are certain key trends that should also be highlighted.

Social media taxes and licences has been a notable trend in the East African region. This has included, for instance, the decision in Uganda to charge users an excise duty on their access to over-the-top services and social networking platforms such as Facebook, Twitter, Skype and WhatsApp.

[224] CIPESA, n 25, p 20.
[225] CIPESA, n 25, p 15.
[226] CIPESA, n 25, p 15.
[227] AFEX, n 185, p 58.
[228] AFEX, n 185, p 58.
[229] CIPESA, n 25, p 15.
[230] CIPESA, n 25, p 15.
[231] Freedom House, n 184.
[232] Freedom House, n 184.

Furthermore, in Kenya and Tanzania, for instance, measures have been put in place to require publishers of online content, such as bloggers, to obtain a licence or register with the relevant authorities in order to post such content on their blogs, social media accounts and websites. These measures risk making the cost to communicate prohibitively expensive for users, and severely impede the right to freedom of expression through onerous administrative burdens and content restrictions.

Content restrictions more generally is a trend seen in all the countries under review, with there being a plethora of laws and policies that impact the exercise of free speech online. Recent developments have included, for instance, the Law Regulating the Media in Burundi and the Electronic and Postal Communications (Online Content) Regulations in Tanzania. Criminal defamation remains on the statute books in countries such as Ethiopia and Rwanda, where imprisonment remains a possible penalty for being found guilty of the offence; in particular, in Rwanda, the recent revisions to the Penal Code have increased the penalties for criminal defamation, including a prison sentence of five to seven years for defamation against the president, which appears to be contrary to the African Court ruling in *Konaté v Burundi*. Concerns regarding content restrictions are exacerbated when the grounds of restriction include vague terms such as “national unity” and “public morality”, as was illustrated by the decision of the Kenya Film Classification Board to restrict distribution of the ‘Rafiki’ film on the basis that it violated Kenyan social mores for promoting homosexuality. It is important to note that such content restrictions are a limitation of the right to freedom of expression, and will only be permissible if the state can demonstrate that the limitation pursues a legitimate aim that is necessary and proportionate.

Intentional network disruptions have also been noted in the countries under review, for instance in Burundi and Ethiopia. In Uganda, there is important ongoing litigation challenging internet shutdowns in the country, which has the potential to serve as an important judicial precedent in other countries. Although concerns were raised that the Kenyan government would seek to shut down the internet during the 2017 presidential elections, it committed not to.

Privacy and data protection remain matters of concern. While Kenya has, for instance, taken recent steps to develop a comprehensive data protection law, there remain a number of states in the sub-region that have yet to do so. Measures such as mandatory SIM card registration in Burundi and Uganda, for instance, have serious consequences for user privacy. Vast state surveillance powers with low levels of safeguards has also been a trend in the countries under review. For example, the Information and Communications Technologies Law in Rwanda places onerous obligations on private sector actors to cooperate with the state to facilitate surveillance, and the Prevention of Terrorism Act in Kenya provides the state with disproportionate surveillance powers in certain circumstances. Through the recent Computer Crime Proclamation, Ethiopia has served to increase its surveillance powers. In a In a similar vein, recent developments of cyberlaws have also served to increase state surveillance powers, in addition to imposing content restrictions.

However, the recent judgments from Kenya in *Okoiti* and in *Bloggers Association of Kenya* provide precedents that can be used and developed in other countries for future litigation. The judgment in *Okoiti*, in particular, provides some guidance for the checks and balances required by states when undertaking surveillance measures, the need to strictly comply with the three-part test for a justifiable limitation of rights, and the need for meaningful stakeholder consultation. Furthermore, in *Bloggers Association of Kenya*, while the conservatory order suspending the entry into force of 26 sections of the

Computer Misuse and Cybercrimes Act is in itself an important interim measure, the further determination of the constitutionality of the impugned sections in the next phase of the litigation will also potentially provide important guidance in the region.

Concerns regarding threats, harassment and attacks against members of civil society, human rights defenders, journalists and online users have been recorded in all of the countries under review. Although in some countries – such as Ethiopia – the situation has improved under the new political regime – other countries – such as Tanzania and Uganda – have seen the situation worsening. In addition to the personal violations suffered, this also violates the right to freedom of expression more broadly, particularly where they are targeted for public statements made. There is urgent need for rights to be safeguarded in the regard, and for affected persons to be able to be assisted in seeking recourse for the harms that they may have suffered.

Lastly, we note that while digital rights litigation is developing well in countries such as Kenya and Uganda, other countries such as Burundi have had no notable digital rights litigation. However, the regional and sub-regional fora have previously presented opportunities for vindicating the right to freedom of expression, for instance the *Mseto* judgment handed down by the EACJ against the government of Tanzania. These remain important fora for digital rights litigation, particularly in countries where access to the domestic courts is considered limited.

PART III: WEST AFRICA

Selected Countries:
Burkina Faso • Cameroon • The Gambia • Ghana • Nigeria • Sierra Leone

Overview and background

West Africa has seen a stark contrast in different government's approaches to digital rights. States such as Ghana, for instance, have been relatively stable in this regard, and seen as something of a guiding light in the region. Other states, such as Cameroon and the previous regime in The Gambia, have been rife with violations of freedom of expression and other civil and political rights, both in terms of the laws enacted and consistent state practice.

Despite these differences, ECOWAS as a REC has been particularly active and influential. As a point of departure, Article 66 of the Revised Treaty of ECOWAS states as follows:

> "**The Press**
> (1) In order to involve more closely the citizens of the Community in the regional integration process, Member States agree to cooperate in the area of information.
> (2) To this end they undertake as follows:
> (a) to maintain within their borders, and between one another, freedom of access for professionals of the communication industry and for information sources;
> (b) to facilitate exchange of information between their press organs; to promote and foster effective dissemination of information within the Community;
> (c) to ensure respect for the rights of journalists;
> (d) to take measures to encourage investment capital, both public and private, in the communication industries in Member States;
> (e) to modernize the media by introducing training facilities for new information techniques; and
> (f) to promote and encourage dissemination of information in indigenous languages, strengthening cooperation between national press agencies and developing linkages between them."

In addition, more specific to digital rights, the ECOWAS Supplementary Act,[233] together with the Supplementary Act on Transactions Within ECOWAS[234] and the Directive on Fighting Cybercrime within ECOWAS are key to the ICT strategy in the sub-region.[235]

A prime example of the role that ECOWAS plays in the sub-region has been seen through the development of data protection laws. ECOWAS as a REC has the most number of states in Africa that have developed comprehensive data protection laws. Furthermore, the Supplementary Act contains its own provisions for data protection principles that are binding on the ECOWAS member states. This includes, for instance, provision in the Supplementary Act that facilitate data transfers between ECOWAS member states, without being subject to the same requirements as in the case of data transfers to states outside of ECOWAS. ECOWAS, and particularly the francophone states within ECOWAS, has also been actively involved in international data protection bodies that seek to strengthen coordination and implementation of data protection laws.

The ECOWAS Community Court of Justice has also been a key litigation forum for upholding the right to freedom of expression in the sub-region. It was created pursuant to Articles 6 and 15 of the Revised Treaty of ECOWAS, with a mandate to ensure the observance of law and of the principles of equity and in the interpretation and application of the provisions of the ECOWAS Revised Treaty and all other subsidiary legal instruments adopted by ECOWAS. The ECOWAS Community Court of Justice exercises jurisdiction over the following states: Benin; Burkina Faso; Cape Verde; Côte d'Ivoire; The Gambia; Ghana; Guinea; Guinea-Bissau; Liberia; Mali; Niger; Nigeria; Senegal; Sierra Leone; and Togo.

Through its jurisprudence, the ECOWAS Community Court of Justice has consistently upheld the right to freedom of expression. For instance, in *Manneh v The Gambia*,[236] the court found that the arbitrary, incommunicado detention and disappearance of a journalist violated the right to liberty; and the right to a fair hearing. Subsequently, in *Hydara Jr v the Gambia*, the court held that a failure to investigate the killing of Mr Deyda Hydara, a journalist and co-founder of The Point Newspaper in the Gambia, was a violation of the positive obligation to investigate and prosecute arising from the right to life. The court further held that a state will violate international and treaty obligations if it fails to protect media practitioners, including those critical of the regime, as freedom of expression also includes freedom to criticise the government and its functionaries subject to limitations imposed by the law.

Most recently, in *Federation of African Journalists and Others v the Gambia*,[237] the court ordered the government to pay compensation to four journalists for violating their rights and subjecting them to

[233] Accessible at http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

[234] Accessible at https://ccdcoe.org/sites/default/files/documents/ECOWAS-100216-PersonalDataProtection.pdf.

[235] Accessible at: https://ccdcoe.org/sites/default/files/documents/ECOWAS-110819-FightingCybercrime.pdf.

[236] ECW/CCJ/JUD/03/08, accessible at: http://www.chr.up.ac.za/index.php/browse-by-country/the-gambia/306-the-gambia-manneh-v-the-gambia-2008-ahrlr-ecowas-2008.html.

[237] Application No. ECW/CCJ/APP/36/15, accessible at: https://www.mediadefence.org/sites/default/files/blog/files/FAJ%20and%20Others%20v%20The%20Gambia%20Judgment.pdf.

torture, and further ordered the government to immediately repeal or amend its laws on criminal defamation, sedition and false news in line with its obligations under international law.

It also bears mention that – unlike the EACJ – the ECOWAS Community Court of Justice has recently held that, having due regard to international best practices and the provisions of fundamental human rights enforcement procedures of most states, claims for the enforcement of human rights cannot be caught by statutes of limitation.[238] Through this ruling, the ECOWAS Court of Justice has therefore accepted that human rights violations are continuous in nature, and the powers of the court to grant relief should not be impeded by procedural hurdles such as time bars.

The ECOWAS Community Court of Justice has been a receptive forum for freedom of expression litigation in West Africa, and has had a significant impact on the development of the right in the sub-region. Although it has also not been directly confronted with digital rights cases, the freedom of expression jurisprudence thus far is a promising indication of the future of digital rights litigation. It is also hoped that the progressive jurisprudence from the ECOWAS Community Court of Justice will have a positive impact on the domestic courts in the sub-region as well.

Country snapshot

(i) Burkina Faso

Article 8 of the Constitution of Burkina Faso, 1991 and the Information Code, 1993 guarantee freedom of expression, freedom of information and freedom of the press. There have been some positive developments in Burkina Faso since the popular uprising in 2014 that led to the end of the former president's 27-year run in power. The subsequent election campaign was described as having been characterised by critical and diversified media coverage, with independence from the state broadcaster as well.[239]

The Information Code is central to the exercise of freedom of expression and press freedom in the country. While it contains various protections, there are also exceptions that are relied on by the state to avoid giving full effect to the provisions. For instance, while Article 49 of the Information Code grants every journalist free access to sources of information, it also provides for exceptions in cases of internal or external security of the state, military secrets, strategic economic interests, ongoing investigations or legal proceedings, and anything deemed to undermine the dignity and privacy of Burkinabés. These exceptions, broadly drafted in their terms, are often relied on by the state to refuse disclosures.

[238] Federation of African Journalists and Others v the Gambia, Application No. ECW/CCJ/APP/36/15, p 21, accessible at https://www.mediadefence.org/sites/default/files/blog/files/FAJ%20and%20Others%20v%20The%20Gambia%20Judgment.pdf.

[239] Freedom House, 'Freedom of the press 2016: Burkina Faso', accessible at https://freedomhouse.org/report/freedom-press/2016/burkina-faso.

The official media regulatory agency in the country is the High Council for Communication, which actively monitors the media, including online outlets. Concerns have been raised, including that six of its nine members are state appointees, and it has been criticised for inconsistent and mismanaged licensing procedures.[240] Also of concern is that the High Council for Communication has the power to summon journalists to hearings about their work, and to suspend or ban outlets in certain circumstances. In May 2015, for instance, it issued a three-month ban on live radio and television broadcasts of a political nature, with the stated intention to protect social cohesion in the run-up to presidential election; however, this ban was withdrawn later that month after a number of television and radio programs ignored the order.[241]

Burkina Faso is seen as one of the leaders in the region on data protection, having been invited by the Council of Europe to accede to Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.[242] The relevant authorities have also started the process of drafting a law to address the needs of internet users and issues of cybercrime in the country.[243]

Burkina Faso has been the subject of two of the major freedom of expression cases before the African Court. Following these decisions, Burkina Faso has removed imprisonment as a penalty for criminal defamation, but through the same law significantly increased the potential fines that can be imposed if convicted of the offence. The range of fines are between 500 000 and 3 million francs, having been reduced following a critical review of the law from the Constitutional Council. Furthermore, in April 2015, an investigation into the 1998 death of journalist Norbert Zongo was reopened, and in December 2015, three former soldiers of the president's guard were charged with the killing.

Following the change in regime, there has been seen to be a marked decrease in the threats and harassment made against journalists and government critics. However, there have been certain incidents of concern. In January 2017, Ali Mamadou Compaoré, a journalist at the national television station, was assaulted in his neighbourhood by two unknown persons.[244] Prior to the attack, Compaoré had reported receiving telephonic threats. Although no direct connection to the assault has been made, Compaoré was known to be critical of the president of Burkina Faso in his reporting, and the attack was condemned by the Association of Journalists of Burkina Faso.

More recently, in June 2018, Naïm Touré, descried as a cyber-activist, was arrested and detained for criticising the National Gendarmerie on his Facebook page for the alleged neglect of a gendarme who was wounded in the course of duty.[245] The Gendarmerie accused Touré of inciting the armed forces to

[240] Freedom House, n 239.

[241] Freedom House, n 239.

[242] Accessible at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

[243] Media Foundation for West Africa, 'Bi-annual policy brief on internet rights in West Africa: January to June 2018', 2018, p 4, accessible at http://www.mfwa.org/wp-content/uploads/2018/08/Bi-Annual-Policy-Brief-on-Internet-Rights-in-West-Africa-January-June-2018.pdf.

[244] Civicus Monitor, 'Journalist attacked and threatened in Burkina Faso', 16 March 2017, accessible at https://monitor.civicus.org/newsfeed/2017/03/16/burkina-faso/.

[245] IFEX, 'Burkina Faso authorities arrest activist for critical social media posting', 22 June 2018, accessible at https://www.ifex.org/burkina_faso/2018/06/23/activist-arrested/.

revolt and subsequently arrested him.[246] On 3 July 2018, the Court of Ouagadougou sentenced Touré to two months in prison on charges of incitement to revolt.[247] He was acquitted for two other charges, namely demoralisation of the armed forces and conspiracy against the security of the state.[248] The arrest and conviction of Touré has been heavily criticised by civil society organisations in Burkina Faso: on 4 July 2018, eight organisations active in the ICT sector issued the following statement:

> "This conviction lacks elegance for our country and sounds like a democratic retreat and an attack on freedom of expression and opinion in Burkina Faso. We, organizations of the world of ICTs, while recognizing some excesses at times in the use of the social networks, regret this decision of justice."

There has been no notable digital rights litigation in Burkina Faso in the period under consideration. This is likely to have been impacted to some extent by the difficulties experienced by civil society organisations from being able to operate in the country, particularly under the previous regime. The African Court has previously handed down two important judgments against the government of Burkina Faso in matters pertaining to freedom of expression, and remains an important fora to be considered for digital rights litigation as well.

(ii) Cameroon

Cameroon does not have a bill of rights, and treaty law in Cameroon has primacy over national law.[249] As such, Cameroon has a commitment to the right to freedom of expression in terms of, among others, the African Charter and the ICCPR. However, digital rights in the country have been marred by a number of internet shutdowns for lengthy periods of time, affecting millions of people in the country. In this regard, a significant portion of 2017 was spent without internet access.

In the first incident, in two Anglophone regions in Cameroon, the internet was shut down for a period of 94 days from 17 January to 20 April 2017.[250] During this time, the abovementioned sections were widely and repeated broadcast through text messages to subscribers.[251] In response to political protests calling for greater socio-political participation, the internet shutdown followed mass arrests of citizens, particularly journalists and bloggers.[252] According to reports, the national telecommunications and ISP, Cameroon Telecommunications, ordered ISPs in the North-West and South-West regions to completely shut down the internet in these regions.[253] A letter from the Cameroon Telecommunications to the

[246] IFEX, n 245.

[247] Civicus Monitor, 'Blogger Naïm Touré sentenced to two months in prison', 17 July 2018, accessible at https://monitor.civicus.org/newsfeed/2018/07/17/blogger-naim-toure-sentenced-two-months-prison/.

[248] Civicus Monitor, n 247.

[249] MLDI, 'An appalling violation of the right to freedom of speech', 31 October 2017, accessible at https://www.mediadefence.org/news/%E2%80%9C-appalling-violation-right-freedom-speech%E2%80%9D.

[250] AFEX, n 185, p 2.

[251] Paradigm Initiative, n 55, p 15.

[252] Paradigm Initiative, n 55, p 16.

[253] IFEX, '45 days and counting: Cameroon's internet shutdown', 20 November 2017, accessible at https://www.ifex.org/cameroon/2017/11/20/internet-shutdown/; Access Now & Internet Sans Frontières, 'Submission to the

Minister of Posts and Telecommunications that the company "coercively enforced" the government's instructions to suspend internet services "in certain sensitive regions".[254] Two months into the shutdown, Orange Cameroon indicated that it "complies with the local legislation and therefore obeys to any national security instruction received from the authorities in accordance with its Telecommunications License."

Despite a statement in September 2017 by the Minister of Posts and Telecommunications that Cameroon is a country where the rights of citizens, including the right to access and share information on the internet, are guaranteed and protected, a second internet shutdown was reported in October 2017.[255] On this occasion, the government again ordered to the internet to be shut down in the Anglophone regions of the country, with social media sites being inaccessible in the rest of the country as well.[256] Save for intermittent periods of the internet being restored, notably for diplomatic visits, it was only ultimately restored in March 2018, although it remained slow and inaccessible in some parts of the country.[257] This has been one of the longest internet shutdowns recorded on the continent.

