ARTICLE 19

Freedom of Expression and the Digital Environment in Eastern Africa

Monitoring report

January–December 2020

ARTICLE 19 EASTERN AFRICA

ACS Plaza

2nd Floor, Lenana Road

PO Box 2653-00100

Nairobi, Kenya

T: +254 727862230

E: kenya@article19.org

W: www.article19.org

Tw: @article19eafric

Fb: @article19easternafrica

A19/EAFR/DIG/2021/001

ISBN: 978-9966-084-17-0

ARTICLE 19 Eastern Africa would appreciate receiving a copy of any materials in which information from this report is used. This report was developed as part of a three-year project financed by the Ford Foundation. Ford Foundation does not necessarily share the opinions here within expressed. ARTICLE 19 Eastern Africa bears the sole responsibility for the content of the document.

Contents

List of Abbreviations

ACHPR	African Commission on Human and Peoples' Rights
ARTICLE 19	ARTICLE 19, Global
ARTICLE 19 EA	ARTICLE 19 Eastern Africa
BAKE	Bloggers Association of Kenya
COST	Cost of Shutdown Tool, NetBlocks
CSO	Civil society organisation
DCI	Directorate of Criminal Investigations (Kenya)
ETB	Ethiopian birr
GPS	Global positioning system
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communications technology
ICT Law	Law Governing ICT, Law No. 24/2016 of 18 June 2016 (Rwanda)
KCCA	Kampala Capital City Authority
NTSA	National Transport and Safety Authority (Kenya)
OHCHR	Office of the United Nations High Commissioner for Human Rights
PWD	Persons with disabilities
RCDF	Rural Communications Development Fund (Uganda)
RMC	Rwanda Media Commission
RURA	Rwanda Utilities Regulatory Authority
TCRA	Tanzania Communications Regulatory Authority
TZS	Tanzanian shilling
UCC	Uganda Communications Commission
UCSAF	Universal Communications Service Access Fund (Tanzania)
UN HRC	United Nations Human Rights Council
USAF	Universal Service and Access Fund (South Sudan)

Executive Summary

The Internet and digital technologies offer crucial spaces for people to seek and impart information on a range of issues and to exercise their right to freedom of expression. The digital environment plays a particularly important role during elections and protests and facilitates individuals' and communities' exercise of a wide range of human rights, both online and offline.

Given its importance, between January and December 2020 (reporting period), ARTICLE 19 Eastern Africa (ARTICLE 19 EA) monitored and documented developments and challenges affecting the digital environment and the protection of the right to freedom of expression online, including during the Covid-19 pandemic. Furthermore, ARTICLE 19 EA outlines issues related to accessibility and affordability of the Internet and problems related to privacy and data protection. This report focuses on six countries: Ethiopia, Kenya, Rwanda, South Sudan, Tanzania, and Uganda.

As for **freedom of expression**, this report documents the use and misuse of problematic laws and policies and Internet disruptions by governments to address 'misinformation', 'disinformation', 'hate speech', and unrest, including those adopted due to the Covid-19 pandemic. These problematic laws and practices have been used to either intimidate, detain, summon,[1] arrest, charge, or imprison 23 Internet and digital technology users for, amongst other things, allegedly publishing false Covid-19 information in Ethiopia, Kenya, Rwanda, Tanzania, and Uganda. Worryingly, governments have adopted laws and regulations that criminalise freedom of expression online, including through the introduction of licensing requirements for Internet users, including bloggers and citizen journalists. This is drastically impacting the ability of Internet users to freely express themselves online on the Covid-19 pandemic and on social and political issues, especially around elections and protests.

As for the **accessibility and affordability** of the Internet and digital technologies, this report notes that all six countries have commendably enacted legal frameworks for universal access and service mechanisms, which is indicative of governments' efforts to bridge the digital divide.[2] However, the implementation of these commitments varies between and amongst all six countries. This is impacting connectivity expansion drives in rural, unserved, and underserved areas, and regional harmonisation efforts. It continues to affect specific groups more than others, including women, the young, the poor, the elderly, and persons with disabilities.[3]

As for **privacy and data protection**, this report details the enactment of data protection laws in Kenya, Uganda, and Rwanda. However, these positive efforts are being overshadowed by the unchecked development and use of digital contact tracing applications and robotic technologies without sufficient safeguards. Rwanda, Tanzania, Ethiopia, Kenya, and Uganda have developed or deployed some of these technologies to varying degrees. Furthermore, one judicial decision in Tanzania is set to have a significant impact on digital anonymity, with far-reaching cross-jurisdictional implications.

This monitoring report is intended for the general public, digital rights advocates, human rights organisations, and strategic litigators in Eastern Africa.

Introduction

The Eastern Africa region is shaped by vastly different contextual realities at the political, economic, and human rights levels. Out of the six focus countries, Ethiopia, Tanzania, and Uganda fared much worse than Kenya, Rwanda, and South Sudan in terms of human rights protection and continue to fall short of their international obligation to respect, protect, and fulfil human rights.[4]

In 2020, ARTICLE 19 EA documented several positive changes in the digital environment promoting human rights and the adoption and use of digital technologies. These included a wide array of digital connectivity solutions by users, corporate entities, and governments that advance the protection of freedom of expression online and other rights in the digital environment.

Despite these positive developments, governments have failed to create an enabling environment for the enjoyment of online rights and freedoms, with numerous violations being noted across the region affecting freedom of expression, access to information, privacy, and data protection. The report provides a detailed overview of these issues, as well as recommendations to governments to bring their practices into full compliance with international human rights standards.

This report is the first of a series documenting developments in the digital environment in Eastern Africa. This, and subsequent reports, will focus on three key issues: challenges to freedom of expression online, challenges to Internet accessibility and affordability, and challenges to privacy and data protection.

The information contained in the report is based on regular monitoring of developments as reported in the media, information provided directly by Internet users, and an assessment of statements issued by state agencies and their representatives. It includes a review of key court judgments and reports from regulators and ICT ministries. It also builds on previous ARTICLE 19 legal analyses and reports examining the impact of legislative and regulatory frameworks and policies on freedom of expression in the six countries.

Applicable International and Regional Freedom of Expression and Privacy Standards

The Right to Freedom of Expression

The right to freedom of expression is protected by Article 19 of the Universal Declaration of Human Rights,[5] and given legal force through Article 19 of the International Covenant on Civil and Political Rights (ICCPR)[6] and Article 9 of the African Charter on Human and Peoples' Rights (the African Charter).[7]

The scope of the right to freedom of expression is broad. It requires states to guarantee to all people the freedom to seek, receive, or impart information or ideas of any kind, regardless of frontiers, through any media of a person's choice, either orally, in writing or in print, in the form of art, or through any other media of choice. The UN Human Rights Committee, the treaty body of independent experts monitoring states' compliance with the ICCPR, has affirmed that the scope of the right extends to the expression of opinions and ideas that others may find deeply offensive.[8] The African Commission on Human and Peoples' Rights (African Commission) affirmed that states have an obligation to 'facilitate the rights to freedom of expression and access to information online and the means necessary to exercise these rights.'[9]

While the right to freedom of expression is fundamental, it is not absolute. A state may, exceptionally, limit the right under Article 19(3) of the ICCPR, provided that the limitation is:

- Provided for by law – any law or regulation must be formulated with sufficient precision to enable individuals to regulate their conduct accordingly;
- In pursuit of a legitimate aim; listed exhaustively as respect of the rights or reputations of others, the protection of national security or of public order (ordre public); or the protection of public health or morals; and
- Necessary and proportionate in a democratic society, i.e. if a less intrusive measure can achieve the same purpose as a more restrictive one, the least restrictive measure must be applied.[10] Article 9(2) of the African Charter also reiterates that the right to express and disseminate opinions must be 'within the law'.

Thus, any limitation imposed by the state on the right to freedom of expression must conform to the strict requirements of this three-part test. Furthermore, Article 20(2) of the ICCPR provides that any advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence must be prohibited by law.