In April 2017, Cameroon's Veritas Law Offices, in collaboration with MLDI, instituted two pending cases challenging the internet shutdowns on two fronts: a judicial review before the High Court; and a constitutional challenge before the Constitutional Court under Registration No. 439.[258] Various CSOs have intervened, and the defendants included the government of Cameroon, Cameroon Telecommunications and other ISPs. The matter before the Constitutional Council began on 4 May 2017,[259] and the judicial review began on 17 September 2017. However, there have been a number of delays to date.[260]

The petitioners seek to challenge the shutdowns on the basis of it being a violation of the rights to freedom of expression, access to information, non-discrimination based on language, and hinders economic, social and cultural rights.[261] It is argued that the interference with the internet violates the

UN Human Rights Committee on concerns and recommendations on Cameroon', 20 September 2017, accessible at https://www.accessnow.org/cms/assets/uploads/2017/09/UNHRCommittee-Submission-Cameroon-1.pdf.

[254] Internet Sans Frontières, Access Now & APC, 'Joint submission to the United Nations Human Rights Council Universal Periodic Review: Cameroon', 2018, accessible at https://www.apc.org/sites/default/files/UPR_-_Cameroon_-_2018.pdf.

[255] Access Now, 'United Nations urged to intervene in Cameroon to stop violence and internet shutdowns', 6 October 2017, accessible at https://www.accessnow.org/united-nations-urged-intervene-cameroon-stop-violence-internet-shutdowns/.

[256] Paradigm Initiative, n 55, p 17.

[257] Quartz Africa, 'The internet, slow and sketchy, is back in Cameroon's Anglophone regions – for now', 5 March 2018, accessible at https://qz.com/africa/1221011/the-internet-slow-and-unstable-is-back-in-cameroons-anglophone-regions/.

[258] MLDI, n 249; Access Now, 'Access Now and ISF file legal interventions against Cameroon shutdown', 24 January 2018, accessible at https://www.accessnow.org/access-now-isf-file-legal-intervention-cameroon-shutdown/.

[259] MLDI, 'MLDI and Veritas Law bring case before the Constitutional Council of Cameroon challenging internet shutdown', 4 May 2017, accessible at https://www.mediadefence.org/news/mldi-and-veritas-law-bring-case-constitutional-council-cameroon-challenging-internet-shutdown.

[260] MLDI, n 249; Access Now, n 258.

[261] Quartz Africa, 'Cameroon is being sued for blocking the internet in its Anglophone regions', 30 January 2018, accessible at https://qz.com/africa/1192401/access-now-and-internet-sans-frontieres-sue-cameroon-for-shutting-down-the-internet/.

right to seek, receive and impact information and ideas through digital means, and that a blanket ban is not proportionate and lacks a legitimate aim.[262]

Another serious concern in the country has been in respect of Law No. 2010/012 of 2010 on Cybercrime and Cybersecurity. This was enacted to govern the security framework of electronic communications networks and information systems. In terms of section 25, network operators, ISPs and operators of information systems are required to retain traffic data of their users for at least ten years, and access, service and content providers must also retain data which allows it to identify users for ten years. Section 55 also requires encrypted, encoded and compressed data to be handed over to authorities upon request. Private keys must also be delivered on request of regulated agents and, if unavailable, the judicial authorities may appoint an expert to perform technical operations to obtain the clear version of the data.

The law further imposes a number of content restrictions. For instance, Section 77(i) states that "[w]hoever uses electronic communication or an information system to act in contempt of race or religion shall be punished with prison terms from 2 years to 5 years or a fine of between 2 million to 5 million CFA francs or both". In terms of section 77(ii), the penalties provided for in section 77(i) shall be doubled where the offence is committed with the aim of stirring up hatred and contempt between citizens.

Similarly, in terms of section 78(i), "[w]hoever uses electronic communications or an information system to design, to publish or propagate a piece of information without being able to attest to the veracity or prove that the said piece of information was true shall be punished with a prison term of 6 months to 2 years or a fine of between 5 million and 10 million CFA francs or both". Section 78(ii) provides further that the penalties provided for in section 78(i) shall be doubled where the offence is committed with the aim of disturbing public peace. The law also holds content and service providers, as well as social networks, liable for content hosted on their servers.[263] Furthermore, in terms of section 83, it a crime to propose sex to a person of the same sex by way of electronic communications, and conviction carries a prison sentence of up to 2 years and a fine up to 1 million CFA francs. Cameroonian law plans to double these penalties when the proposals are followed by sex.[264]

Government officials have frequently expressed their frustrations with the use of social media and other websites in Cameroon. Concerns regarding privacy violations have been highlighted following the statement by the Minister of Post and Telecommunications in April 2017 that the country was implementing surveillance programmes to monitor the activities of citizens online.[265] The National Agency for Information and Communication Technologies has also previously detailed how social media and websites are monitored in Cameroon, and that it uses a technical platform that searches for profiles

[262] CIPESA, 'Litigating against internet shutdowns in Cameroon', 4 March 2018, accessible at https://cipesa.org/2018/03/litigating-against-internet-shutdowns-in-cameroon/; Quartz Africa, n 261.

[263] Paradigm Initiative, n 55, p 16.

[264] Access Now & Internet Sans Frontières, n 253.

[265] Internet Sans Frontières, 'Internet back in Anglophone Cameroon, but more surveillance?', 25 April 2017, accessible at https://12internetwithoutborders.org/fr/internet-back-in-anglophone-cameroon-but-more-surveillance/.

on social networks using keywords to detect "illicit content representing a potential threat for the national security and the image of Cameroon".[266] In December 2017, Patrice Nganang was arrested at Douala International Airport as he prepared to board a flight to Zimbabwe for a Facebook post allegedly insulting the President of Cameroon.[267] Although the hearing was scheduled for 14 January 2018, the Attorney General of Yaoundé asked the tribunal to drop all charges against the writer.

There were previous reports that the government was preparing a social media bill in an effort to limit the dissemination of what the government considers as rumours online, but this has been denied by the Minister of Telecommunications and Post.[268] As mentioned above, this is already punished in some measures under the Law on Cybercrime and Cybersecurity.

Privacy concerns have also been raised in respect of the new national identity card and the overhaul of the system of identification. Although the electronic and biometric identity cards are designed to combat fraud,[269] the country does not have a comprehensive data protection framework which leads to concerns regarding the protection of personal information.

The pending challenges to the internet shutdowns that have been experienced in the country will potentially provide important guidance on this issue in Cameroon, and for other countries that have been similarly affected. The permissibility, justifiability and ambit of state power in this regard are matters that are in urgent need of clarity to ensure that users' rights are not violated through future internet shutdowns. These judgments may also serve to inform the state's conduct in respect of social media and users' rights online going forward to ensure that freedom of expression and privacy are respected and upheld.

(iii) The Gambia

The Constitution of The Gambia, 1997 guarantees the right to freedom of expression and press freedom. Under the presidency for former President Jammeh, fundamental freedoms were severely restricted.[270] Under the Jammeh-led government, various laws were amended to provide for increased penalties for certain offences, with other laws being enacted to undermine the right to freedom of expression and media freedom.[271] For instance, the Criminal Code provided for criminal defamation with a minimum prison sentence of one year plus fines, and was further amended in April 2013 to penalise individuals for giving false information to public servants, with a prison sentence of up to five years. Former President Jammeh publicly stated that he would "not compromise or sacrifice the peace,

[266] Access Now & Internet Sans Frontières, n 253.

[267] Internet Sans Frontieres, 'Cameroon: Internet freedoms and democracy activist Nganang is free', accessible at https://internetwithoutborders.org/893-2/.

[268] Internet Sans Frontieres, 'Cameroon's reflection on the 'false news' debate stirs censorship fears', accessible at https://internetwithoutborders.org/cameroonian-governments-dangerous-stance-against-a-free-and-open-internet/.

[269] Gemalto, 'A new national identity card for Cameroon and much more than just a new ID', 28 January 2018, accessible at https://www.gemalto.com/govt/customer-cases/new-national-identity-card-for-cameroon.

[270] Paradigm Initiative, n 55, p 25.

[271] Paradigm Initiative, n 55, p 25.

security, stability, dignity, and the well-being of Gambians for the sake of freedom of expression".[272] Jammeh was defeated in the December 2016 elections by the incumbent Adama Barrow, and the new government promised to protect human rights, including online.[273] Internet users faced increasing restrictions and censorship in the lead-up to presidential elections in December 2016.

Popular messaging apps WhatsApp, Viber, and Skype were blocked for over five months in the lead-up to the elections, with the majority of blocked websites and applications becoming available when the new president assumed office – although gambling and pornography websites remained blocked.[274] There was also a 48-hour internet blackout on the eve of the election, in terms of which the authorities ordered ISPs to shut down internet services, international calls and SMS messaging.[275] Additionally, several online activists were detained without charge for days and subject to ill-treatment in prison prior to elections.[276] During the period of 9 to 21 January 2017, members of civil society were forced to flee the country.[277] Government and newspaper websites were hacked and remained offline for days during an impasse when the former president refused to concede the election.

The conditions for internet and press freedom have improved significantly under the new president.[278] However, the apparatus for blocking content remains in place as state control over the country's dominant telecommunications provider, Gamtel, gives the authorities the ability to restrict access to internet content without oversight. Experts believe that the former government blocked specific IP addresses and domain names at the level of the internet gateway.[279] Procedures for blocking content also remain lacking in transparency; according to former officials, the Jammeh government intentionally avoided issuing written orders for website blockings and internet shutdowns, to maintain a degree of plausible deniability.[280]

The telecommunications sector is regulated under The Gambia Public Utilities Regulatory Authority Act, 2001, in terms of which the Public Utilities Regulatory Authority was established in 2004 to regulate the activities of telecommunication service providers and other public utilities.[281] The Gambia has one of the highest mobile phone penetrations in Africa, but overall internet penetration is low with connection speeds generally being very low when compared to the global average.[282] Cost remains one of the primary hindrances to internet access in the country, as well as a significant urban-rural divide and interruptions to the power supply; the introduction of 3G wireless connections via mobile devices has

[272] The Point, 'President Jammeh meets with the Independent Press', 17 March 2011, accessible at http://bit.ly/1R19tQm.

[273] Freedom House, 'Freedom on the net 2017: The Gambia', accessible at https://freedomhouse.org/report/freedom-net/2017/gambia.

[274] Freedom House, n 273.

[275] Freedom House, n 273.

[276] Freedom House, n 273.

[277] Paradigm Initiative, n 55, p 26.

[278] Freedom House, n 273.

[279] Freedom House, n 273.

[280] Freedom House, n 273.

[281] Paradigm Initiative, n 55, p 25.

[282] Freedom House, n 273.

improved internet accessibility, even though only a small subset of the population can afford the data packages.[283]

The Gambian government's control over the telecommunications infrastructure enables it to restrict access to the internet and mobile phone services with little to no oversight or transparency.[284] The government has also imposed obligations and restrictions on internet café operators. For instance, under an April 2013 directive that remains active, cybercafé owners are required to register with the regulatory agency for an operating license (in addition to a requisite business license) through an application that requires details of the ISP, the number of computers installed, and services provided.[285] Cybercafes must renew their licenses every year and pay annual renewal fees of USD 20 to the regulatory body or face closure. In September 2013, the regulator issued further guidelines that dictated specific requirements on the physical layout of cybercafes and the signs they must display. Since the regulations came into effect, dozens of cafes have reportedly closed down, likely as a result of the economic obstacles imposed by the strict regulations as well as increasing mobile broadband access.[286]

Observers believe the former government proactively monitored and intercepted citizens' communications, particularly the communications of activists and independent journalists who were perceived as threats to national security, as intercepted phone and email communications were often used as evidence in trials against government critics.[287] However, the scope of the government's technical surveillance capabilities remains unknown, and it is uncertain whether the new government has continued to carry out the same surveillance practices.[288]

Unchecked surveillance remains a concern. Article 138 of the Information and Communications Act gives broad powers to national security agencies and investigative authorities to monitor, intercept, and store communications in unspecified circumstances, while also giving the regulator the authority to "intrude [sic] communication for surveillance purposes", all without judicial oversight.[289] In addition, the law requires service providers to "implement the capability to allow authorized interception of communications." Article 141 also obliges service providers to retain metadata for three years. Mandatory SIM card and local domain name registration requirements also still exist.

In December 2015, the former government unveiled plans to set up a new National Cyber Security Strategy that aimed to establish a Computer Incidence Reporting Team to monitor cyber threats.[290] Preliminary documents indicated that the strategy addressed personal data protection, electronic transactions, electronic records and signatures, and computer misuse and cybercrime, all of which are

[283] Media Foundation for West Africa, 'The West Africa internet rights monitor: Monitoring report for April to June 2017', 2017, p 10, accessible at http://www.mfwa.org/wp-content/uploads/2017/09/brochureMFWA17.pdf.

[284] Freedom House, n 273.

[285] Public Utilities Regulatory Authority, 'Internet/cybercafé registration form,' accessible at http://bit.ly/1hsvbjZ.

[286] Freedom House, n 273.

[287] Freedom House, n 273.

[288] Freedom House, n 273.

[289] Freedom House, n 273.

[290] Freedom House, n 273.

currently regulated by Information Communication Act and the Criminal Procedure Act. It is unclear what the future of this is in light of the new regime.

Concern has also been raised about the Official Secrets Act, 1922. For instance, it imposes high fines and imprisonment for publishing confidential information and forces journalists to divulge sources even where the publication is for the public good; furthermore, together with the Oath of Secrecy, it bars public officials from divulging information to the media without authorisation from superiors.[291] Notwithstanding amendments, the Official Secrets Act retains certain seemingly antiquated provisions, such as section 13 which empowers the President to require a person "who owns or controls any telegraphic cable or wire, or any apparatus for wireless telegraphy, used for the sending or receipt of telegrams to or from any place out of The Gambia to produce to him or her, or to person named in the warrant, the originals and transcripts, either of all telegrams, or of telegrams of any specified class or description, or of telegrams sent from or addressed to any specified person or place, sent or received to or from any place out of The Gambia by means of a cable, wire or apparatus, and all other papers relating to any such telegrams".

Furthermore, while there have been positive developments under the new regime, there have also been incidents that have given rise to concern. In February 2018, Ismaila Ceesa, a political analyst and lecturer who has been a prominent critic of the Barrow administration, was arrested, detained, charged and released for comments he made to a local newspaper, which were published both online and in print.[292] Furthermore, a group of soldiers stood trial in 2018 for treason in relation to messages in a WhatsApp group, although little is known about the nature of the allegations and the trial process against them.[293] There have also been reports of violence against journalists, including that of Pa Modou Bojang, an online journalist, who in June 2018 was beaten and detained by members of the Police Intervention Unit while covering a protest, and his digital recorder seized.[294]

There have been important developments in respect of content restrictions in the country. In February 2018, the ECOWAS Court of Justice in the case *of Federation of African Journalists and Others v The Gambia*[295] held that the Gambian laws on libel, sedition and false news disproportionately interfere with the rights of Gambian journalists, and accordingly directed that the Gambia immediately repeal or amend these laws in line with its obligations under international law. The set of laws on sedition, false news and defamation, had been used in the case against four journalists Fatou Camara, Fatou Jaw Manneh, Alhagie Jobe, and Lamin Fatty, who were arrested and tortured by the regime of Yahya Jammeh. The laws were found to have violated freedom of the press and access to information, and the Gambian government was pointed out as having arbitrarily arrested, harassed and detained

[291] International Research and Exchanges Board, 'Media sustainability index 2012', 2012, accessible at https://www.irex.org/sites/default/files/pdf/media-sustainability-index-africa-2012-the-gambia.pdf.

[292] Freedom House, 'Freedom on the net 2018: The Gambia', accessible at https://freedomhouse.org/report/freedom-net/2018/gambia.

[293] Freedom House, n 292.

[294] Freedom House, n 292.

[295] Accessible at https://www.mediadefence.org/sites/default/files/blog/files/FAJ%20and%20Others%20v%20The%20Gambia%20Judgment.pdf.

the journalists, and forced them into exile for fear of persecution as a consequence of their work as journalists. The court declared that, having critically examined the criminal laws of the Gambia, the criminal sanctions imposed on the applicants were disproportionate and not necessary in a democratic society where freedom of speech is a guaranteed right under the international provisions cited.

Thereafter, in May 2018, in the case of *Gambia Press Union and Others v Attorney General*,[296] the Gambian Supreme Court declared that the criminal defamation law and the law on false news on the internet to be unconstitutional. However, in respect of the law on sedition, it was held that the law was only unconstitutional to the extent that a publication relates to government and other public officials, but retained the law in respect of the president. This, however, is not aligned with the decision of the ECOWAS Court of Justice in *Federation for African Journalists*, and it is therefore arguable that any charges of sedition in respect of the President will fall foul of the order of the sub-regional court.

Although these cases did not deal directly with digital rights, they nevertheless have important implications for the exercise of freedom of expression online, as these content restrictions applied equally to online users as they did offline. During the previous regime, civil society organisations, human rights defenders and the media faced serious challenges within the country, as is highlighted by the ECOWAS Court in the *Federation for African Journalists* judgment. This also resulted in many having to leave the country. Under the new regime, there are indeed better prospects for digital rights litigation within the country. The ECOWAS Court has also been an important fora for litigants seeking to vindicate their rights against the government of The Gambia. Furthermore, The Gambia is the most recent country to enter a declaration in terms of Article 34(6) of the African Court Protocol to permit individuals and NGOs to file cases before the African Court, which therefore also presents the African Court as another possible fora for litigation.

(iv) Ghana

Ghana's Constitution of 1992 guarantees freedom of expression and access to information. As at 2016, Ghana had an internet penetration rate of approximately 28.4%.[297] Despite increases in internet penetration, there remains a digital gap between urban and rural areas, the cost of data services is quite expensive for many people, and challenges relating to digital literacy and online violence keep many women offline.[298] A 2016 report published by the World Wide Web Foundation indicates that less than 20% of women in Ghana have access to the internet.[299]

Ghana was one of the first countries in Africa to connect to the internet, and has one of the most vibrant and competitive telecommunications markets in Africa that has seen a lot of growth and development in its internet environment.[300] There are currently six mobile service operators in the country: Scancom

[296] SC Civil Suit No. 1/2014, accessible at https://www.mediadefence.org/news/gambia-mixed-result-supreme-court-delivers-judgment-important-constitutional-challenges-free.

[297] Internet Live Stats, 'Internet users by country (2016)', 2016.

[298] AFEX, n 185, p 9.

[299] World Wide Web Foundation, 'Women's rights online report card: Ghana', 2016.

[300] AFEX, n 185, p 14; Media Foundation for West Africa, n 283, p 7.

(MTN); Vodafone; Bharti Airtel; Globacom (GLO); Millicom (TIGO); and Expresso.[301] There are three other ISP companies that provide Wi-Fi services and data bundle services in the country.[302] Ghana is considered to have a relatively competitive telecommunications market.[303]

In 2016, ahead of the presidential elections, the police administration threatened to shut down social media. However, this received significant outcry, and resulted in the administration at the time assuring the public that social media would not be shut down.

Ghana's internet landscape is guided by several provisions in a number of legal frameworks, including the Electronic Communications Act 775 of 2008, the Electronic Transactions Act 771 of 2008, the Data Protection Act 843 of 2012 and Anti-Terrorism Act 762 of 2008, as well as a National Cyber Security Policy and Strategy to combat cybercrime and other internet-related crimes in the country (although this has not as yet been implemented).[304] Ghana also has a well-established and respected data protection framework.[305]

There are, however, aspects of concern. This includes, for instance, section 60 of the Data Protection Act, 2012 that allows the government to access personal data of individuals without a warrant or judicial approval in the interest of protecting national security.[306] Furthermore, section 208 of Criminal Code provides that "any person who publishes or reproduces any statement, rumour or report which is likely to cause fear and alarm to the public or disturb the public peace, knowing or having reason to believe that the statement, rumour or report is false is guilty of a misdemeanour."[307] The provision requires the publisher to have taken "reasonable measures to verify the accuracy of the statement, rumour or report" before publishing.[308]

Ghana has high incidences of cybercrime.[309] The country has been the subject of a number of cyber-attacks aimed at government agencies, ministries and financial institutions, including a December 2016 cyber-attack that targeted the Electoral Commission's website during an election.[310] The Electronic Communications and Transactions Act, 2009 limits the liability of intermediaries for hosting, caching, linking or mere conduits.

In terms of the Anti-Terrorism Act, 2008, a senior police officer, with the written consent of the Attorney-General and the Minister of Justice, may apply to a court for an order to require the interception of

[301] AFEX, n 185, p 6.

[302] AFEX, n 185, p 6.

[303] AFEX, n 185, p 6.

[304] AFEX, n 185, p 8.

[305] AFEX, n 185, pp 14-15; Government of Ghana, 'Ghana commended for enacting data protection law', undated, accessible at http://www.ghana.gov.gh/index.php/media-center/news/2370-ghana-commended-for-enacting-data-protection-law.

[306] AFEX, n 185, p 8.

[307] CIPESA, n 25, p 19.

[308] CIPESA, n 25, p 19.

[309] AFEX, n 185, p 9.

[310] AFEX, n 185, p 10.

communications for the purpose of obtaining evidence of commission of an offence under the law. However, under section 100 of the Electronic Communications Act, the President is permitted to make written requests and issue orders to operators or providers of electronic communications networks or services requiring them to intercept communications, provide any user information or otherwise in aid of law enforcement or national security. It has been noted that the framework under the Anti-Terrorism Act provides several oversight mechanisms, unlike the latter procedure under the Electronic Communications Act which lacks sufficient oversight as the exercise of such powers are exclusively at the President's discretion.[311]

The National Media Commission (Content Standards) Regulations, 2015 (Legislative Instrument 2224), whose operation was halted by the Supreme Court, would have presented a challenge for media freedom had it been passed as it required broadcasters to seek authorisation from the National Media Commission before broadcasting content on any public electronic communications network, public electronic communications service and broadcasting service.[312]

In general, freedom of expression, access to information and privacy rights are largely respected.[313] However, there have been some incidents of concern. For instance, a graduate of the Kwame Nkrumah University of Science and Technology, Jones Kyei Nyarko, was arrested for having threatened in a Facebook post to kill the US Ambassador to Ghana, Robert Porter Johnson. Nyarko was arrested in January 2016, and later arraigned before an Accra High Court, during which he pleaded not guilty. Further, in April 2017, a young female police officer made comments on Facebook which was thought to be disparaging of the people of Wa in the Upper West Region of Ghana. She was consequently summoned by the Inspector General of Police.

Although there has been some litigation, such as the decision of the Supreme Court to halt the operation of the National Media Commission (Content Standards) Regulations, there has not been any notable digital rights litigation in Ghana. It should be noted that Ghana is generally considered to respect digital rights, with there being a high degree of internet freedom in the country.

(v) Nigeria

Sections 37 and 39 of Nigeria's Constitution of 1999 guarantees fundamental human rights and freedoms of citizens including freedom of expression and access to information.[314] As at 2016, Nigeria had an internet penetration rate of approximately 46.1%.[315] Increasing access to the internet is driven by affordable data services for mobile subscribers.[316] However, on the flipside, power cuts frequently

[311] CIPESA, n 25, p 32.

[312] CIPESA, n 25, p 22.

[313] AFEX, n 185, pp 14-15.

[314] AFEX, n 185, p 26.

[315] Internet Live Stats, 'Internet users by country (2016)', 2016.

[316] Freedom House, 'Freedom on the net 2017: Nigeria', accessible at https://freedomhouse.org/report/freedom-net/2017/nigeria.

disrupt service and access that also undermines the quality of internet service.[317] There is also a significant digital gender divide in the country, as well as challenges in respect of language literacy.[318] The Internet Service Providers Association of Nigeria (ISPAN) was formed in 2001.[319] The main ISPs operating in Nigeria include MTN, Globacom, Airtel, MainOne, Swift, Spectranet, Smile and 9Mobile.[320] Nigeria's internet infrastructure has grown significantly over the past 10 years.[321] A robust civil society has helped to protect and enhance internet freedoms for Nigerians.[322]

There has been one instance of a network disruption that occurred in 2013, when the Nigerian military shut down mobile telephone services in three states in Nigeria as part of its counter-terrorism operations against Boko Haram.[323] Although the military claimed that its objectives were met, concerns have nevertheless been raised that the measure cut off internet access for most Nigerians in the north-east region and terrorist activities continued during the period in which the internet was shut down.[324] It has been reported that, relying on section 146 of the National Communications Act, 2003, the government has made efforts to take down websites and blogs that the government deems to be offensive, under the guise of national security.[325] In November 2017, it was revealed that service providers had blocked 21 websites – including the Naij.com news outlet, with the blocking order reportedly having come from the national security adviser.[326] However, the complex nature of Nigeria's internet infrastructure makes it difficult to carry out systematic filtering or censorship.[327]

There are a number of proposed pieces of legislation aimed at regulating online behaviour.[328] Most notably, the Digital Rights and Freedoms Bill is considered a favourable bill, supported by civil society in Nigeria, and has been passed by the Senate.[329] The core objective of the Digital Rights and Freedoms Bill is to protect the fundamental freedoms of every Nigerian online, and touches on aspects relating to the current digital environment, including data privacy, lawful interception, surveillance, e-governance, and freedom of information, opinion and expression online.[330] The Digital Rights and Freedom Bill is now awaiting presidential assent to become law; when passed into law, it will be the country's first

[317] Freedom House, n 316.

[318] Freedom House, n 316.

[319] AFEX, n 185, p 26.

[320] Paradigm Initiative, n 55, p 38.

[321] AFEX, n 185, p 32.

[322] Freedom House, n 316.

[323] AFEX, n 185, pp 31-32.

[324] AFEX, n 185, p 32.

[325] Paradigm Initiative, n 55, p 39.

[326] Freedom House, 'Freedom on the net 2018: Nigeria', accessible at https://freedomhouse.org/report/freedom-net/2018/nigeria.

[327] AFEX, n 185, p 27.

[328] AFEX, n 185, p 27.

[329] Web Foundation, 'Web Foundation urges Nigeria to turn Digital Rights and Freedoms Bill into law', 24 July 2018, accessible at https://webfoundation.org/2018/07/web-foundation-urges-nigeria-to-turn-digital-rights-and-freedoms-bill-into-law/; Digital Watch Observatory, 'Nigerian Senate passes Digital Rights and Freedom Bill', 13 March 2018, accessible at https://dig.watch/updates/nigerian-senate-passes-digital-rights-and-freedom-bill.

[330] AFEX, n 185, p 30.

specific law on digital rights and internet freedoms.[331] Experts have called for the replication of Nigeria's Digital Rights and Freedom Bill by other African countries.[332]

Other legal frameworks have given rise to concern. In July 2017, following a meeting on 'Hate speeches, fake news and national unity', the National Council on Information recommended setting up a council to regulate the use of social media.[333] Thereafter, in May 2018, the Senate proposed a broadly worded Hate Speech Bill, which seeks to eliminate hate speech on the grounds of ethnicity, religion or race, amongst other grounds; the Hate Speech Bill also seeks to establish an Independent National Commission for Hate Speeches, whose mandate would be to enforce hate speech laws across the country.[334] The Hate Speech Bill would impose extreme sanctions, including a death sentence for any person found guilty of any form of hate speech that results in the death of another person.[335]

Furthermore, a draft Lawful Interception of Communications Regulation introduced by National Communication Commission is still under discussion and if implemented, would enable interception both with and without a warrant under different circumstances, and would require mobile phone companies to store voice and data communications for three years.[336] Although leaked information has revealed the government's acquisition of mass surveillance equipment, the extent of the government's capabilities are not yet known.[337]

Nigeria already enforces mandatory SIM card registration, which is of particular concern in the absence of a comprehensive data protection law.[338] While the lack of an overarching data protection law is of concern, the abovementioned Digital Rights and Freedoms Bill does contain certain data protection provisions.[339] Data localisation is mandated under the Guidelines for Nigerian Content Development in Information and Communications Technology, issued by the Nigerian National Information Technology Development Agency in 2013, which requires ICT companies to "host all subscriber and consumer data locally within the country."[340] While the stated aim is to boost local content and ICT development, but the requirement risks compromising user privacy and security, given the absence of adequate data protection laws.[341] The extent to which the guidelines have been enforced remained unclear as there have been no reports that international ICT companies have been compelled to comply.[342]

[331] Media Foundation for West Africa, n 243, p 4.

[332] IT Web Africa, 'Nigeria's digital rights bill sets example for Africa say experts', 26 April 2018, accessible at http://www.itwebafrica.com/ict-and-governance/265-nigeria/244150-nigerias-digital-rights-bill-sets-example-for-africa-say-experts.

[333] AFEX, n 185, p 32.

[334] Media Foundation for West Africa, n 243, p 9.

[335] Media Foundation for West Africa, n 243, p 9.

[336] AFEX, n 185, p 29.

[337] Freedom House, n 316.

[338] Freedom House, n 316.

[339] AFEX, n 185, p 29.

[340] AFEX, n 185, p 29.

[341] AFEX, n 185, p 29.

[342] AFEX, n 185, p 29.

The government has also announced its plans to launch two communications satellites that have the capability to conduct mass surveillance over citizens.[343] The government has further announced its plans to review legislation granting oversight over print and online publications and to seek to register media houses.[344]

In March 2016, the government introduced the Communication Service Tax Bill which, if passed, will impact the affordability of internet access by imposing a 9% tax on consumers for communications services, such as SMS, data, and voice services.[345] Further, in 2017, it was announced that the nation's security agencies and military authority had commenced monitoring social media for incidents of hate speech and incitement that threatens the unity of the country.[346] Despite having received a lot of criticism from civil society, the government is yet to reconsider its decision.[347]

In addition to these proposed laws, the existing Cybercrime Act, 2015 has given rise to particular concern, especially that it is being vigorously used to target citizen journalists and social media critics of the government.[348] For instance, under section 7 of the Cybercrime Act, cybercafés must make their registers available to law enforcement personnel whenever needed, with no express requirement for judicial oversight. Cybercafés are also required to obtain licenses, but the large number of unlicensed cybercafés in operation suggest that the regulator has not enforced the requirement.[349] An October 2013 directive from the regulator requires cybercafes to maintain an up-to-date database of subscribers and users, including their full names, physical addresses, passport photos, and telephone numbers.[350]

Sub-sections 24(a) and 24(b) of the Cybercrime Act impose harsh penalties that violate the right to free expression under the guise of ensuring national security. Furthermore, there have been a number of arrests on charges of 'cyberstalking' for online writings that criticised government officials and powerful or influential individuals,[351] although none of these cases has led to a conviction.[352] In January 2017, a high court ruled against Paradigm Initiative, Media Rights Agenda and Enough Is Enough Nigeria, which had sought to challenge the constitutionality of sections 24 and 38 of the Cybercrime Act. The court ruled that the impugned sections were not unconstitutional.[353] An appeal has been lodged at the Appeal Court.

[343] Paradigm Initiative, n 55, p 38.
[344] AFEX, n 185, p 32.
[345] Freedom House, n 316.
[346] Paradigm Initiative, n 55, p 38; Media Foundation for West Africa, n 243, p 9.
[347] Media Foundation for West Africa, n 243, p 9.
[348] AFEX, n 185, p 30.
[349] Freedom House, n 316.
[350] Freedom House, n 316.
[351] AFEX, n 185, p 31.
[352] Freedom House, n 316.
[353] Paradigm Initiative, n 55, p 39.

The documented incidents against online users include the following:[354]

- In November 2016, Aku Obidinma, a radio broadcaster, was held in detention for a period of 60 days for Facebook posts criticising the Imo state government.[355]
- In January 2017, Jerry Edoho, a journalist with Ibom Nation newspaper, was arrested by the police for sharing a post on Facebook alleging a plane crash by one of Nigeria's airplanes.
- That same month, the offices of Premium Times, a news website, were raided by the Nigerian police after defamation complaints of the legal representatives of the Chief of Army staff. Both the publisher and the judiciary correspondent were arrested, and a search of the premises was reportedly conducted without a warrant.
- Further in February 2017, Audu Maikori, a businessman, was arrested for tweets he posted on the Southern Kaduna killings in Northern Nigeria. Maikori had withdrawn and apologised for the false claims in his tweets, stating that he was misled by his source. A Federal High Court in Abuja ordered the Governor of the Kaduna state and the police to pay Maikori to pay 40 million naira as compensation for the illegal arrest.
- In March 2017, the police arrested Kemi Olunloyo, a blogger, for an Instagram post that made allegations of infidelity against a Nigerian pastor.
- Also in March 2017, Gambo Saeed was sentenced to nine months' imprisonment by a magistrate court for defaming the governor of Katsina state.
- In April 2017, Austin Okai was arrested for his social media posts considered to be unacceptable by the Kogi State government, and Midat Joseph, Bureau Chief of the Leadership Newspaper was arrested for alleged incitement on a WhatsApp group that called for protests against the killing of civilians.
- In June 2017, Frank Utoo was arrested in Abuja for comments made on Facebook where were deemed to be insulting by a prominent political leader, and Danjuma Katsina, a journalist, was arrested over comments questioning the legitimacy of a newly elected member of Nigeria's House of Representatives. Katsina was released after one day and given no reasons for his detention.
- In July 2017, Biodun Baba, a primary school teacher, was arraigned before a magistrate court for allegedly insulting the Senate President on Facebook, although the charges were withdrawn.
- In August 2017, Johnson Musa was arrested by State Security Service operatives for posting an image of the state governor's residence in Abuja in a WhatsApp post, together with comments that were deemed inappropriate by the authorities.

On 1 January 2018, Nigerian security forces detained two journalists, Timothy and Daniel Elombah, the editor and chief executive of the independent *Elombah* news website, over an allegedly defamatory article about the Nigerian Inspector-General of Police.[356] The authorities released Daniel Elombah the same day he was arrested; Timothy Elombah was released on 500,000 naira bail after spending 25

[354] Paradigm Initiative, n 55, p 39; Freedom House, n 326.

[355] Paradigm Initiative, n 55, p 39.

[356] IFEX, 'Nigeria: Publisher Daniel Elombah released, but Tim Elombah remains in police custody', 11 January 2018, accessible at https://www.ifex.org/nigeria/2018/01/11/arrests-elombah-brothers/; CPJ, 'Two Nigerian journalists charged with cybercrime', 27 February 2018, accessible at https://cpj.org/2018/02/two-nigerian-journalists-charged-with-cybercrime.php.

days in police custody.[357] On 1 March 2018, the two were charged with cybercrime, despite the Vice-President, Yemi Osibanjo, querying the Inspector-General of Police over the arrest and detention.[358] In an instance of positive redress, a high court in Abuja awarded 5 million naira against the Nigerian police force over the arrest and detention of the two journalists, and further granted an injunction against the respondents from arresting and restraining the movement of the applicants.[359]

On 29 May 2018, a blogger, Saint Mienpamo, reportedly escaped death when persons suspected to be militants broke into his house.[360] According to reports, the suspected militants went to the blogger's house with two policemen under the guise of effecting his arrest over a blog post dealing with an alleged attack on the boat of a former militant leader and recent Caretaker Chairman of Southern Ijaw Local Council, Joshua Machiver, by suspected members of the State Waterway Security. Mienpamo was beaten by his attackers, and thereafter taken to the house of a militant leader where he was threatened with death. The incident has since been reported at the Ekeki Police station.

(vi) Sierra Leone

While the Constitution of Sierra Leone, 1991 protects the right to freedom of expression, an amendment has been proposed to include a chapter titled 'Information, communication and the media'. Its stated aim is to bring about an independent media, both online and offline, and guarantees the freedom and independence of the media, with the exclusion of propaganda for war, incitement to violence, hate speech or advocacy for hatred. The Constitution Amendment Committee has recommended the establishment of an 11-member media regulatory body.[361]

Access to the internet in markedly low in Sierra Leone, with an internet penetration rate of 2.4% of the population at 2016.[362] ISPs operating in Sierra Leone include Airtel, Africell, AFCOM, Smart, Sierratel, Onlime and Diakem.[363]

Elections were held in the country in February 2018. Preceding the elections, the government launched a nationwide campaign to educate citizens against the 'misuse' of social media, with 24 000 people reportedly being deployed across the country to support this effort.[364] During the elections, several reports show that the authorities in the country shut down the internet and disconnected mobile communication services after the elections ended on 31 March 2018 in a presidential run-off.[365]

[357] Committee for the Protection of Journalists, 'Two Nigerian journalists charged with cybercrime', 27 February 2018, accessible at https://cpj.org/2018/02/two-nigerian-journalists-charged-with-cybercrime.php.

[358] Media Foundation for West Africa, n 243, p 6.

[359] Media Foundation for West Africa, n 243, p 9.

[360] Media Foundation for West Africa, n 243, p 7.

[361] Paradigm Initiative, n 55, p 39.

[362] Internet Live Stats, 'Internet users by country (2016)', 2016.