Freedom of Expression Online

In 2012, the UN Human Rights Council (UN HRC) recognised that the 'same rights that people have offline must also be protected online.'[11] The Human Rights Committee also clarified that limitations on electronic forms of communication or expression disseminated over the Internet must be justified according to the same criteria as non-electronic or offline communications.[12]

While international human rights law places obligations on states to protect, promote, and fulfil human rights, it is widely recognised that business enterprises also have a responsibility to respect human rights.[13] Importantly, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Special

Rapporteur on FoE) has long held that censorship measures should never be delegated to private entities.[14] The Special Rapporteur recommended that any demands, requests and other measures to take down digital content must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under Article 19(3) of the ICCPR.[15]

The Special Rapporteur on FoE clarified the scope of legitimate restrictions on different types of expression online; he identified three different types of expression for the purposes of online regulation:

1. Expression that constitutes an offence under international law and can be prosecuted criminally;
2. Expression that is not criminally punishable but may justify a restriction and a civil suit; and
3. Expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility, and respect for others.[16]

He clarified that the only exceptional types of expression that states are required to prohibit under international law are child pornography, direct and public incitement to commit genocide, 'hate speech', and incitement to terrorism. However, he clarified that even legislation criminalising these types of expression must be sufficiently precise, and there must be adequate and effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body.[17] Notably, even legislation prohibiting the dissemination of child pornography over the Internet through the use of blocking and filtering technologies is not immune from complying with these requirements.

Subsequently, the Special Rapporteur on FoE noted that states should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and the standards of legality, necessity, and legitimacy outlined by the Human Rights Committee.[18] He went on to assert that states and intergovernmental organisations should refrain from establishing laws that would require the ‘proactive’ monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship. He also recommended that states refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression.

Other free speech mandates also clarified for scope of specific restrictions of online expression. In their 2017 Joint Declaration on freedom of expression, ‘fake news’, disinformation, and propaganda, the four international mandates on freedom of expression expressed concern at ‘attempts by some governments to suppress dissent and to control public communications through […] efforts to “privatise” control measures by pressuring intermediaries to take action to restrict content.’[19] They emphasised that intermediaries should never be liable for any third-party content relating to those services unless they specifically intervene in that content, or refuse to remove it (despite having the requisite technical capacity) when required to do so by an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body such as a court.

This was echoed in the recently revised African Commission on Human and Peoples’ Rights (ACHPR) Declaration.[20] The African Commission further imposes an obligation on states to ‘facilitate the rights to freedom of expression and access to information online and the means necessary to exercise these rights.’[21] According to these principles, states are required to refrain from prohibiting free expression, or to do so only under strict

circumstances, as well as to take positive steps to enable free expression. The protection of anonymity is a vital component in protecting the right to freedom of expression as well as other human rights. A fundamental feature enabling anonymity online is encryption. Without the authentication techniques derived from encryption, secure online transactions and communication would be impossible.

The legal protection of online anonymity has so far received limited recognition under international law. Traditionally, the protection of anonymity online has been linked to the protection of the right to privacy and personal data. In May 2015, the Special Rapporteur on FoE stressed that restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.[22]

The Right to Privacy

The right to private communications is protected under international law through Article 17 of the ICCPR which, inter alia, states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence. The right to privacy complements and reinforces the right to freedom of expression: it is essential for ensuring that individuals are able to freely express themselves, including anonymously, should they so choose.[23] The mass surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

In General Comment No. 16 on the right to privacy, the Human Rights Committee clarified that the term 'unlawful' means that no 'interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives'[24] of the ICCPR. The Human Rights Committee further stated that 'relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by that authority designated under the law, and on a case-by-case basis.'[25]

The previous UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism argued that restrictions on the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test, in a similar manner to the right to freedom of expression under Article 19.[26] In terms of surveillance, within the context of terrorism in this instance, he stated that 'states may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on the showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.'[27]

The Special Rapporteur on FoE also observed that 'the right to privacy can be subject to restrictions or limitations under certain exceptional circumstances.'[28] This may include state surveillance measures for the purposes of the administration of criminal justice, prevention of crime or combatting terrorism.' In 2014, the UN High Commissioner for Human Rights observed that 'any limitation to privacy rights reflected in Article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available.'[29]

The ACHPR's Declaration recognises that the right to privacy and the right to freedom of expression are 'mutually reinforcing rights that are essential for human dignity and the overall promotion and protection of human and peoples' rights.'[30]

Access to the Internet and Digital Technologies

The Internet and digital technologies continue to demonstrate their essential role as facilitators of development agendas and enablers of a broad range of rights, online and offline. These rights, most of which are captured and promoted in the African Declaration on Internet Rights and Freedoms,[31] include online freedom of expression, access to public health information, access to electoral information about political parties and candidates, online assembly, and inclusive participation, amongst others.