[363] Paradigm Initiative, n 55, p 43.

[364] Paradigm Initiative, n 55, p 43.

[365] AFEX, 'Sierra Leone joins global trend: Shuts down internet and mobile services during elections', 2 April 2018, accessible at http://www.africafex.org/digital-rights/sierra-leone-joins-global-trend-shuts-down-internet-and-mobile-services-during-elections__trashed.

According to ISPs, this was done in an effort to stop the Electoral Commission and others from disseminating the elections results.[366]

There are a number of laws that have led to cause for concern in respect of the enjoyment of freedom of expression. In 2016, Sierra Leone appeared poised to introduce restrictive measures to curtail social media use, with a series of meetings being held between National Telecommunications Commission, lawmakers and state security professionals to propose legislation to govern the 'irresponsible use' of social media.[367] It appears that this law has since been reconsidered, with a senior official from the Ministry of Information and Communication statin that: "[W]e do not want the international community coming in and saying we are harassing people".[368] Since the decision to halt this law, the monitoring of WhatsApp groups has reportedly become commonplace amongst the authorities, seemingly both to obtain evidence for prospective prosecutions and to keep their finger on the pulse of online discussions.[369]

However, the Public Order Act, 1965 remains on the statute books and criminalises the publication of materials with the intent to incite the public. Concerns have been raised that the legislation is vaguely worded, and has been abused to imprison journalists and activists over the years.[370] In 2016, Theresa Mbomaya was arrested for forwarding a message in a WhatsApp group promoting an upcoming demonstration and implying that any vehicle trying to disrupt the demonstration could be set on fire.[371] She was detained for five days, but following protests around the courthouse calling for her release, media criticism of the government response and a volunteer coalition of 32 lawyers, her release was successfully negotiated.[372] This was, in part, what led to the government reconsidering the proposed legislation regulating the use of social media.

However, the following year in July 2017, Francis Josiah appeared in court on six charges of defamatory libel for an allegedly offensive WhatsApp post against the family of the Minister of Information, for which he was granted 100 million leones bail.[373] In a positive development, it appears that Sierra Leone may repeal their criminal defamation laws, with the Minister of Information-designate having assured journalists that the country's criminal and seditious libel laws would be abolished under his tenure.[374] However, this is not the first time that a promise has been made to repeal these provisions.[375] It is also

[366] Paradigm Initiative, n 55, p 39.

[367] Mail & Guardian, 'How Sierra Leone polices social media', 28 May 2018, accessible at https://mg.co.za/article/2018-05-28-how-sierra-leone-polices-social-media.

[368] Mail & Guardian, n 367.

[369] Mail & Guardian, n 367.

[370] Paradigm Initiative, n 55, p 39.

[371] Mail & Guardian, n 367.

[372] Mail & Guardian, n 367.

[373] Paradigm Initiative, n 55, p 44.

[374] IFEX, 'On digital rights, States and citizens stake opposing claims: May in Africa', 7 June 2018, accessible at https://www.ifex.org/africa/2018/06/07/digital-space/; Journal du Cameroun, 'Sierra Leone: Information Minister-designate vows to repeal criminal libel law', 4 May 2018, accessible at https://www.journalducameroun.com/en/sierra-leone-information-minister-designate-vows-to-repeal-criminal-libel-law/.

[375] Journal du Cameroun, n 374.

not a complete answer to the concerns raised, as other concerning provisions remain, including the offence of publishing false news for which journalists have been arrested in the past.[376]

There has been no notable digital rights litigation in the period under consideration, although the support shown to Theresa Mbomaya following her arrest for forwarding a message in a WhatsApp group promoting is notable. There are a number of hurdles faced by CSOs seeking to operate in Sierra Leone. In this regard, there is a new policy that recently entered into force that may have a detrimental impact on CSOs. This was raised by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and the UN Special Rapporteur on the Situation of Human Rights Defenders.[377] This likely impacts on the vindication of digital rights in the country, as well as other fundamental rights more broadly.

Concluding observations

As with East Africa, there are certain trends in the opportunities and challenges experienced by the countries under consideration in the sub-region. There have been certain positive developments that are noteworthy, such as the Information Code in Burkina Faso that grants various protections for freedom of expression and press freedom, and the Digital Rights and Freedoms Bill in Nigeria that seeks to safeguard digital rights. These frameworks can be replicated in other countries to develop rights-based laws pertaining to the internet.

However, there have also been concerning developments. For instance, several countries have undergone intentional network disruptions, including total internet shutdowns. For instance, members of the public in Cameroon were without internet access for a significant portion of 2017. Reports of internet shutdowns in The Gambia and Sierra Leone were also noted, particularly during election periods. In The Gambia, it has been noted that despite the regime change, the apparatus for blocking content remains in place as state control over the country's dominant telecommunications provider gives the authorities the ability to restrict access to internet content without oversight. This highlights the need for private sector accountability, in addition to constraints on the exercise of public power.

The internet shutdowns are currently being challenged before court in Cameroon. This jurisprudence has the potential to provide an important precedent for other countries that have also been subjected to internet shutdowns to bring similar challenges in their own courts.

Content restrictions remain prevalent in a number of laws in the sub-region, with news laws – such as the Hate Speech Bill in Nigeria – raising new concerns regarding the impact on freedom of expression. The judgments pertaining to The Gambia are important in this regard, as they emphasise the need to comply with the three-part test for a justifiable limitation, including the requirement of proportionality. As

[376] Freedom House, 'Sierra Leone: Freedom of the press 2016', accessible at https://freedomhouse.org/report/freedom-press/2016/sierra-leone.

[377] UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression & UN Special Rapporteur on the Situation of Human Rights Defenders, Reference OL SLE 1/2018, 22 February 2018, accessible at https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_SLE_22.02.2018.pdf.

noted above, the ECOWAS Court held in *Federation of African Journalists* that the laws on libel, sedition and false news disproportionately interfere with the rights of Gambian journalists, and accordingly directed that The Gambia immediately repeal or amend these laws in line with international law obligations. The subsequent decision of the Supreme Court of The Gambia in *Gambia Press Union* declared the laws on criminal defamation, false news and sedition in respect of government and other public officials, although it retained the offence of sedition in respect of the president. These laws are in no way unique to The Gambia, and other countries with similarly restrictive laws that disproportionately infringe the right to freedom of expression – both online and offline – may consider similar challenges.

Cybercrimes and cybersecurity laws have given rise to particular concern in the countries under consideration. For instance, the Law on Cybercrime and Cybersecurity in Cameroon places onerous obligations on ISPs, and further imposes harsh penalties for violations of the content restrictions set out therein. In Nigeria, The Cybercrime Act has been used to target citizen journalists and social media critics of the government, for instance on charges of 'cyberstalking'. There is currently a constitutionality challenge to certain sections of the Cybercrime Act in Nigeria before the Appeal Court, which if successful can provide useful guidance for other countries in the sub-region.

On a related note, surveillance and the monitoring of social media has also been prevalent in the countries under review, without adequate safeguards to ensure the protection of freedom of expression and privacy. For instance, The Gambia does not require judicial oversight for the conduct of surveillance. In Cameroon, the Minister of Post and Telecommunications stated that the country was implementing surveillance programmes to monitor the activities of citizens online. Similarly, in Nigeria, it was announced that the security agencies and military authority had commenced monitoring social media for incidents of hate speech and incitement that threatens the unity of the country. This can have a chilling effect on freedom of expression, and significantly hinder the enjoyment of the right for users online.

In respect of digital rights litigation, there are important challenges pending in Cameroon and Nigeria regarding internet shutdowns and cybercrimes respectively. The regional and sub-regional courts have also been important fora for freedom of expression litigation, for instance in the African Court's *Konaté* judgment against the government of Burkina Faso and the ECOWAS Court's *Federation of African Journalists* judgment against the government of The Gambia. These judgments have both led to the amendment of laws in line with international obligations, as well as secured recourse for the individuals affected. They remain available fora for digital rights litigation.

PART IV: SOUTHERN AFRICA

Selected Countries:
Angola • Botswana • Namibia • South Africa • Zambia • Zimbabwe

Overview and background

SADC as a REC has been less influential than the EAC and ECOWAS in influencing the realisation of freedom of expression or impacting ICT policy development. In general, the SADC region is facing a harsh socio-economic environment, with the general trend across the media landscape has been dwindling media revenues and the downsizing of media operations.[378] SADC has not made any serious effort to address this, and does not appear to have responded in any meaningful way to rights violations being seen in the region.

Although SADC member states have recognised that ICTs are enablers of stronger economic development, and committed through the 2001 Declaration on Information and Communication Technologies to prioritising rural and remote areas, underprivileged urban areas, institutions of learning and other communities of special benefit as a way of bridging the digital divide, internet penetration in SADC remains low.[379] In 2012, SADC also developed a regional infrastructure development plan with the vision of establishing affordable, always-on connectivity for the SADC region, but the objectives set out therein have largely not been met.[380] Similarly, the 2013 SADC Data Protection Model Law,[381] which seeks to ensure the harmonisation of ICT policies, has done little to influence policy in the SADC region.

In general across the region, freedom of expression has suffered significant challenges. The media continues to operate under the weight of repressive instruments that seek to limit the flow of information, control the practice of journalism and the right to establish media houses, as well as criminalise freedom of expression and artistic expression.[382] These challenges are compounded by the fact that the SADC Tribunal has been rendered defunct, and unlike the EACJ and the ECOWAS Community Court of

[378] Zimbabwe Situation, 'Strengthening regional advocacy for media freedom in Southern Africa', 24 April 2018, accessible at https://www.zimbabwesituation.com/news/strengthening-regional-advocacy-for-media-freedom-in-southern-africa/.

[379] Research ICT Africa, n 1.

[380] Research ICT Africa, n 1.

[381] Accessible at https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf.

[382] Newsday, 'Freedom of expression on shaky ground in Southern Africa', 26 April 2018, accessible at https://www.newsday.co.zw/2018/04/freedom-of-expression-on-shaky-ground-in-southern-africa/.

Justice, the SADC Tribunal does not offer any reprieve or redress for individuals seeking to vindicate their rights. As described on the website of the SADC Tribunal:[383]

> "After several judgements ruling against the Zimbabwean government, the Tribunal was *de facto* suspended at the 2010 SADC Summit. On 17 August 2012 in Maputo, Mozambique, the SADC Summit addressed the issue of the suspended SADC Tribunal. The SADC Summit resolved that a new Tribunal should be negotiated and that its mandate should be confined to interpretation of the SADC Treaty and Protocols relating to disputes between Member States."

The current position is that there is a moratorium in place on the appointment or re-appointment of members to the SADC Tribunal, as well as on the receiving of new cases. There is further a 2014 amendment to the revised Protocol of the SADC Tribunal that seeks to preclude individuals from lodging disputes before the SADC Tribunal, limiting this instead to only states. Although this proposed amendment has not received the requisite number of signatures to enter into force, the moratorium has had the same net effect of rendering the SADC Tribunal incapable of receiving complaints of rights violations.

It is unclear when the SADC Tribunal will be in a position to resume its functions, and what form that will take if it does indeed resume. However, even prior to it being rendered defunct, it had not delivered any notable judgments on freedom of expression. It is therefore difficult to predict whether the SADC Tribunal will be a receptive forum for digital rights cases if it does resume, as this will depend in significant part on what powers and jurisdiction the SADC Tribunal has at that stage.

In terms of litigation, certain countries have active litigation organisations working on matters of digital rights, including the Legal Resources Centre in South Africa and Zimbabwe Lawyers for Human Rights in Zimbabwe. While other countries in the sub-region do not yet have active domestic organisations actively engaging on digital rights, there are key organisations working across the sub-region, including the Southern African Litigation Centre and the Collaboration on International ICT Policy in East and Southern Africa.

Country snapshot

(i) Angola

Internet penetration in Angola stood at 23% in 2016 according to the ITU.[384] High costs remain the most significant challenge to access.[385] In Angola's June 2013 report titled 'The commitment of Angola in the communications and IT sector according to the recommendations of the World Summit on the Information Society',[386] it was noted that some of the measures being taken in Angola include the development of government data centres and a technological campus, the implementation of fibre-optic

[383] Accessible at http://www.sadc.int/about-sadc/sadc-institutions/tribun/.

[384] Internet Live Stats, 'Internet users by country (2016)', 2016.

[385] Freedom House, n 392.

[386] Accessible at http://unctad.org/meetings/es/Presentation/CSTD_2013_Ministerial_WSIS_Angola.pdf.

networks, and the building of multimedia libraries. One of the key identified objectives included to ensure connection between all the technological infrastructures of the state. The government has also started a programme called Angola Online, a free Wi-Fi service.[387] A significant development in the landscape has been the reports that the government plans to sell a 45% minority stake in the state-owned telecommunication provider, and hold an auction for a fourth industry operator.[388]

Information rights are contained in Articles 30 to 34 of the Constitution of Angola, 2010. Notably, the Constitution contains extensive provisions on the right to privacy in particular. Further in this regard, Angola was initially punted to be a leader in data protection in the region, with the Personal Data Law 22/11 having become effective in June 2011.[389] However, despite the president having passed Decree No. 214/16[390] in October 2016 to establish the organisational framework for a data protection authority, this body has not as yet been created.

The Electronic Communications and Information Society Services Law 23 of 2011 is the key piece of legislation regulating the online space. In particular, it provides for the rights of citizens to enjoy protection against abuse or violations of their rights through the internet and other electronic means. In 2011, the government announced that it would scrap the proposed cybercrimes legislation amidst consternation regarding its provisions.[391] The law, had it been passed, made it illegal to share information electronically that could destroy, alter or subvert state institutions or damage national integrity or independence, with a prison sentence of up to 12 years.

A number of measures have been enacted in Angola that restrict online freedom of expression. The government has for years been calling for the regulation of social media. Finally, in January 2017, the president enacted a set of new social media laws through the enactment of five pieces of legislation, known as the Social Communications Legislative Package, which enable the government to control and censor critical information online.[392] The five laws comprising the Social Communications Legislative Package are the press law, the television law, the broadcast law, the code of conduct law for journalists, and the statutes of the Angolan Regulatory Body for Social Communication.[393]

In terms of these new laws, the Angolan Regulatory Body for Social Communication has been created, with the power to regulate journalists' conduct and investigate online content producers without judicial

[387] Accessible at https://www.state.gov/documents/organization/265434.pdf.

[388] Business Day, 'Angola wants international investors in state-owned telecoms provider', 1 December 2017 (accessible at https://www.businesslive.co.za/bd/world/africa/2017-12-01-angola-wants-international-investors-in-state-owned-telecoms-provider/.

[389] Accessible at https://media2.mofo.com/documents/Law_22_11_Data_Privacy_Law.pdf.

[390] Accessible at http://www.e-comlaw.com/data-protection-law-and-policy/article_template.asp?ID=1559&Search=Yes&txtsearch=supervisory%20authority.

[391] BBC, 'Angola victory for cyber activists?', 27 May 2011, accessible at https://www.bbc.com/news/world-africa-13569129.

[392] Freedom House, 'Freedom on the net 2017: Angola', accessible at https://freedomhouse.org/report/freedom-net/2017/angola.

[393] Human Rights Watch, 'Angola: Events of 2017', 2017, accessible at https://www.hrw.org/world-report/2018/country-chapters/angola.

oversight and suspend or ban websites that fail to abide by its standards of "good journalism."[394] In terms of the new laws, the Regulatory Body for Social Communication must "organise and maintain a database on behalf of media organisations and companies subject to [its] supervision, to permit assessment of their compliance with the law".

It further has, among others, the following powers: to enforce compliance with professional journalistic ethics and standards; to enforce compliance with any applicable laws, regulations and technical requirements within the scope of its competence; to verify compliance by radio and television operators with both the generic and specific aims and conditions of their respective charters and activities; and to investigate and adjudicate on complaints about potential or actual transgressions of the legal or regulatory norms, both from interested parties and on its own initiative.[395]

The law also gives the Ministry of Social Communication the authority to oversee how media organisations carry out editorial decisions, and to fine or suspend the activities of violators. It also criminalises publication of a text or image that is offensive to individuals. One of the major concerns was that the law would be relied on to silence critics in the run-up to the 2017 presidential elections. Ultimately, however, the elections proceeded with no reported restrictions on internet freedom, and the internet was seen to be the main outlet for critics and opposition parties during the election period.[396] Although the elections proceeded without evidence of online censorship, concerns have still been raised that Angola's internet infrastructure could allow for such censorship to take place, with suggestions that the country's repressive offline media and freedom of expression environment is increasingly reflected online.[397] Moreover, during the election campaign, election observers from the AU and SADC, amongst others, criticised the pro-ruling party coverage by the state media.[398]

In March 2017, the opposition party launched a constitutional challenge to the law before the Constitutional Court, but this has not as yet been finalised; in the meantime, the law remains in force.[399] There is also a pending constitutional challenge to the Penal Code before the Constitutional Court, instituted by the Angolan Journalists Union, regarding criminal defamation and slander that are punishable with fines and imprisonment for up to six months. There is a pending constitutionality challenge against this law before the Constitutional Court.[400] Although not specifically digital rights cases, these pending constitutionality challenges will impact the rights of users both online and offline.

[394] Freedom House, n 392.

[395] Daily Maverick, 'Angola to silence social media with new regulatory body', 16 August 2016, accessible at https://www.dailymaverick.co.za/article/2016-08-16-angola-to-silence-social-media-with-new-regulatory-body/.

[396] Freedom House, n 392.

[397] Open Technology Fund, 'Angola: An emerging battleground for digital rights', 1 February 2018, accessible at https://www.friendsofangola.org/archives/10653.

[398] Human Rights Watch, n 393.

[399] Freedom House, n 392.

[400] Human Rights Watch, n 393.