Although there is no binding 'right to Internet access' under international law, the Declaration of Principles on Freedom of Expression and Access to Information in Africa calls on states to 'recognise that universal, equitable, affordable and meaningful access to the Internet is necessary for the realisation of freedom of expression, access to information and the exercise of other human rights.'[32] This is reiterated in the African Declaration on Internet Rights and Freedoms – a civil society initiative – which affirms the vital role played by the Internet and calls on states to ensure that access to the Internet is made 'available and affordable to all persons in Africa without discrimination on any ground.'[33] Likewise, the Special Rapporteur on FoE noted the need to develop 'effective policies to attain universal access to the Internet.'[34] The UN HRC resolution (2018) reinforced the 'importance of building confidence and trust in the Internet, not least with regard to freedom of expression, privacy and other human rights so that the potential of the Internet as, inter alia, an enabler for development and innovation can be realised, with full cooperation between governments, civil society organisations (CSO), the private sector, the technical community and academia.'[35]

Criminalising Online Expression in Eastern Africa – Case Studies

During the reporting period, a variety of problematic content was shared on the Internet and social media platforms, mirroring challenges faced in other regions to tackle, for example, various forms of 'hate speech' or 'misinformation'. Despite this, there have been a number of cases where public authorities relied on restrictive laws and policies to target activists and independent media, intimidate and harass Internet users, stifle legitimate criticism of public health measures and authorities, and monitor and control Covid-19 narratives.

In addition to broad and restrictive laws and policies, governments in the region promoted and adopted heavy-handed approaches, and imposed or threatened to impose criminal sanctions to tackle problematic content, resulting in a criminalisation of online free expression.

Criminalising Online Expression in Tanzania: Worst Performer in 2020

Tanzania Prime Minister Kassim Majaliwa issued a warning on 21 March against the spread of false Covid-19 information, warning that those who spread such false information would be 'dealt with'.[36] A list of authorised experts with permission to educate the public about Covid-19 was issued by the Ministry of Health.[37] Reports indicate that the Tanzania Communications Regulatory Authority (TCRA) encouraged citizens to report individuals posting messages on 'social media platforms that "distort" Covid-19 related information' to the TCRA.[38]

Tanzanian authorities relied on the Electronic and Postal Communications (Online Content) Regulations 2018 which do not comply with international freedom of expression standards. In March, ARTICLE 19 EA identified three instances where digital technology users faced criminal sanctions for allegedly failing to obtain a licence from TCRA before publishing content online under the Regulations 2018 for allegedly failing to obtain a licence from TCRA before publishing content online.[39] In April alone, ARTICLE 19 EA identified three instances where the Regulations 2018 were used to target Internet users who allegedly uploaded 'unofficial' information and false statistics about Covid-19, and allegedly published and disseminated false Covid-19 information.[40] In May, one individual was found guilty of sedition and incitement; it remains unclear whether this was restricted to print material or whether it also incorporated online material.[41]

In July, the Regulations 2018 were revised, and Regulations 2020 were adopted, affecting a wider group of digital technology users than before. Specifically, the regulations include vague and overly broad terms; they impose onerous licensing requirements and fees based on the content offered; they contain extremely severe criminal and civil sanctions; and they consolidate and expand the TCRA powers, which should rightly reside with an independent body, such as the courts.

The regulations have also expanded the 'prohibited content' provisions and continue to restrict various categories of online expression, some of which constitute legitimate expression, including those promoting critical discussions about sexuality, gender, and reproductive health.[42] Contravening the Regulations 2020 attracts a fine of TZS5 million (USD2,148) or a jail term of 12 months, or both.

Criminalising Online Expression in Kenya

The Cabinet Secretary for Health in Kenya issued a statement in March warning against the spread of false Covid-19 information. The Cabinet Secretary stated: "these rumours must stop […] but because I know empty appeals will not work, we will proceed and arrest a number of them to prove our point."[43]

In Kenya, freedom of expression is severely restricted by the Computer Misuse and Cybercrimes Act 2018. In 2018, ARTICLE 19 EA and the Kenya Union of Journalists supported a case lodged by the Bloggers Association of Kenya (BAKE) which contested the legality and constitutionality of 26 provisions of the Computer Misuse and Cybercrimes Act 2018.[44] The three organisations argued that these provisions violate the right to freedom of expression, the right to privacy, and press freedom. The Computer Misuse and Cybercrimes Act 2018 was declared valid in its entirety on 20 February. However, this was subsequently nullified by the High Court (subject to remedial action being taken by parliament within nine months) on 29 October.[45]

In March alone, ARTICLE 19 EA identified three instances where Sections 22 and 23 of the Computer Misuse and Cybercrimes Act 2018 were used to target Internet users whose posts countered the government's official Covid-19 narrative.[46] Between April and December, ARTICLE 19 identified three more instances where these same provisions were used to target Internet users who created and uploaded online content, including posts and websites, commenting on Kenya's political situation and detailing corruption scandals.[47] These users included bloggers, editors, citizen reporters, content creators, and politicians. Notably, Sections 22 and 23 of the Computer Misuse and Cybercrimes Act 2018 both carry criminal sanctions of two years' and 10 years' imprisonment, respectively.

Concerningly, ARTICLE 19 EA has observed the arbitrary misuse of Sections 22 and 23 of the Computer Misuse and Cybercrimes Act 2018 by one arm of the National Police Service, namely the Directorate of Criminal Investigations (DCI). ARTICLE 19 EA has also identified instances where allegedly offending posts and/or websites have been pulled down and/or temporarily disabled whilst individuals were in the DCI's custody. Individuals who were in DCI custody told ARTICLE 19 EA that the DCI officers placed direct pressure on them to either edit the content of articles or pull-down articles, in their individual capacity or via website administrators.[48] Others were directed to 'desist from sharing any coronavirus related information' on social media handles or 'risk being re-arrested' and having bond terms cancelled.[49]

Criminalising Online Expression in Uganda

On 22 March, the Uganda Communications Commission (UCC) issued a statement clarifying that the criminal sanctions in the 'Computer Misuse Act, the Data Protection and Privacy Act (2019) and/or other Penal Laws of Uganda' would be used to prosecute people spreading misinformation and fake news'.[50]

ARTICLE 19 previously raised concerns about the compatibility of several provisions of Uganda's Penal Code (CAP 120) with international freedom of expression standards.[51] This framework is often used to stifle freedom of expression and target journalists, human rights defenders, bloggers, peaceful protesters, and others.

Between February and December, ARTICLE 19 EA documented one positive ruling which overturned a flawed 'cyber-harassment' sentence under Section 24 of the Computer Misuse Act 2011.[52] However, two Internet and digital technology users[53] were

charged under Section 171 of the Penal Code (CAP 120). Section 171 carries a heavy criminal sanction of up to seven years. Additionally, during the same period, two Internet users were arrested; one individual was not formally charged in court and it remains unclear whether the other individual was charged.[54] This legislative framework was used during the Covid-19 pandemic to criminalise expression denying the existence of Covid-19 in Uganda, and as an 'excuse'[55] to punish Internet users, including journalists and writers, for non-Covid-19 related offences.

Criminalising Online Expression in Rwanda

On 13 April, the Rwanda Media Commission (RMC) issued a press release announcing that bloggers providing information on YouTube are not journalists and do not form part of the cohort of authorised/essential services, unless they have been accredited.[56] The RMC also claimed that bloggers are not authorised to interview people.[57] The RMC's press release regarding bloggers is at odds with the provision under Article 19 of Rwanda's own Media Law which provides that 'every person has the right to receive, disseminate or send information through [the] Internet. He/she is entitled to the right of creating a website through which he/she disseminates the information to many people. Posting or sending information through the Internet does not require the user to be a professional journalist.'[58]

Rwanda's ICT Law[59] requires extensive reforms[60] to ensure its compliance with international human rights law and standards. Articles 22 and 60 of the ICT Law grant unchecked powers to the ICT Minister and the Rwanda Utilities Regulatory Authority (RURA) to suspend or restrict electronic communications networks or services, and to prohibit the 'improper use of public electronic communication network[s]' using vague terms.[61] Specifically, Article 60 of the ICT Law fails to comply with the proportionality and necessity requirements in the ICCPR and the African Charter, and encourages self-censorship and unchecked restrictions on online expression in Rwanda.