(ii) Botswana

The right to freedom of expression is contained in section 12 of the Constitution of Botswana. Although Botswana is traditionally seen as an example of a peaceful democracy, concerns have been raised that the state media outlets operate directly under the oversight of the political leadership, and the private media sector struggles to survive and develop economically within a market dominated by government operators.[401] Concerns were also raised following the suspension of judges in 2015 over a petition against the Chief Justice compromised their freedom of expression and the independence of the judiciary.[402]

The Botswana telecommunications market is composed of four main operators: Botswana Telecommunication Corporation, Mascom, Orange and BoFiNet.[403] Botswana's first National Policy for ICT Development was adopted in 2017, in terms of which the main objective was to transform Botswana from a 'factor endowments' economy to an efficient and innovation-driven economy.[404] In 2016, the government of Botswana completed the process of privatising the Botswana Telecommunication Corporation, and publicly listed the company on the national stock exchange.[405] The Botswana Communication Regulatory Authority, in collaboration with the Department of Environmental Affairs, also developed guidelines to facilitate the sharing of communication infrastructure amongst players in the market, which was intended to bring an end the monopoly of the Botswana Telecommunication Corporation in the wholesale market and improve upstream competition.[406]

In Botswana, section 93 of the Penal Code restricts abusive, obscene or insulting language in a public gathering directed towards the President, a member of Parliament or any public officer; section 95 outlaws threatening breach of the peace or violence; section 96 addresses incitement to violence and disobedience of the law; and section 140 addresses writing or uttering words with the intent to wound religious feelings.[407] Although the Penal Code does not expressly state as such, the offences can apply both online and offline.

Section 17 of Botswana's Cybercrime and Computer-Related Crimes Act, 2007 prohibits the unlawful disclosure by service providers of information collected, and provides a maximum penalty of P40,000, or to imprisonment for a term not exceeding two years, or to both. In 2017, the Minister for Defence, Justice and Security indicated that the legislation was in need of amendment and update to deal with

[401] Media4Democracy, 'Botswana: Strengthening media institutions as drivers of democracy', 27 July 2018, accessible at https://media4democracy.eu/botswana-strengthening-media-institutions-as-drivers-of-democracy/.

[402] Amnesty International, 'Suspension of judges in Botswana potentially threatens freedom of expression and judicial independence', 10 July 2017, accessible at https://www.amnestyusa.org/press-releases/suspension-of-judges-in-botswana-potentially-threatens-freedom-of-expression-and-judicial-independence/.

[403] Research ICT Africa, 'Botswana telecommunications limp a decade after policy changes', February 2017, p 1, accessible at https://researchictafrica.net/polbrf/Research_ICT_Africa_Policy_Briefs/2017%20Policy%20Brief%201_Botswana%20.pdf.

[404] Research ICT Africa, n 403, p 2.

[405] Research ICT Africa, n 403, p 2.

[406] Research ICT Africa, n 403, p 2.

[407] CIPESA, n 25, p 14.

modern security concerns, including to deal with matters of online defamation, cyber-harassment, cyber-stalking and revenge pornography.[408]

Botswana is yet to enact the Data Protection and Privacy Bill, 2017 or introduce a freedom of information bill, despite failed attempts to do so.[409]

There have been several sporadic incidents over the last few years. In January 2015, a website belonging to the only private daily newspaper in Botswana, *Mmegi*, was hacked and deleted by unknown culprits.[410] According to the publication, they suspected that hackers wanted to intimidate and delay their business.[411] In January 2016, Mmegi experienced a cyber-attack that destroyed a significant amount of its archived material.[412] Mmegi's editor claimed that the Directorate of Intelligence and Security Services was behind the attack, and that it had been carried out as retaliation for an article claiming that the Directorate on Corruption and Economic Crime had questioned the former head of the Directorate of Intelligence and Security Services about the wealth he had purportedly amassed.[413]

In May 2016, the offices of the Botswana Gazette were raided and three staff temporarily detained over a news report implicating the Botswana Directorate of Intelligence and Security Services and Botswana Democratic Party in corruption.[414] One of the journalists was charged for disclosing information related to an ongoing investigation.[415] Furthermore, Outsa Mokone, an editor of Sunday Standard, was charged with sedition but later acquitted, following a story published in the newspaper alleging that the president was involved in a late-night car crash that was not reported to the police.[416] In September 2016, Botswana security services arrested an individual for allegedly producing and disseminating a satirical digitally-manipulated image of the President.[417]

In March 2017, three journalists from the INK Centre for Investigative Journalism were briefly detained and threatened by plain-clothes security agents in the village of Mosu.[418] The journalists had tried to access the area where the new home of President Khama was allegedly being constructed amid allegations of corruption, and the security agents told them that the building site was a "restricted area" and that they would be shot on sight if they tried to return.

[408] Your Botswana, 'Botswana amends cybercrime law, ammunition bill', 19 November 2017, accessible at https://yourbotswana.com/index.php/2017/11/19/botswana-amends-cybercrime-law-ammunition-bill/.

[409] CIPESA, n 25, p 12.

[410] MISA, 'Botswana: Newspaper website hacked again, and deleted', 26 January 2015, accessible at http://misa.org/issues/free-expression-online/botswana-newspaper-website-hacked-again-and-deleted/.

[411] MISA, n 410.

[412] CIPESA, n 25, p 20.

[413] CIPESA, n 25, p 20.

[414] CIPESA, n 25, p 22.

[415] CIPESA, n 25, p 22.

[416] CIPESA, n 25, p 22.

[417] CIPESA, n 25, p 14.

[418] Amnesty International, 'Botswana 2017/2018', accessible at https://www.amnesty.org/en/countries/africa/botswana/report-botswana/.

On 19 April, the Court of Appeal upheld an earlier decision by the High Court and turned down the application of a teacher who had challenged his dismissal from employment on the grounds that it violated his constitutional right to freedom of expression.[419] The teacher was dismissed after he published an opinion piece in May 2011 on the country's political situation, following a national strike by public sector employees. The teacher was subsequently found guilty at a disciplinary hearing had found the teacher guilty of contravening section 34(a) of the Public Service Act.

Outsa Mokone, editor of the *Sunday Standard*, faces a criminal sedition charge following his arrest in 2014 after publishing articles alleging President Khama's involvement in a road accident.[420] In December 2016, he was released on bail and asked to appear at the magistrate's court every two months and to seek permission before leaving the country. Mokone was charged with "publishing a seditious publication contrary to section 51(1)(c) as read with section 50(1)(a) of the Penal Code; read with Section 332(1) of the Criminal Procedure and Evidence Act." In September 2018, Mokone's attorney confirmed that the state had finally withdrawn the sedition charges against Mokone.[421] Mokone also challenged the constitutionality of section 50 and 51, arguing that it infringed the right to freedom of expression contained in section 12 of the Constitution of Botswana.[422]

Although the cases mentioned above implicated the right to freedom of expression, there has not been any notable digital rights litigation in Botswana during the period under consideration.

(iii) Namibia

Article 21 of the Constitution of Namibia provides for the right to freedom of speech and expression, and freedom of the media.[423] Protections for civil liberties are generally seen to be robust.[424] Although Namibia had been ranked as the most free country in Africa in terms of media freedom by Reporters Without Borders, in 2018 it lost this place to Ghana.[425] Concerns have been raised following the detention of two visiting international journalists and confiscating of equipment, ongoing threats to regulate the media, a Cabinet memorandum to direct government advertising and information primarily to state-owned media, and the absence of the promised law on access to information.[426]

[419] Amnesty International, n 418.

[420] Amnesty International, n 418.

[421] Agence de Presse Africaine, 'Botswana gov't withdraws sedition charges against editor', 3 September 2018, accessible at http://apanews.net/index.php/en/news/botswana-govt-withdraws-sedition-charges-against-editor.

[422] Amnesty International, n 418; Agence de Presse Africaine, n 421.

[423] Accessible at http://www.namibia-1on1.com/namibiaconstitution-1.html.

[424] Freedom House, 'Freedom in the world 2017: Namibia', accessible at https://freedomhouse.org/report/freedom-world/2017/namibia.

[425] Namibian Broadcasting Corporation, 'Namibia loses top ranking on World Press Freedom Index', 25 April 2018, accessible at http://www.nbc.na/news/namibia-loses-top-ranking-world-press-freedom-index.17169; Gwen Lister, 'Namibian media: Mostly free but fragile', 22 March 2018, accessible at https://www.tandfonline.com/doi/full/10.1080/00358533.2018.1448348?scroll=top&needAccess=true.

[426] Namibian Broadcasting Corporation, n 425; Namibia Media Trust, 'Much more needs to be done to consolidate freedom of the media', 3 May 2017, accessible at https://www.nmt.africa/News/16/Much-more-needs-to-be-done-to-consolidate-freedom-of-the-media---NMT.

As described in the most recent ranking by Reporters Without Borders:[427]

> "Namibia's constitution guarantees free speech and protects journalists, but the lack of a freedom of information law continues to obstruct their work. Those who dare to criticize the authorities are often the target of government threats and seek a refuge on the Internet, where they are not subject to control. At the same time, self-censorship is common in the state-owned media. Public order and security legislation is often used to restrict the freedom to inform, while journalists are sometimes the targets of insults or attacks by political parties. Pro-government media receive a large chunk of their revenue available from advertising, which threatens the financial prospects of the privately-owned media and independent news coverage."

In terms of online regulation, in June 2017 the government tabled the Social Media Use Policy in the National Assembly, which was subsequently adopted.[428] This policy outlines guidelines for government officials' use of social media accounts in an official capacity, and further advised on its use outside of official hours.[429] In addition to the policy, the government also published an implementation plan from 2016/17 to 2019/20.[430] Its stated aims include to improve government transparency, participation and interaction with the public. However, concerns have been raised that the implementation of the policy is not feasible, and that most appropriate platform from which a ministry, office or agency should preferably engage the public on the internet is a website of their own which allows for secure communication between the public and the relevant body, and at the same time protects the data sovereignty of the Namibian government and citizens' personal information from falling into the hands of third parties through cyber-attacks.[431]

In 2017, the Namibian Ombudsman undertook a study into racism and discrimination in the country.[432] The study noted that: "Racial name-calling or racial slurs, stereotyping or racial profiling of a person, is not only highly offensive and humiliating, but it also constitutes a violation of a person's right to dignity and equality. Such utterances and their effect are to be viewed against the background of our history of racism and racial abuse. People often offend, stereotype and perpetuate imbalances on the ground of race through interaction with others fuelled by prejudice that has been passed on from generation to generation."[433] In particular, the report of the Ombudsman highlights the Racial Discrimination Prohibition Act 26 of 1991 and the exceptions set out therein – including section 14(2) which exonerates racist language and publication if it is a subject of public interest, part of a public debate and the truth

[427] Reporters Without Borders, 'Namibia: Journalists under control', accessible at https://rsf.org/en/namibia.

[428] Namibian Broadcasting Corporation, 'NA adopts government's Social Media Use Policy and Communication Plan', 14 June 2017, accessible at http://www.nbc.na/news/na-adopts-governments-social-media-use-policy-and-communication-plan.6400.

[429] Paradigm Initiative, n 55, p 28.

[430] Accessible at http://www.nied.edu.na/assets/documents/05Policies/NationalCurriculumGuide/Social_Media_Policy.pdf.

[431] The Namibian, 'Downside of a Social Media Use Policy', 27 June 2017, accessible at https://www.namibian.com.na/166217/archive-read/Downside-of-A-Social-Media-Use-Policy.

[432] Ombudsman: Namibia, 'A nation divided: Why do racism and other forms of discrimination still persist after twenty-seven years of Namibian independence', 2017, accessible at https://www.ombudsman.org.na/wp-content/uploads/2017/11/Report_on_Racism_Discrimination.pdf.

[433] Ombudsman: Namibia, n 432, p 24.

or on reasonable grounds believed to be true; and the exclusion from prosecution if someone contravenes section 11(1) with the intention to improve race relations and to remove racial insult, tension and hatred.[434] In the concluding observations and recommendations, the Ombudsman raises concerns that "the current legal framework does not provide sufficient protection of a person's rights to equality and dignity and equal access to our courts", and calls for the establishment of a simplified court system or tribunal to assist victims of racism, hate speech and similar offences.[435] The Ombudsman further calls for racial slurs that are considered to be highly offensive and inflict racial abuse to be prosecuted as hate speech, rather than *crimen iniuria*.[436]

Concerns have been raised regarding the draft Electronic Transaction and Cybercrime Bill,[437] in order to "provide for a general framework for the promotion of the use of electronic transactions in government services and private contracts; to provide for the legal recognition of electronic transactions; to provide for the admission of electronic evidence; to provide for consumer protection in electronic commerce; to regulate the liability of service providers for actions of their clients; to provide for the protection of critical and important data; to create certain offences; to create certain powers for the investigation of offences and to provide for matters incidental thereto". In particular, concerns have been raised about Chapter 8 regarding cybercrimes and the powers of investigation in criminal matters, notably that it permits unauthorised access to communications, warrantless surveillance and interception, without containing provisions for personal data and privacy protection.[438]

In March 2017, the Communications Regulatory Authority of Namibia announced the enforcement of SIM card registration.[439] However, this process was halted because Part 6 of Chapter V of the Communications Act, which sets out the legal provisions for the registration of SIM cards, had not yet been implemented.[440] However, surveillance more broadly has raised concerns in the country. In particular, while reports have revealed that Namibia has purchased interception and surveillance technologies from British companies, the official stance of the Namibian authorities has been that Part 6 of the Communications Act, 2009 – which authorises telecommunications interception – has not been gazette and operationalised.[441] This raises concerns regarding the legality of interception activities that may be undertaken.[442]

The Editors Forum of Namibia have also made attempts to strengthen online journalism, including through the preparation of the Code of Ethics and Conduct for Namibia Print, Broadcast and Online

[434] Ombudsman: Namibia, n 432, p 21.

[435] Ombudsman: Namibia, n 432, pp 23-24.

[436] Ombudsman: Namibia, n 432, p 24.

[437] Accessible at http://www.mict.gov.na/documents/32978/0/Latest+Copy+of+the+ETC+Bill+%281%29.pdf/0a64ae18-b008-4bab-b86a-ed6adc244d25.

[438] Paradigm Initiative, n 55, p 37.

[439] Paradigm Initiative, n 55, p 28.

[440] Paradigm Initiative, n 55, p 28.

[441] The Namibian, 'The rise of the Namibian surveillance state', 16 February 2018, accessible at https://www.namibian.com.na/174510/archive-read/The-rise-of-the-Namibian-surveillance-state.

[442] The Namibian, n 441.

media.[443] In 2017, various disinformation campaigns were circulating widely online ahead of the Swapo Congress.[444]

As referred to above, in mid-2016 the authorities temporarily detained two Japanese journalists shortly after they interviewed a cabinet minister about Namibia's use of North Korean workers on military construction projects.[445] The journalists were released, and their seized equipment was eventually returned.[446]

There has not been any notable digital rights litigation during the period under consideration. While the country is generally considered to have a high level of internet freedom, there are concerns that have arisen, particularly in respect of government surveillance. As such, there may be opportunities for future digital rights litigation.

(iv) South Africa

Chapter 2 of the Constitution of the Republic of South Africa, 1996 guarantees the rights to freedom of expression, access to information and privacy. As at 2016, South Africa had an internet penetration rate of approximately 52%.[447] Access to the internet is relatively easily accessible in in urban areas and larger cities in South Africa.[448] Access remains a key concern, and various multi-stakeholder initiatives exist to connect the unconnected, including a partnership between the World Economic Forum and the Department of Telecommunications and Postal Services to connect all South Africans to the internet by 2020.[449] South Africa has four South Africa has four mobile operators (MTN, Vodacom, Cell C and Telkom Mobile), and two fixed operators (Telkom and Neotel), with extensive coverage across the country.

High costs remain the most significant barrier to ICT access, both in terms of devices and services. In 2018, the Independent Communications Authority of South Africa published the End-User Subscription Regulations in an effort to implement measures to reduce the cost to communicate. The implementation has, however, been halted pending an interdict application instituted by one of the mobile operators.[450] Enquiries into the cost of data have also been conducted by parliament, the regulator and the competition authorities, with the Competition Commission of South Africa having engaged in public hearings in November 2018.[451]

[443] Namibia Media Trust, n 426.

[444] Namibia Media Trust, 'NMT calls for restraint ahead of Swapo Congress', 20 October 2017, accessible at https://www.nmt.africa/News/24/NMT-calls-for-restraint-ahead-of-Swapo-Congress.

[445] Freedom House, n 424.

[446] Freedom House, n 424.

[447] Internet Live Stats, 'Internet users by country (2016)', 2016.

[448] AFEX, n 185, p 42.

[449] World Economic Forum, 'Internet For All', accessible at https://www.weforum.org/projects/internet-for-all.

[450] Tech Central, 'Cell C seeks urgent interdict against ICASA', 7 June 2018, accessible at https://techcentral.co.za/cell-c-seeks-urgent-interdict-against-icasa/81665/.

[451] Competition Commission of South Africa, 'Data market inquiry', accessible at http://www.compcom.co.za/data-market-inquiry/.

The two key laws government the ICT regulatory framework in South Africa are the Electronic Communications and Transactions Act, 2002 and the Electronic Communications Act, 2005. The Electronic Communications and Transactions Act establishes a formal structure to define, develop, regulate and govern e-commerce in South Africa. This includes, for instance, limiting the liability for ISPs or intermediaries. The Electronic Communications Act seeks to promote convergence in the broadcasting and telecommunications sector, to provide a framework for the convergence of these sectors, and to make new provision for the regulation of electronic communication services.

The Electronic Communications Amendment Bill, which has been submitted to the National Assembly for approval, has the potential to significantly overhaul the ICT landscape in South Africa. In particular, it seeks to introduce a wholesale open access network, in terms of which spectrum will be retrieved from the existing operators and made available to new entrants to the market. This has been met with a mixed response, and significant consternation from the mobile operators.[452] In September 2018, the Department of Telecommunications and Postal Services called for public comment on the proposed policy and policy directions to the regulator on the licensing of unassigned high-demand spectrum.[453] According to the media statement, this followed Cabinet's approval of the study conducted by the Council for Scientific and Industrial Research, which confirmed that a portion of radio frequency spectrum can be assigned to the wholesale open access network, with excess capacity going to the industry.[454]

The Department of Telecommunications and Postal Services had previously interdicted the regulator from auctioning spectrum to expand telecommunications networks, in favour of the publicly-owned model of spectrum allocation.[455] However, in September 2018, the Minister of Telecommunications and Postal Services indicated that a settlement agreement had been reached, in terms of which the regulator would withdraw the invitation to apply and the Minister would withdraw the court challenge.[456]

In addition to the legislative framework, South Africa's ICT policy is detailed in two key policy documents: South Africa Connect,[457] which sets specific targets for connectivity; and the National Integrated ICT

[452] Tech Central, 'The WOAN could succeed, but only if done right', 21 February 2018, accessible at https://techcentral.co.za/woan-succeed-done-right/79712/.