Similarly, the 2013 Media Law[62] offers a restrictive definition of a 'professional journalist' that fails to recognise 'citizen journalists' and freelance journalists, among others. This definition is not in line with the UN definition of journalism as 'a function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the Internet or elsewhere.'[63]

Between April and December, ARTICLE 19 EA identified two instances where Covid-19 guidelines and the ICT Law were used to target individuals uploading information about human rights violations to online platforms.[64] These laws were used to unduly restrict the activities of citizen reporters and bloggers uploading Covid-19 reports on YouTube, despite their crucial documentation of offline human rights violations.

Criminalising Online Expression in Ethiopia

On 29 March, the Ethiopian Prime Minister's office reminded law enforcement officers that they have been tasked with 'taking action against individuals and groups unleashing terror on people's health and sense of safety.'[65]

On 13 February, Ethiopia passed the Proclamation on Hate Speech and Disinformation[66] which falls short of international and regional freedom of expression standards.[67] The Proclamation contains inadequate definitions and provisions and heightens the risk of increased policing and surveillance by both state organs and private bodies. This

Proclamation also fails to specify the independent body tasked with overseeing the implementation of the Proclamation.[68]

Furthermore, the Proclamation fails to differentiate between different types of hate speech based on its severity[69] which risks encouraging self-censorship due to fears of being an accessory to an offence. Additionally, Article 8 of the Proclamation requires 'any enterprise that provides social media service', including 'social media service providers and social media enterprises' to actively monitor, suppress, prevent, and 'remove or take out of circulation disinformation or hate speech content',[70] lest they face liability, in breach of international standards on freedom of expression.

Between March and April, ARTICLE 19 EA identified two instances where Internet users were targeted for spreading false Covid-19 information, and where Articles 4, 5, and 7 of the Proclamation we were used to impose charges.[71] The prohibition against hate speech and disinformation under Articles 4 and 5 of the Proclamation is accompanied by stiff civil and criminal penalties. Article 7(4) imposes a fine of ETB100,000 (USD2,613) or a three-year jail term for any person found guilty of these two vague offences.

Accessibility and Affordability of Digital Technologies

The Covid-19 pandemic magnified that those without access to the Internet and digital technologies are marginalised, economically and socially. Broadband penetration rates are still low in Eastern Africa.[72] Statistics make this point clear but reveal very little information about the reliability, quality, and sustainability of access to the Internet and digital technologies in the region. Furthermore, the Covid-19 pandemic revealed glaring connectivity gaps in all six countries. In turn, these gaps demonstrate the transference of offline inequalities to the digital environment, including documented gendered, income, and age-centric challenges to universal broadband connectivity.[73]

ARTICLE 19 EA has identified two challenge affecting efforts to promote universal, inclusive, and affordable Internet access. These include Internet disruptions and poor, limited, or non-existent information about universal access/service mechanisms, which impacts an assessment of their efficacy. In turn, Internet disruptions retard universal access/service efforts whereas poor information restricts stakeholders from effectively addressing connectivity gaps using coordinated efforts.

Universal Access/Service Funds

Universal access/service funds seek to progressively promote access to affordable digital services to the population, especially in rural, unserved, and underserved areas. Increasing emphasis is being placed on a simultaneous provision of good quality digital connectivity and relevant content.[74]

At the policy and legislative levels, governments' commitment to universal access/service mechanism objectives and the promotion of nationwide access to digital services relies on the regular publication of annual mechanism reports. Annual reports offer a contextualised standard for the public and CSOs to hold governments to account at national, regional, and international fora, and offer a metric to assess connectivity rates, both in-country and within a specific region. This report calls on governments across Eastern Africa to commit, now more than ever, to proactively disclosing connectivity information in line with open data calls and standards.

Rwanda, Kenya, Uganda, and Tanzania took proactive steps to implement various universal access/service projects, pre-Covid-19.

In South Sudan, given the nascent nature of the Universal Service and Access Fund (USAF), no projects have been implemented yet. However, efforts have been made to expand the regulatory framework (through the development of draft USAF legislation), strengthen internal structures, and assess the gaps in the demand and supply of ICT services. Commendably, the South Sudanese USAF steward notes – in the six-month's report – that tangible steps have been taken to actualise an assessment of the state of ICT infrastructure service, access, and usage in South Sudan.[75]

Rwanda, Kenya, Tanzania, and South Sudan released reports between 2018 and 2020.[76] Despite this, it is not possible to fully analyse the extent to which ICT ministries, communications regulators, and statutorily created boards have fulfilled their universal access/service fund objectives to enhance ICT access in rural, unserved, and underserved areas, nor to assess the efficacy of these mechanisms.

This stems from a reporting failure by governing authorities in Rwanda, Tanzania, and Kenya who either consistently failed to document the *total* universal access budget against the *actual* amount expended for specific projects, or provided inadequate information preventing a comprehensive calculation, or both. In turn, this affects an examination of the funding mechanism's adherence to best practice demanding transparency and prevented CSOs and other actors from ascertaining how the funds were used, who they were allocated to, and who benefitted from projects.

Specifically, the reports published by regulators in Kenya and Rwanda fail to detail the specific location (county, district, village, ward) of areas which have actually benefitted from universal access/service funds. This is problematic as such information could enable CSOs and the general public to assess the medium-long term benefits of the mechanisms, including identifying uptake by the benefitting community. Commendably, Tanzania stood out as the best-case example in this arena due to its proactive and detailed disclosure of information about the regions, districts, wards, schools, and telecentres which had benefitted from the UCSAF, as well as its release of a publicly accessible register of universal service provision.[77]

Uganda and Ethiopia stood out as outliers in this regard. The UCC has not released annual reports on the Rural Communications Development Fund (RCDF) since the 2014/2015 period, as of December 2020. This is despite UCC's own recognition, in the RCDF Operational Guidelines 2017/18–2021/22 (RCDF III), that annual reports constitute one of the sources and means of verifying that the RCDF's expected results have been achieved.[78] ARTICLE 19 EA notes that RCDF project briefings, which were last captured in 2019 via its blog, falls short of the annual reporting requirements set out in Uganda's legislative and regulatory framework. Ethiopia is the only country that has not operationalised its mechanism promoting universal access, and regulations governing Ethiopia's Universal Access Fund have not yet been drafted by the Council of Ministers, as of December 2020.

Internet Disruptions

Contrary to universal access drives, Ethiopia and Tanzania disrupted access to the Internet and telecommunication services in response to political unrest, and during the election period.

Ethiopia continues to rely on mass and region-specific Internet shutdowns to respond to political unrest. Against a backdrop of a postponed election,[79] on 4 November, the government disrupted telephone and Internet services in Tigray before launching an ongoing military operation. The disruption hindered the free flow of, and access to, timely information and news, while the operation claimed the lives of numerous individuals.[80]

Prior to this, Ethiopia implemented a nationwide connectivity disruption on 29 June. This was triggered by the death of popular Oromo musician and activist Haacaaluu Hundeessa and justified using the 'national security' argument.[81] The Ethiopian government proceeded to partially,[82] then fully, restore access to the Internet on 23 July.[83] However, this shutdown arbitrarily prevented people from exercising numerous rights, including their rights to online and offline freedom of expression, assembly and association, and access to information. The NetBlocks Cost of Shutdown Tool (COST) tool estimates that the 23-day shutdown cost around ETB3 billion (USD103 million).[84]

Similarly, Tanzania scaled up its targeted onslaught on political opponents, and disrupted telecommunications services, social media, and online communications platforms between July and December. This occurred prior to, and immediately after, the heavily

disputed October elections.[85] On 27 October, Tanzania imposed restrictions on 'social media and online communication platforms via multiple Internet providers', including Twitter, WhatsApp, Facebook, and Instagram.[86] Twitter's Public Policy Team confirmed that it had documented 'some blocking and throttling of Twitter'.[87] Prior to this, on 24 October, the TCRA issued an order to service providers, including Viettel Tanzania plc, to 'temporarily suspend [the] offering of bulk short messaging and bulk voice calling services' from 24 October to 11 November.[88] A few days after the elections, and following a targeted arrest of several opposition leaders, the US Ambassador Donald Wright indicated, on 2 November, that telecommunications services were still affected.[89]