[453] Accessible at https://techcentral.co.za/wp-content/uploads/2018/09/DTPS-Policy-Direction-on-the-licensing-of-High-Demand-Spectrum.pdf.

[454] South African Government, 'Minister Siyabonga Cwele invites public to comment on licensing of unassigned high demand spectrum', 28 September 2018, accessible at https://www.gov.za/speeches/media-statement-minister-telecommunications-and-postal-services-dr-siyabonga-cwele-invites.

[455] Freedom House, 'Freedom on the net 2017: South Africa', accessible at https://freedomhouse.org/report/freedom-net/2017/south-africa.

[456] Ministry of Telecommunications and Postal Services, 'Joint statement: Minister Dr Siyabonga Cwele and the Council of ICASA agree to settle the spectrum court challenge and to initiate the licensing of unallocated high demand spectrum', 26 September 2018, accessible at https://www.ellipsis.co.za/wp-content/uploads/2018/09/Joint-DTPS-ICASA-Media-Statement-on-spectrum-case-Settlement-26-Sep-2018.pdf.

[457] Accessible at http://www.gov.za/documents/electronic-communications-act-south-africa-connect-creating-opportunity-ensuring-inclusion.

Policy White Paper.[458] There is also the e-Government Strategy and Roadmap, that sets out the government's plans in relation to bringing government services online.

In terms of content restrictions, there are certain common law offences that have remained in existence. For instance, criminal defamation is still an offence in South Africa, despite an undertaking by the ruling party to abolish it.[459] Incitement is also an offence in terms of the Riotous Assemblies Act, 1956, although there is currently a constitutionality challenge pending that has been brought by an opposition party leader who faces charges of incitement for statements made to his supporters.[460]

In general, there is a high level of media freedom in the country. However, under the previous president, journalists in the country faced various threats and harassment, both online and offline, as part of attempts by powerful individuals and groups that sought to shape the political and economic landscape through corrupt relationships and deals to benefit their own private interests.[461] In *South African National Editors Forum v Black Land First*,[462] the South African High Court granted an interdict in favour of the media broadly, prohibiting the respondent from "engaging in any of the following acts directed towards the applicants: Intimidation; Harassment; Assaults; Threats; Coming to their homes; or acting in any manner that would constitute an infringement of their personal liberty", and from "making any threatening or intimidating gestures on social media … that references any violence, harm and threat." The court subsequently held the respondent in contempt of court for continuing to engage in certain activities, including the harassment of members of the media, following the interdict having been granted.

At present, the ICT policy landscape in South Africa is in something of a state of flux, which has contributed to significant regulatory uncertainty. Some laws, such as the Copyright Amendment Bill, seek to modernise existing legal frameworks to make it more relevant in the digital age.[463] However, other laws potentially have significant consequences for freedom of expression.

The Films and Publications Amendment Bill, which was passed by the National Assembly in March 2018, has been widely criticised for the potential risk it poses to enabling censorship through the classification regime.[464] n. In particular, it proposes giving wide powers to the Film and Publication Board to regulate user-generated content – including YouTube videos, pictures and music – and to block non-

[458] Accessible at https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/National_Integrated_ICT_Policy_White.pdf.

[459] Dario Milo, 'The timely demise of criminal defamation law', 4 October 2015, accessible at http://blogs.webberwentzel.com/2015/10/the-timely-demise-of-criminal-defamation-law/.

[460] The Citizen, 'Malema land occupation court case postponed to 2019', 27 July 2018, accessible at https://citizen.co.za/news/south-africa/1987425/malema-land-occupation-court-case-postponed-to-2019/.

[461] The Conversation, 'Media freedom remains fragile in South Africa', 18 October 2017, accessible at http://theconversation.com/why-media-freedom-remains-fragile-in-south-africa-85868.

[462] Accessible at http://www.saflii.org/za/cases/ZAGPJHC/2017/179.html.

[463] The Conversation, 'South Africa takes steps to adjust copyright law to the digital age', 6 August 2017, accessible at https://theconversation.com/south-africa-takes-steps-to-adjust-copyright-law-to-the-digital-age-81490.

[464] Freedom House, n 455.

compliant distributors at the ISP level.[465] The next step is for it to be considered by the National Council of Provinces, whereafter it can be submitted to the President for assent.[466] The Film and Publication Board has also proposed revisions to the tariffs and has sought to direct video streaming services to pay a registration fee to distribute content under the self-classification criterion imposed on online distributors by the Film and Publication Board.[467] Although some major content distributors such as Google and Apple had paid the licence fees by the end of 2017, others such as Netflix and Microsoft had not paid.[468] Netflix in particular has lobbied for self-regulation of content on its platform.[469]

A further proposed law that has led to significant concerns is the Prevention and Combatting of Hate Crimes and Hate Speech Bill, if passed, would expand the definition of 'hate speech', and explicitly aims to monitor electronic forms of communication.[470] While concerns have been raised regarding the vague wording and the chilling effect that it may have on freedom of expression, the Bill has been justified in part on the basis following a number of racist social media posts that have gone viral. For instance, in 2016, Penny Sparrow received a R150 000 fine for a racist post she published on Facebook.[471] Thereafter, in March 2018, a magistrate's court sentenced Vicky Momberg to three years' imprisonment, with one year suspended, following a guilty verdict of *crimen iniuria* for racist speech.[472] This was the first time that a sentence of imprisonment has been handed down for *crimen iniuria* in the post-apartheid era in South Africa. More recently, the Equality Court found against Velaphi Khumalo, an employee in the provincial government, who stated on Twitter that: "I want to cleans this country of all white people. we must act as Hitler did to the Jews" (sic) and that "white people in south Africa deserve to be hacked and killed like Jews" (sic). The Equality Court declared the statements to be hate speech, ordered that Khumalo publish a written apology, and referred the matter for consideration by the Director of Public Prosecutions as to whether criminal action should be taken.[473]

This includes the Cybercrimes and Cybersecurity Bill, which among other things, aims to regulate malicious communications such as the distribution of images that are intimate in nature without the consent of the person involved. An earlier version of the Cybercrimes and Cybersecurity Bill had included a provision making it a criminal offence to distribute a harmful data message that is inherently

[465] BusinessTech, 'Parliament has passed the 'internet censorship' bill – here's what it means for you', 8 March 2018, accessible at https://businesstech.co.za/news/media/229911/parliament-has-passed-the-internet-censorship-bill-heres-what-it-means-for-you/.

[466] BusinessTech, n 465.

[467] Freedom House, 'Freedom on the net 2018: South Africa', accessible at https://freedomhouse.org/report/freedom-net/2018/south-africa.

[468] Freedom House, n 467.

[469] BusinessTech, 'Government set on regulate YouTube, Netflix and other streaming services in South Africa', 6 October 2017, accessible at https://businesstech.co.za/news/broadband/203326/government-set-on-regulating-youtube-netflix-and-other-streaming-services-in-south-africa/.

[470] AFEX, n 185, p 47.

[471] Tech Central, 'Penny Sparrow fined R150 000', accessible at https://techcentral.co.za/penny-sparrow-fined-r150-000/65969/.

[472] News24, 'Vicki Momberg sentenced to an effective 2 years in prison for racist rant', 28 March 2018.

[473] Accessible at https://www.politicsweb.co.za/documents/sahrc-vs-velaphi-khumalo-equality-court-judgment.

false, but this has since been removed.[474] While South Africa has a comprehensive data protection law – the Protection of Personal Information Act, 2013 – the substantive provisions of the law are not yet in force, despite having been signed into law in 2013, and the appointment of the regulator in 2016. South Africa has been the subject of a number of massive data breaches in recent years, which has spurred concern for the need to have these laws.[475]

Unlawful surveillance in the country is a significant concern, particularly in respect of the surveillance of journalists.[476] There is currently a constitutionality challenge[477] pending against various provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002.[478] The case has the potential to significantly reform the current surveillance landscape and put in place better oversight mechanisms. The factual basis of the case follows investigative journalist, Sam Sole, having received proof that his communications were intercepted during an investigation, and challenges various provisions of the existing law, including the lack of user notification provisions, the onus for the granting of interception directions, and the lack of regulation over bulk interception. The date for hearing has not been set as yet.

A further case has also been instituted, in this instance by the Right2Know Campaign, against three of the major telecommunications operators in the country – MTN, Cell C and Telkom – seeking details of when and how often they accede to requests from law enforcement and other government agencies to facilitate interception and surveillance.[479] Vodacom is not party to the legal proceedings, after it agreed to supply the information sought under an access to information request in terms of the Promotion of Access to Information Act, 2000. At present, section 42 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act contains a blanket secrecy provision prohibiting the disclosure of information relating to directions issues in terms of the law. The matter is expected to be heard in 2019.[480]

The litigation pertaining to surveillance are amongst the most important digital rights cases in the country at present. These cases will provide much-needed guidance on the constitutionality of the surveillance laws and the necessary safeguards that are required. In general, the courts have a strong record of upholding freedom of expression and privacy. The hate speech cases regarding racist posts on social media have also received significant attention, although concerns have been raised that the lower courts have not been consistent in their decisions and sentences. The courts have also been willing to

[474] IT Web, 'Fake news too hot to handle for Cybercrimes Bill', 1 November 2018, accessible at https://www.itweb.co.za/content/P3gQ2MGXQ4dqnRD1.

[475] Fin24, 'Five massive data breaches affecting South Africans', 19 June 2018, accessible at https://www.fin24.com/Companies/ICT/five-massive-data-breaches-affecting-south-africans-20180619-2.

[476] Right2Know, 'Spooked: Surveillance of journalists in SA', June 2018, accessible at https://cdn.24.co.za/files/Cms/General/d/7622/a417e7e9f1a74853979b36a87b400b07.pdf.

[477] Accessible at http://www.justice.gov.za/legislation/acts/2002-070.pdf.

[478] amaBhungane, 'AmaB challenges snooping law', 20 April 2017, accessible at https://amabhungane.org/advocacy/advocacy-amab-challenges-snooping-law/.

[479] Tech Central, 'Court battle to get Rica data from mobile operators', 7 November 2018, accessible at https://techcentral.co.za/court-battle-to-get-rica-data-from-mobile-operators/84945/.

[480] Tech Central, n 479.

grant interdicts in appropriate cases for online activities, such as in *South African National Editors Forum,* as well as in the matter of *KS v AM* in which the respondent was interdicted from publishing sexual video footage and photographs of the applicant on Facebook.[481]

(v) Zambia

The Constitution of Zambia (Amendment) Act, 2016 was enacted in January 2016, implementing a new constitution. However, the amendments lacked the protection of fundamental rights and freedoms. A constitutional referendum was held in August 2016 alongside general elections to seek voter approval of new amendments to the constitution's bill of rights, which provided specific protections for print, broadcast, and electronic media freedom, and explicitly prohibited the government from exercising control or interfering with media activities.[482] However, despite being approved by 71% of voters, the referendum failed to garner the minimum voter turnout threshold of 50% required to validate the results.[483]

The disputed August 2016 presidential and national assembly elections placed freedom of expression under threat in the country, most notably owing to mobile broadband networks being reportedly disrupted for up to 72 hours in parts of the country with strong opposition support and certain news outlets going offline after accusing the government of election fraud.[484] Two mobile providers – MTN and Airtel – confirmed the disruptions but did not provide a reason, leaving it unclear whether the outage was ordered by the government.[485] A 90-day state of emergency was also imposed to quell rising tensions.[486]

Zambia was among the early adopters of the internet in sub-Saharan Africa with the installation of dial-up and satellite technology at the University of Zambia in the early 1990s, though access has grown slowly ever since. ISPs operating in Zambia include Microlink Solution, CEC Liquid Telecommunications, Zamtel, Iconnect Zambia, Vodafone, CopperNet Solutions, Hai Telecommunications, Paratus Telecom, ZamNET, A Plus Technologies, IWAY Zambia, Preworx Zambia, VSAT Communication Ltd and Massnet Innovation Solutions. The costs involved in ICT ownership and access to internet services are a major barrier to access for the majority of Zambian citizens, especially in rural areas. Concerns have been raised that partial state ownership of the country's fibre backbone and control over connections to the international internet may enable the government to restrict connectivity at will.[487]

---

[481] Accessible at http://www.saflii.org/za/cases/ZAGPJHC/2017/297.html.

[482] Accessible at http://ccmgzambia.org/wp-content/uploads/2016/06/Constitution-of-Zambia-Amendment-Bill-Bill-of-Rights.pdf.

[483] Lusaka Times, 'Referendum vote flops, fails to meet the threshold', 19 August 2016, accessible at https://www.lusakatimes.com/2016/08/19/referendum-vote-flopsfails-meet-threshold/.

[484] Freedom House, 'Freedom on the net 2017: Zambia', accessible at https://freedomhouse.org/report/freedom-net/2017/zambia.

[485] Freedom House, n 484.

[486] Freedom House, n 484.

[487] Freedom House, n 484.

Zambia was also the first country in Sub-Saharan Africa to censor online content in 1996, when the government demanded the removal of a banned edition of *The Post* from the newspaper's website by threatening to hold the ISP, Zamnet, criminally liable for the content.[488] Although intermediaries are not held liable in terms of the Electronic and Communications Act, 2009, there have nevertheless been instances of the government directing online media editors to remove material considered offensive or problematic on request. Concerns have been raised that this has led to a growing level of self-censorship, and have led bloggers and journalists to write anonymously to avoid harassment or threat of legal action.[489]

Zambia's Penal Code contains sections that implicate the right to freedom of expression, including Article 191 87 of the Penal Code and Cap 87 of the Laws of Zambia, which criminalise defamation of the President. In terms of Article 53 of the Penal Code, the president also has a discretion to ban publications regarded as contrary to the public interest. Furthermore, Article 67(1) prohibits the publication of false news which is likely to cause fear and alarm to the public or disturb public peace, and renders an offender liable for three years' imprisonment.

The Electronic Communications and Transactions Act, 2009 is the key ICT law in the country. It provides for a 'notice and takedown' procedure, and places no general obligation on service providers to monitor unlawful activities on their platforms or impose liability for the use of location tools by a service provider.[490] Part X limits the liability of intermediaries for hosting, caching, linking or mere conduits. Of concern, certain provisions provide for sweeping surveillance powers with little to no oversight, including Article 79 requiring service providers to enable interception and store call-related information; Article 77 requiring service providers to install both hardware and software that enable communications to be intercepted in "real-time" and "full-time" upon request by law enforcement agencies or under a court order; and service providers being required to transmit all intercepted communications to a Central Monitoring and Coordination Centre managed by the Communications Ministry.[491]

Zambia also imposes a system of mandatory SIM card registration in accordance with the Information and Communication Technologies (ICT) Act, 2009 and the Statutory Instrument on the Registration of Electronic Communication Apparatus, 2011. According to reports, subscriber details may be passed directly to the secret service for the creation of a mobile phone user database.[492]

In August 2018, Cabinet approved for review the Cybersecurity and Cybercrimes Draft Bill, which had been introduced in April.[493] Concern has been expressed that this law has the potential to infringe on internet freedoms, including providing for penalties of up to one year in prison, fines or both for "any

[488] Freedom House, n 484.

[489] Freedom House, n 484.

[490] CIPESA, n 25, p 25.

[491] Freedom House, n 484.

[492] Freedom House, n 484.

[493] Freedom House, 'Freedom on the net 2018: Zambia', accessible at https://freedomhouse.org/report/freedom-net/2018/zambia.

electronic communication, with the intent to coerce, intimidate, harass or cause substantial emotion distress to a person".[494]

Zambia has yet to enact the Electronic Commerce Bill, 2017 or the Data Protection Bill, 2017.[495] Concerns have been raised about the surveillance capabilities and practices of the state; in July 2017, Thomas Allan Zgambo and Clayson Hamasaka, both journalists, sued the mobile phone company Airtel for intercepting a total of 225 phone conversations between 2013 and 2014 and diverting the calls to a number belonging to state intelligence.[496] In January 2018, the Minister of Transport and Communications stated that the Zambia Information and Communications Technology Authority has the capability to monitor all digital devices in the country, although it has been noted that the evidence of this is lacking.[497] Mandatory SIM card registration has been applied since September 2012.[498] Further of concern to anonymity online, in October 2016 the Zambia Information and Communications Technology Authority raided the premises of a number of ISPs and internet cafés that it accused of operating illegally, which was seen as an attempt to limit online anonymity.[499]

Several individuals were arrested for critical comments made on Facebook, including an opposition politician, a university student, and an independence activist from the minority Barotseland region, marking an increase from years past. In April 2017, Chilufya Tayali, the Economic and Equity Party leader, was arrested and charged with criminal libel under section 191 of the Penal Code, over a post on his Facebook page against the Inspector General of Police.[500] In the post, Tayali accused the Inspector General of Police of "covering up for his inefficiencies when he charged and arrested United Party for National Development (UPND) leader … with treason".[501] In a related case, in May 2017, Patriotic Front Deputy Secretary General Mumbi Phiri sued Asher Hakantu for posting defamatory words on a Whatsapp group, where he alleged Mumbi Phiri came to political prominence through sacrificing her son.[502] Similarly, Edward Makayi was arrested for defamatory remarks against the President and other state officials on a Facebook page under the name of Royson Edwards M, contrary to section 59 of Cap 87 of the Laws of Zambia which prohibits defamation of the President.[503]

In May 2017, Kwalela Kafunya, a Zambian medical doctor, was arrested and charged for defamation, allegedly having disparaged the President on a Facebook account created under a pseudonym.[504] Munyinda Munukayumbwa, an activist from the contentious Barotseland region, was separately arrested on charges of sedition for a Facebook post criticizing the government for marginalising the

[494] Freedom House, n 493.
[495] CIPESA, n 25, p 12.
[496] Freedom House, n 493.
[497] Freedom House, n 493.
[498] Freedom House, n 493.
[499] CIPESA, n 25, p 22.
[500] CIPESA, n 25, p 17.
[501] Paradigm Initiative, n 55, p 51.
[502] Paradigm Initiative, n 55, p 51.
[503] Paradigm Initiative, n 55, p 51.
[504] CIPESA, n 25, p 17.

region.[505] In July 2018, the police arrested a man from the Luapula provice for allegedly defaming the President through derogatory posts across four different Facebook accounts, and charged him with defamation under the Penal Code.[506]

Homosexuality remains a criminal offence in Zambia, which has had an impact on certain content regulation. For instance, January 2018 the Zambian police also announced a search for a lesbian couple after they had shared intimate photographs on Facebook.[507]

There has not been any notable digital rights litigation in Zambia, despite there being certain aspects of the existing legal framework and state conduct that has given rise to concern. As one of the leaders in the adoption of the internet on the continent, Zambia certainly has a potential role to play in ensuring that digital rights are secured for those internet users.

(vi) Zimbabwe

The Constitution of Zimbabwe guarantees the right to privacy, the right to freedom of association and assembly, the right to freedom of conscience, and the right to freedom of expression and the media. As at 2016, Zimbabwe had an internet penetration rate of approximately 21%.[508] Internet access in Zimbabwe is challenged by poor telecommunications and electricity infrastructure, low bandwidth, high cost of internet services and widespread poverty.[509] There is a significant urban-rural divide in Zimbabwe.[510] In an attempt to address the urban-rural digital divide, the government uses the Universal Services Fund to address rural connectivity challenges, and has adopted an infrastructure-sharing policy through Statutory Instrument 137 (2016) to help eliminate duplication of existing and future telecommunication infrastructure to maximise its reach.[511] Zimbabwe's ICT market comprises 16 licensed internet service providers registered with the Zimbabwe Internet Service Providers Association, and include Africom Zimbabwe, Afrihost, Aptics, Clay Bytes Solutions, Econet Wireless, FBNet, Frampol, Liquid Telecom, Powertel, SADACNET, Telco, Telecel, Utande, YoAfrica, ZARnet, and ZOL Zimbabwe.[512] There are also five licensed telecommunication operators, namely, TelOne, NetOne, Telecel, Econet and Africom.[513]

In March 2018, the President launched the National Policy for ICT, which sets out to centralise control over the country's internet backbone.[514] There is also a framework for anticipated cyber laws, such as

[505] Freedom House, n 484.
[506] Freedom House, n 493.
[507] Freedom House, n 493.
[508] Internet Live Stats, 'Internet users by country (2016)', 2016.
[509] AFEX, n 185, p 64.
[510] AFEX, n 185, p 66.
[511] AFEX, n 185, p 67.
[512] Paradigm Initiative, n 55, p 52.
[513] Paradigm Initiative, n 55, p 52.
[514] Freedom House, 'Freedom on the net 2018: Zimbabwe', accessible at https://freedomhouse.org/report/freedom-net/2018/zimbabwe.

the Data Protection Bill, the Electronic Transaction and Electronic Commerce Bill and the Computer Crime and Cyber Crimes Bills.[515] However, concerns have been raised regarding certain clauses, including the centralisation of information storage, management and protection through the establishment of a National Data Centre which will house all internet gateways and infrastructure. In a positive development, the new administration dropped plans to establish a Ministry of Cybersecurity, Threat Detection and Mitigation, which observers had believed was aimed at curbing freedom of expression online.[516]

In respect of the Cybercrime and Cybersecurity Bill, 2017, which was originally introduced in 2013 as the Computer Crimes and Cybercrimes Bill, 2013, this is aimed at curbing cybercrimes in the country. The Cybercrime and Cybersecurity Bill has undergone a process of public consultation. According to its long title, it aims, among other things, to "to provide for and to consolidate cyber-related offences with due regard to the Declaration of Rights under the Constitution and the public and national interest". Concerns have been raised in particular about section 17 of the Cybercrime and Cybersecurity Bill, which criminalised the transmission of false data messages intending to cause harm. In this regard, section 17 provides that "any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes data to any other person concerning an identified or identifiable person knowing it to be false with intent to cause psychological or economic harm shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment".

Concerns have also been raised regarding other laws. For instance, surveillance is governed in terms of the Interception of Communications Act, 2007, Statutory Instrument 142/2013 and the Postal and Telecommunications (Subscriber Registration) Regulation, which make service providers legally liable for the information that travel across their networks, including third party content.[517] Non-compliance or failure to cooperate by service providers is a criminal offence.[518] Furthermore, in terms of section 2 of the Interception of Communications Act, ISPS and telecommunications service providers are required to maintain records of users over a stipulated period, which includes all call-related information, defined as "information that identifies the origin, destination, termination, duration ... of each communication generated or received by a customer or user ... and, where applicable, the location of the user within the telecommunications system". Concern has been raised that this requirement lacks oversight and clarity on its implementation, and may therefore lead to self-censorship.[519] Zimbabwean law does not provide for the limitation of liability of intermediaries for hosting, caching, linking, or mere conduits.

There are also concerns in respect of the existing public order and national security laws have been used to target the media and activists both offline and online, including the Access to Information and Protection of Privacy Act, the Public Order and Security Act and the Official Secrets Act.[520] Furthermore,

[515] AFEX, n 185, p 65.
[516] Freedom House, n 514.
[517] AFEX, n 185, p 68.
[518] AFEX, n 185, p 68.
[519] CIPESA, n 25, p 30.
[520] AFEX, n 185, p 66.

the Criminal Law Codification and Reform Act places restrictions on certain types of speech; for instance, in terms of section 33, "undermining [the] authority of or insulting [the] President" in any printed or electronic medium is a crime against the state.[521] It is an offence to make statements that publicly cause hatred, contempt or ridicule of the person or office of the President or Acting President of Zimbabwe, and is punishable by a fine of up to two million Zimbabwe dollars or a years' imprisonment or both.[522] The vaguely defined "criminal insult" is also an offence.[523] Notably, in 2016, in *Misa-Zimbabwe and Others v Minister of Justice and Others*,[524] the Constitutional Court of Zimbabwe declared the offence of criminal defamation unconstitutional and inconsistent with the right to freedom of expression as protected under the Constitution of Zimbabwe. However, concerns have been raised that section 17 of the Cybercrime and Cybersecurity Bill attempts to bring back the offence relating to publication of falsehoods.[525]

In November 2017, Zimbabwean authorities arrested Martha O'Donovan, an American citizen working with a Zimbabwean media organisation, and charged her with two counts of "subverting constitutional government as defined in section 22(2)(a)(i) of the Criminal Law (Codification and Reform) Act" and "undermining authority of or Insulting President as defined in section 33(2)(b) of the Criminal Law (Codification and Reform) Act". The particulars of the first count alleged that between February and November 2017, O'Donovan "systematically sought to incite political unrest through the expansion, development and use of a sophisticated network of social media platforms as well as running accounts namely Magamba Network Trust @Matigary and @OpenParlyZw which she operates together with different users with a view to overthrow or attempt to overthrow the Government by unconstitutional means'. The particulars confirmed that the Zimbabwean authorities had been monitoring online activity in Zimbabwe, particularly content that is considered to be critical of the government.

On 22 October 2017, the police managed to trace the IP address that had accessed the Twitter account @Matigary to a computer that belonged to O'Donovan. It was therefore alleged that O'Donovan "engaged in working to raise foreign funding to capacitate a sophisticated online programme of action that is designed to culminate in online activism translating to an offline uprising" to "replicate offline uprisings like what happened in Tunisia and Egypt". It was further alleged that O'Donovan was 'the mastermind behind an organised social media campaign aimed at overthrowing or attempting to overthrow the government by unconstitutional means.

The particulars of the second count alleged that O'Donovan who was one of the Administrators of a Twitter account called @Matigary posted a message on Twitter which read "we are being led by a selfish and sick man". The message had an attachment of a photo of President Robert Mugabe and a portrait illustration purporting that the President is surviving on the use of a catheter in passing out urine.

[521] Freedom House, 'Freedom on the net 2018: Zimbabwe', accessible at https://freedomhouse.org/report/freedom-net/2018/zimbabwe.

[522] CIPESA, n 25, p 14.

[523] Freedom House, 'Freedom on the net 2018: Zimbabwe', accessible at https://freedomhouse.org/report/freedom-net/2018/zimbabwe.

[524] Case No CCZ/07/15.

[525] State v Chimakure, Kahiya and ZimInd Publishers (Pvt) Ltd, Constitutional Application No. SC 247/09, accessible at https://globalfreedomofexpression.columbia.edu/cases/chimakure-ors-v-the-attorney-general/.

The authorities considered the message abusive, indecent or obscene and aimed at undermining the authority or insulting the President.

In January 2017, high floor tariff prices for data announced by POTRAZ came into effect, but three days later, the Minister of Information Communication Technology issued a directive for immediate suspension of the increase, despite the fact that two network operators had already effected the increases.[526]

In 2016, social movements such as #ThisFlag and #Tajamuka built a following and utilised social media to organise protests, including the largest citizen-led mass stay-away, that led to social movement leaders Pastor Evan Mawarire and Promise Mkwanazi being arrested.[527] In February 2017, Mawarire was arrested on return from the United States where he had sought refuge months earlier, and was charged with "subverting a constitutional government" and "inciting Zimbabweans from all walks of life either locally or internationally to revolt and overthrow a constitutionally elected government", including through the use of social media. The case is still pending before the courts.[528]

In February 2017, Mawarire circulated another video on social media in which he yet again criticised Zimbabwe's economic policies and urged Zimbabweans to revolt against them. He was subsequently arrested and charged in terms of section 22(2) of the Criminal Law (Codification and Reform) Act, Chapter 9:23, although these charges were later dropped.[529]

There have also been incidents of citizens and online journalists being questioned for stories that they have published.[530] For instance, in October 2017, following the publication of a story in News Day that the former First Lady had donated used underwear to supporters, the author of the story was arrested and charged with criminal nuisance.[531] Kenneth Nyangani, the author, was released on bail pending trial.[532]

There have been concerns about network disruptions. Econet Wireless, for example, issued a press statement is 2015 indicating that it had gone to court on a number of occasions to prevent law enforcement officers from taking cell data records of specific customers.[533] There are no transparency reports published on government requests and compliance by service providers.[534] In July 2016, there was a two-hour disruption of WhatsApp across the country's three main mobile networks.[535] According to a report published by Freedom House, sources in the telecommunications sector confirmed that they

[526] AFEX, n 185, p 67.
[527] AFEX, n 185, p 65.
[528] Paradigm Initiative, n 55, p 54.
[529] Paradigm Initiative, n 55, p 54.
[530] AFEX, n 185, p 70.
[531] Paradigm Initiative, n 55, p 55.
[532] Paradigm Initiative, n 55, p 55.
[533] Econet Wireless, 'Press release on protection of customer information and privacy', 30 March 2015.
[534] AFEX, n 185, p 69.
[535] AFEX, n 185, p 71.

received instructions from the government to shut down the internet.[536] However, although concerns were raised about potential network disruptions during the 2018 presidential elections, this does not appear to have occurred.

There has not been any notable digital rights litigation in Zimbabwe during the period under consideration, although the 2016 judgment in *MISA-Zimbabwe* was important for freedom of expression more broadly.

Concluding observations

There is significant policy uncertainty in the countries under consideration, with a number of proposed laws currently pending that have serious implications for freedom of expression, privacy and access to ICTs. Furthermore, certain laws have only been partially implemented. The state of data protection laws in the countries under consideration offers a good illustration of this. For example, Botswana and Zambia have bills pending; Angola has a law in force but has not yet appointed a regulator; and South Africa has a law that has been passed and a regulator that has been appointed, but has not yet brought the substantive provisions into force. Such uncertainty leads to confusion and frustrations amongst members of the public.

Content restrictions are seen in all the countries under review. For instance, South Africa and Namibia are grappling with hate speech. In South Africa, instances of racist speech in online posts that have gone viral have been held to be hate speech by the courts. The Department of Justice's response has been the Prevention and Combating of Hate Crimes and Hate Speech Bill, although concerns have been raised that the provisions are overbroad and may have a chilling effect on freedom of expression.

Criminal defamation also remains an offence in some countries, such as in Zambia in respect of the president. In Angola, there is currently a pending constitutionality challenge to the Penal Code. In 2016, in *MISA-Zimbabwe*, the offence was declared unconstitutional in Zimbabwe, which may serve as an important precedent for other litigants seeking to challenge criminal defamation laws in their own countries.

Attempts to regulate social media and online content has given rise to concern. This includes, for instance, the Films and Publications Amendment Bill in South Africa that proposes giving wide powers to the Film and Publication Board to regulate user-generated content and to block non-compliant distributors at the ISP level, as well as the enactment of the Social Communications Legislative Package in Angola following years of the government calling for the regulation of social media. These content and regulatory measures have the potential to severely impede the enjoyment of freedom of expression online, and should be tested to ensure that the limitation is indeed necessary and proportionate.

A number of countries currently have cybercrimes legislation under consideration, including Namibia, South Africa and Zambia. In terms of content restrictions, provisions such as that contained in the

[536] Freedom House, 'Freedom on the net 2016: Zimbabwe', 2016.

Cybercrimes and Cybersecurity Bill in Zambia – which provides for penalties for "any electronic communication, with the intent to coerce, intimidate, harass or cause substantial emotion distress to a person" – are overly broad and vague, and may constitute an unjustifiable limitation of free speech. The concerns raised in respect of Chapter 8 of the Electronic Transaction and Cybercrime Bill are also serious in nature, particularly to the extent that it permits unauthorised access to communications, warrantless surveillance and interception.

Surveillance is a matter of concern in all the countries under consideration. As indicated above, the contradictory position in Namibia is that the government appears to have purchased interception and surveillance technologies, but has maintained an official stance that Part 6 of the Communications Act – which authorises telecommunications interception – has not been gazette and operationalised, therefore giving rise to concerns regarding the legality of interception activities that may be undertaken. In South Africa, the constitutionality challenge to the Regulation of Interception of Communications and Provision of Communication-Related Information Act, as well as the other surveillance-related cases that have been instituted, have the potential to provide important guidance on surveillance and interception laws, which may assist other countries in future litigation.

Although these are important pending digital rights cases, there has been limited digital rights litigation in the countries under consideration. As the SADC Tribunal is presently defunct, recourse before the sub-regional body is not available as is the case in East and West Africa. Furthermore, there are no Southern African countries that have entered a declaration in terms of Article 34(6) of the African Court Protocol to permit individuals and NGOs to file a complaint before the African Court. As such, only domestic courts are available to pursue recourse for digital rights violations

PART V: WHERE TO NEXT? OPPORTUNITIES FOR LITIGATION

The advent of the internet has brought with it incredible opportunities to facilitate the enjoyment of fundamental rights, but has also led to a number of challenges. Both states and private actors have sought to exploit this, and in doing so have resulted in a wide array of rights violations across the region and further abroad. To date, there remains a lack of respect for fundamental rights online in a number of countries, perpetuated by both public and private sector actors.

Regrettably, there has been a dearth of well-drafted ICT policies that appropriately embraces a rights-based approach. Rather, the typical trend has seen such laws and policies being drafted in a manner that ignore the practicalities of expression online, that encroaches on freedom of expression and privacy, or that seek to attribute further powers to the security and intelligence authorities in the state. Proactive engagement on policy development and reform has certainly yielded some positive results, and as highlighted in the *Okoiti* judgment in Kenya regarding certain intended surveillance measures, a failure to engage in meaningful stakeholder consultation may render decisions constitutionally non-compliant.[537] However, parties are often required to resort to litigation in an effort to challenge the laws in court.

A related concern in this regard pertains to policy uncertainty. Statements made by public officials or proposed laws that contain proposals that may impact freedom of expression – particularly regarding intended content or platform regulation – can give rise to alarm and cause members of the public to be unsure as to the status or effect thereof. This is potentially exacerbated where this is targeted at minority groups who may already face other barriers in freely expressing their points of view.

There is an expansive body of freedom of expression jurisprudence that has developed in many countries across the region, and that has been well-entrenched by the regional and sub-regional fora. However, this jurisprudence has typically focused on more traditional forms of expression and the media. Litigation focused on digital rights and freedom of expression online is still relatively nascent in the region, although some countries – most notably, Kenya – are starting to develop a useful body of jurisprudence that will likely be of assistance to other African states. As such, and in light of the current landscape, there is an array of opportunities for future litigation. Prospective litigants may also find comparative jurisprudence from other jurisdictions of value on digital rights, such as the European Union and the United States, where digital rights litigation has been more established over the last decade.

- ***Privacy and data protection***

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

[537] Okoiti, n 122.

member states of the European Union following the coming into force of the General Data Protection Regulation of the European Union[538] – only 18 out of the 55 African states have comprehensive data protection laws, not all of which have been fully operationalised. This leaves persons in those countries exposed to exploitative data practices that can severely infringe their rights to privacy among others.

In *Justice K.S. Puttaswamy (Retd) v Union of India*,[539] the Indian Supreme Court read a right to privacy into the Constitution of India, and ordered the government to enact a comprehensive data protection law. The court emphasised the need to protect personal data from exploitation and the responsibility on the government to ensure that citizens are appropriately protected. A similar approach could be considered in other states where no comprehensive data protection law exists.

For those states that do have comprehensive data protection legislation, a key component will be the structural and functional independence of the data protection authorities that are appointed. Enforcement of the data protection legislation will be a matter on which civil society and other stakeholders need to be vigilant. Aspects to be considered that may be a matter of interpretation of the data protection legislation include the existence of a so-called 'right to be forgotten', inter-state agreements for data transfers, and remedies in the event of data breaches.

In the existing climate in many African states that includes wide scale mandatory collections of data – for instance, for the purpose of mandatory SIM card registration or for the population of biometric databases – a framework to ensure the lawful processing of personal data is imperative to ensure that the processing takes place in an appropriate manner that safeguards the privacy rights of data subjects.

A further important aspect of the right to privacy is that of anonymity online. This is impeded, for instance, where ISPs are compelled to disclose the identities of users who post anonymously online. Anonymity is an important component of the right to freedom of expression, as the willingness of internet users to engage in debates of general interest, particularly on controversial or taboo subjects, is encouraged by the possibility that they can do so anonymously.[540] Measures must be put in place to ensure that ISPs cannot be compelled to disclose user data unless there are legal protections in place to protect against arbitrary abuse. In particular, and at a minimum, this should only be permitted when subject to a court order that meets the test of necessity and proportionality, taking into account all relevant factors.[541]

- ***Surveillance and appropriate safeguards***

[538] Accessible at https://gdpr-info.eu/.

[539] Writ Petition (Civil) No. 494 of 2012, accessible at http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

[540] MLDI, 'MLDI files intervention at European Court seeking to protect anonymity of users online', 10 October 2017, accessible at https://www.mediadefence.org/news/mldi-files-intervention-european-court-seeking-protect-anonymity-users-online.

[541] MLDI, n 540, p 5.

Linked to the right to privacy, surveillance laws are increasingly coming under scrutiny globally. Human rights violations are frequently committed under the guise on national security or anti-terrorism measures. Following the Edward Snowden leaks in 2013, the surveillance powers of the United States and the United Kingdom were put under scrutiny. Since then, a picture has begun to emerge of the wide ambit of surveillance activities globally, and the extent to which this impacts everyday activities.

Although surveillance may have a legitimate role to play in law enforcement activities – provided that meets the three-part test for a justifiable limitation, namely that it is prescribed by law, is necessary to pursue a legitimate aim and is proportionate – it is essential that surveillance laws and practices contain the necessary safeguards. The *Okoiti* judgment in Kenya provides important guidance in this regard,[542] and the constitutional challenge to the Regulation of Interception of Communications and Provision of Communication-Related Information Act in South Africa will be an important test case in this regard. Key safeguards include, for instance, user-notification provisions in the event of having been placed under surveillance, and proper oversight and warrant provisions to ensure that surveillance activities are only authorised in necessary and appropriate circumstances.

The European Court of Human Rights has developed a significant body of jurisprudence regarding surveillance when tested against right to privacy contained in Article 8 of the European Convention on Human Rights, finding for instance that impugned laws were drafted with insufficient clarity, afforded authorities too wide a discretion to intercept and examine communications, and lacked adequate and effective guarantees against arbitrariness and the risk of abuse inherent in any system of secret surveillance.[543] These cases can offer useful guidance to prospective litigants seeking to challenge similar provisions in the surveillance laws in their own states.

- ***Cybercrimes and cybersecurity***

Of similar concern, a number of countries have also recently enacted or proposed cybercrimes and cybersecurity legislation. These laws have, for instance, been enacted under the guise of addressing serious concerns regarding the misuse of the internet, such as unlawful hacking, hate speech, the spread of disinformation, and the dissemination intimate images without consent. While these may indeed be legitimate concerns, such laws also present risks of being veiled attempts to curtail citizen participation or stifle criticism.[544] In particular, such laws tend to be overbroad, and do not comply with necessary safeguards and human rights standards. In a similar vain to the safeguards discussed in relation to surveillance above, these should similarly be applied when dealing with cybercrimes and cybersecurity legislation.

[542] Okoiti, n 122.

[543] For an overview, see European Court of Human Rights, 'Factsheet: Mass surveillance', accessible at https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf.

[544] Media Foundation for West Africa, n 243, p 7.

The need for collaborative approaches when dealing with cybercrimes and implementing cybersecurity measures has repeatedly been emphasised.[545] It is important in this regard to ensure that special steps are taken to involve stakeholders who could find it difficult to participate or who are more vulnerable to cyber threats, including civil society and marginalised communities.[546] As has been noted by Research ICT Africa, collaboration should extend not only to public and private sector entities who own and control critical information infrastructure, but also stakeholders from other sectors (including the technical community and the banking and finance sectors) and not-for-profit stakeholder groups.[547] Furthermore, Research ICT Africa notes that commercial interests should not be the main driver for private sector stakeholders to participate in collaborative cybersecurity efforts; rather, the private sector should innovate and mitigate threats.[548]

- ***Expanding digital access***

There is still a significant digital divide across the region. Although various states have committed in policy documents towards achieving universal access, this has not yet been achieved. Access refers to a number of interrelated considerations, including infrastructure, spectrum, quality of service, and the costs of data and devices. This raises serious concerns, as an ongoing digital divide has the potential to further entrench socio-economic and gender imbalances, as certain groups – particularly those living in rural or peri-urban areas – are not able to enjoy the benefits or potential opportunities that the internet has to offer. As noted by the Media Foundation for West Africa: "Internet access still remains a challenge in rural areas. People in the rural areas have less access to the Internet, compared to those in the urban areas, and are left on the fringe of the digital revolution."[549]

Internationally, various proponents have advocated for there to be a recognised right to the internet. Although this has not as yet been expressly recognised under international law, there is at least a recognition that the internet is indispensable for the full realisation of a range of other fundamental rights, and has been recognised in the domestic laws of a number of states.

Litigation in this regard could take a number of forms. For instance, it could be targeted at testing the extent to which states have put in place reasonable measures to realise the existing commitments that have been made. This could also be targeted towards particularly segments of society, such as schools or women and girls. Countries, such as Estonia, Greece and Finland, already recognise a right to the internet in some form in their domestic legal frameworks.[550] France

[545] Research ICT Africa, 'Collaborative cybersecurity: The Mauritius case', October 2018, p 1, accessible at https://researchictafrica.net/wp/wp-content/uploads/2018/11/Policy-Brief-ADPP-N-1-Collaborative-Cybersecurity-Mauritius-Case.pdf.

[546] Research ICT Africa, n 545, p 1.

[547] Research ICT Africa, n 545, p 1.

[548] Research ICT Africa, n 545, p 1.

[549] Media Foundation for West Africa, n 243, p 3.

[550] Diplo Foundation, 'Right to access the internet: The countries and the laws that proclaim it', 2 May 2011, accessible at https://www.diplomacy.edu/blog/right-access-internet-countries-and-laws-proclaim-it.

and Costa Rica, for example, have seen successful litigation that has led to the government being required to promote and guarantee universal access.[551]

There is also possible litigation regarding licensing and access to spectrum for new entrants into the market – particularly in countries where there are entrenched monopolies or oligopolies – in the interest of expanding competition in the market, creating opportunities for smaller enterprises and ultimately reducing costs to increase access.

- ***Addressing threats and harassment online***

Notably, in order to fully enjoy the benefits and opportunities that the internet has to offer, it is important for users to feel that they can safely access the internet and express themselves without being subjected to online violence. However, the lived experiences of many users includes online harassment, threats, cyberstalking, instances of revenge pornography, blackmail and more. Although not always the case, women and sexual minorities are often the targets of such attacks. As has been noted by APC: "Increased prevalence of online violence against women, the lack of effective measures to prevent and contain it, and the ensuing impunity must be addressed as part of the struggle to eliminate all forms of gender-based violence. … The internet, once a liberating space, is also, increasingly, a space of violence, particularly violence targeting women."[552]

Such online violence is an overt expression of discrimination and inequality that exists offline, but which is amplified online.[553] Some countries, such as Ghana and South Africa, are considering laws to deal with the non-consensual sharing of intimate images; further, Ghana has implemented the Computer Emergency Response Team to monitor online incidents to ensure the safety of online users.[554] However, few countries have enacted policies that deal with the issues holistically, are up-to-date with technological developments, and appropriately balance the right to freedom of expression.[555]

In addition to policy measures, it is imperative that there is enforcement and accountability for those who commit acts of online violence. Courts, prosecutors and law enforcement officials need to be properly trained and resourced to deal with such matters. More broadly, litigation in this regard can also include assisting those who have suffered harm through the court processes to ensure redress

[551] Diplo Foundation, 'Right to access the internet: The countries and the laws that proclaim it', 2 May 2011, accessible at https://www.diplomacy.edu/blog/right-access-internet-countries-and-laws-proclaim-it.

[552] APC, 'Issue paper: Due diligence and accountability for online violence against women', 31 July 2017, accessible at https://www.apc.org/sites/default/files/DueDiligenceAndAccountabilityForOnlineVAW.pdf.

[553] Global Fund for Women, 'Online violence: Just because it's virtual doesn't make it any less real', accessible at https://www.globalfundforwomen.org/online-violence-just-because-its-virtual-doesnt-make-it-any-less-real/#.W-lUOJMzaUk.

[554] GenderIT, 'What can Ghana do about the harassment faced by women online', 6 November 2018, accessible at https://www.genderit.org/feminist-talk/what-can-ghana-do-about-harassment-faced-women-online.

[555] APC, 'Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences', November 2017, accessible at https://www.apc.org/en/pubs/online-gender-based-violence-submission-association-progressive-communications-united-nations.

and seek to curb ongoing conduct. For instance, in *KS v AM*,[556] the court granted an interdict against the respondent from publishing explicit sexual video footage and photographs of the applicant on social media platforms in terms of the Domestic Violence Act, 1998, and further directed the respondent to hand over all digital devices under his control in order for a forensic expert appointed by the applicant's attorneys to permanently remove all records of the applicant from the devices.

- ***Net neutrality***

Net neutrality refers to the principle that ISPs should treat all data that travels over their networks fairly, without improper discrimination in favour of a particular website or service.[557] Discrimination in this regard may relate to affecting information in a way that halts, slows or otherwise tampers with the transfer of any data, except for a legitimate network management purpose, such as easing congestion or blocking spam.[558] The UN Special Rapporteur on Freedom of Expression has noted that net neutrality promotes the widest possible access to information, and that states' positive duty to promote freedom of expression argues strongly for net neutrality in order to promote the widest possible non-discriminatory access to information.[559]

Two common ways in which net neutrality is impacted is through paid prioritisation schemes – through which providers give preferential treatment to certain types of internet traffic over others for payment or other commercial benefit – and through zero-rating – this being the practice of not charging for the use of Internet data associated with a particular application or service.

This has been a rife debate in the US over the past year. However, this issue has not yet seen significant traction in African states, although a breach of net neutrality is one of the grounds on which the social media tax is being challenged before the Constitutional Court in Uganda.[560] With the increasing number of zero-rated offerings, for example, and given its obvious appeal in African countries where there are low levels of access and high costs of data, it is certainly a matter that requires attention.

- ***Intentional network disruptions***

Intentional network disruptions – commonly referred to as 'internet shutdowns' – are an extreme measures analogous to banning a newspaper or broadcaster. Practically, this can take the form of blocking access to the internet in its entirety, or to certain websites or applications, such as Facebook or WhatsApp. In 2016, the UN Human Rights Council sates that it "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information

[556] Case No. A3032-2016, accessible at http://www.saflii.org/za/cases/ZAGPJHC/2017/297.html.

[557] Electronic Frontier Foundation, 'Net neutrality', accessible at https://www.eff.org/issues/net-neutrality.

[558] American Civil Liberties Union, 'What is net neutrality?', accessible at https://www.aclu.org/issues/free-speech/internet-speech/what-net-neutrality.

[559] Accessible at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement.

[560] CNN, 'Uganda government sued over social media tax', 2 July 2018, accessible at https://edition.cnn.com/2018/06/01/africa/uganda-social-media-tax/index.html.

online in violation of international human rights law, and calls upon all States to refrain from and cease such measures".[561]

However, such disruptions have continued across the region, typically taking the form of an order by the state authorities to relevant ISPs to give effect to such disruption. As has been noted by the UN Special Rapporteur on Freedom of Expression, internet shutdowns are often ordered covertly and without a legal basis, and violate the requirement that the restrictions must be provided for in law.[562] Similarly, shutdowns ordered pursuant to vaguely formulated laws and regulations, or in terms of laws and regulations that are adopted and implemented in secret, also fail to satisfy the legality requirement.[563] In circumstances where the network disruption occurs in the absence of an empowering legal provision, this would be ripe for judicial intervention.

A successful example was seen in *CM Pak Limited v Pakistan Telecommunication Authority*,[564] wherein the Islamabad High Court in Pakistan ruled that the Federal Government and the Pakistan Telecommunication Authority had impermissibly suspended or caused the suspension of mobile cellular services or operations in Pakistan. According to the court, the only instance permitted under domestic law whereby mobile services or operations could be suspended was if the President proclaimed a state of emergency; in the absence of any such proclamations – and notwithstanding national security concerns – any actions, orders or directives issued by the Federal Government or the Telecommunication Authority was declared to be illegal, *ultra vires* and without lawful authority and jurisdiction. The court noted further that causing the suspension of services or operations outside of instances permitted under the law may expose the Federal Government and the Telecommunication Authority to claims of compensation or damages by the licensees or the users of mobile services.

Even in circumstances where the network disruption is ordered in terms of an empowering legal provision, the UN Special Rapporteur on Freedom of Expression that network shutdowns invariably fail to meet the standard of necessity,[565] and are generally disproportionate.[566] Accordingly, litigation may still be instituted to challenge the network disruption on these grounds.

[561] Accessible at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13.

[562] Report of the UN Special Rapporteur on Freedom of Expression to the UN General Assembly, A/HRC/35/22, 30 March 2017, para 8, accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement.

[563] Report of the UN Special Rapporteur on Freedom of Expression to the UN General Assembly, A/HRC/35/22, 30 March 2017, para 10, accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement.

[564] FAO No. 42 of 2016, accessible at http://www.livelaw.in/pak-court-holds-suspension-mobile-services-federal-govt-ground-national-security-illegal-read-judgment/.

[565] Report of the UN Special Rapporteur on Freedom of Expression to the UN General Assembly, A/HRC/35/22, 30 March 2017, para 14, accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement.

[566] Report of the UN Special Rapporteur on Freedom of Expression to the UN General Assembly, A/HRC/35/22, 30 March 2017, para 15, accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement.

- ***Social media taxes***

  The recent spate of laws aimed at taxing social media users is a relatively new challenge that needs to be addressed. These laws appear on the face of it to be inimical with the right to freedom of expression, and lacking both in having a legitimate aim or being proportionate. It is unlikely that such laws in their current form will pass muster if appropriately challenged before the courts.

  Thus far, this has been a trend most seen in the East African region, although in August 2018 the West African state of Benin also passed a decree taxing its citizens for accessing the internet and social media applications.[567]

- ***Private sector accountability***

  Increasingly, ISPs – including social media platforms, telecommunications companies and ISPs – exercise significant control over the everyday activities of internet users. However, many do so in a manner that lacks transparency or appropriate oversight, with a resultant risk in users' rights being violated in exchange for accessing the services being offered. The private sector has also been complicit in agreeing to requests made by governments to, for instance, disrupt networks or provide communication-related information to facilitate surveillance activities.

  Compelling fuller and better disclosures by the private sector can go a long way in better understanding the role that it plays, and achieving some measure of accountability. But there is also arguably more that can be done to ensure that private sector companies – particularly those with large user-based that have a significant impact on the enjoyment of fundamental rights of large numbers of users online – abide by standards and practices that are rights-compliant.

  To date, much of the freedom of expression litigation across the region has been focused on the relevant state authorities. However, while states are indeed the primary duty-bearers when it comes to rights, the ever-increasing role of the private sector should also be tested and held to account in a manner that upholds fundamental rights, including freedom of expression online.

For strategies on litigating digital rights, please see: MLDI, 'Digital rights litigation guide', accessible at https://www.mediadefence.org/resources/.

[567] Internet Sans Frontières, 'Bénin: Taxer les réseaux sociaux entrave la liberté d'espression et l'économie numérique', 28 August 2018, accessible at https://internetwithoutborders.org/benin-taxer-les-reseaux-sociaux-entrave-la-liberte-dexpression-et-leconomie-numerique/; Quartz Africa, 'Benin is the latest African nation taxing the internet', 4 September 2018, accessible at https://qz.com/africa/1377582/benin-is-taxing-use-of-social-media-apps-like-facebook-whatsapp/.

SELECTED RESOURCES

- AFEX, 'Internet freedom in Africa: Baseline report of eight countries', 2017: http://www.africafex.org/afex/wp-content/uploads/2017/09/AFEX-Internet-Freedom-in-Africa-Report-2017.pdf

- CIPESA, 'State of internet freedom in Africa 2017', September 2017: https://cipesa.org/?wpfb_dl=254

- Freedom House, 'Freedom on the net 2017', November 2017: https://freedomhouse.org/report/freedom-net/freedom-net-2017

- Freedom House, 'Freedom on the net 2018', November 2018: https://freedomhouse.org/report/freedom-net/freedom-net-2018

- Internet Live Stats, 'Internet penetration in Africa', 31 December 2017: https://www.internetworldstats.com/stats1.htm

- Human Rights Watch, 'World report 2018': Events of 2017', 2017: https://www.hrw.org/world-report/2018

- Media Foundation for West Africa, 'Bi-annual policy brief on internet rights in West Africa: January to June 2018', 2018: http://www.mfwa.org/wp-content/uploads/2018/08/Bi-Annual-Policy-Brief-on-Internet-Rights-in-West-Africa-January-June-2018.pdf

- MLDI, 'Digital rights litigation guide', 2018: https://www.mediadefence.org/resources/mldi-digital-rights-litigation-guide

- MLDI, 'Training manual on digital rights and freedom of expression online', 2018: https://www.mediadefence.org/resources/mldi-training-manual-digital-rights-and-freedom-expression-online

- Paradigm Initiative, 'Digital rights in Africa 2017 report', May 2018: http://web.paradigmhq.org/download/digital-rights-in-africa-report-2017-2/

APPENDIX: QUESTIONNAIRE

1.	Name:		
2.	Organisation:		
3.	Designation:		
4.	E-mail address:		
5.	In which country/ies is your organisation based?	In which country/ies does your organisation operate?	
6.	In what type of work relating to digital rights and online freedom of expression does your organisation engage? Please check the appropriate box(es) below. • Litigation ☐ • Policy / law reform ☐ • Advocacy ☐ • Research ☐ • Other ☐ Please provide any information on your current or past work relating to digital rights and online freedom of expression that you think might be relevant for the research report.		
7.	Context: Are there any relevant factors or developments relating to the context in the country/ies in which you operate that impact digital rights and freedom of expression online? This might include, for instance, recent elections or national security threats.		
8.	Policy / law reform: Are there any recently proposed or adopted laws or policies in respect of digital rights and online freedom of expression in the country/ies in which you operate? If so, please provide any relevant information, such as current status of the laws or policies, the public response, and the rationale for it.		

9.	Litigation: Have there been any recent judgments, or any anticipated or ongoing litigation, in respect of digital rights and online freedom of expression in the country/ies in which you operate? If so, please provide any relevant information, such as judgments or other court documents.
10.	Challenges: What do you consider to be the biggest challenges or threats to digital rights and online freedom of expression in the country/ies in which you operate?
11.	Opportunities: What do you consider to be the next opportunities for law reform or litigation in respect of digital rights and online freedom of expression in the country/ies in which you operate?
12.	Please provide any suggestions for other individuals or organisations working on digital rights and online freedom of expression who you would recommend we contact.
13.	Please provide any attachments or links to resources that you think would be useful for the report.
14.	May we acknowledge in the research report that you and your organisation were consulted for input? Please check the appropriate box below. Yes ☐ No ☐ We note that we only intend to include your name, the name of your organisation, and a link to your organisation's website. We will not attribute specific viewpoints to you in the report.