Restrictions on Privacy and Data Protection

Covid-19 Applications

The protection of personal data is essential for mitigating risks to privacy and enhancing trust in an increasingly interconnected and data-driven world. Some countries have taken positive steps to protect privacy in the context of Covid-19 pandemic. For instance, Immaculate Kassait was sworn in as Kenya's first Data Commissioner in November, following Kenya's National Assembly's (parliament) approval of the President's nomination.[90] Uganda took steps to expand its data protection regulatory framework.[91] Rwanda's Cabinet approved the draft Data Protection Bill in October.[92]

Worryingly, most countries also deployed contact tracing applications (apps) and robotic technologies which rely on contentious features, such as facial recognition and global positioning system (GPS) technology. In Kenya, the Ministry of Health scaled up its Covid-19 contact tracing system (Medic Mobile),[93] while the National Transport and Safety Authority (NTSA) planned to introduce a contact tracing app in June as part of its expansion of Section 30(2) of the NTSA Act 2012 via regulations.[94] These government efforts were mirrored by private entities' efforts, including the development of Bluetooth and geo-sensing technology apps (Linda Application and KoviTrace) by local firms[95] and individuals.[96]

In Rwanda, contact tracing apps relying on phone data profiles, and transmission towers were deployed by RURA in May.[97] Concerningly, reports indicate that Rwanda went a step further and deployed humanoid robots equipped with facial recognition technologies during the same month.[98] Law enforcement agencies have used these digital technologies to monitor individuals in isolation centres as well as track-and-trace individuals who violated Covid-19 rules in public spaces.

In Uganda, a private firm developed a contact tracing application (Covid Tracer) in May which uses overlapped GPS and Bluetooth (smartphone) technologies.[99] Reports indicate that this app will use 'blurred' location history, but it is not clear 'how the blurring is being done or how it effectively traces contact history with blurred data'.[100] In South Sudan, contact tracing initiatives were rolled out, but these were largely analogue processes.[101]

In Ethiopia, the Ministry of Health developed a national Covid-19 surveillance and tracking system with the support of the United States Agency for International Development's Digital Health Activity.[102] Furthermore, it was reported that by June, over seven apps (including the Covid-19 Ethiopia app and Debo) had been developed for contact tracing and data sharing purposes by health workers.[103]

Although these apps and technologies may assist in dealing with the pandemic, ARTICLE 19 EA is concerned that these initiatives were deployed, and continue to be used, without appropriate human rights safeguards.[104] This concern is more pressing due to the failure to uphold transparent and open processes, using publicly available and constant updates, and the lack of a serious, meaningful and transparent engagement between the government, private entities, and the public. Furthermore, data is only as strong as the operating environment within which it is deployed, and all six countries have watered down human rights protections in one way or another.

Specifically, ARTICLE 19 EA is concerned that these digital tools may be used by governments, during and after the pandemic, for surveillance purposes in contravention of various human rights standards and best practices. Crucially, GPS and facial recognition technologies carry significant risks for various individuals and communities, including profiling risks and reduced anonymity protections, and create a chilling effect on the exercise of numerous rights on online platforms, including the freedoms of expression, assembly, and association. This is especially problematic in countries which have held, or are set to hold, their general or parliamentary elections, such as Tanzania in October 2020, Uganda and Ethiopia in 2021, Kenya in 2022, and Rwanda between 2023 and 2024.

Case Study

Digital Rights in Tanzania: The Right to Digital Anonymity and the Decision Affecting the Refusal to Disclose Whistleblowers' Identities

In 2016, three court cases[105] were brought against Maxence Melo, the founder and owner of JamiiForums – an online social networking website – as a result of Melo's alleged refusal to, inter alia, disclose the identities, including 'Internet protocol addresses, email addresses and phone numbers'[106] of whistleblowers exposing corruption scandals on JamiiForums. Melo, in his refusal to comply with police disclosure notices, cited privacy concerns and the need to maintain the digital anonymity of Internet users.

Maxence Melo leaves court in Dar es Salaam yesterday after being convicted of obstructing police investigations. © JamiiForums. Source: CPJ.[107]

Melo was acquitted in one case in 2018, but convicted in two cases in April 2018 and on 8 April 2020.[108] Out of these two convictions, Melo was found to have failed to comply with an order of disclosure of data in his possession under Section 22(2) of the Cybercrimes Act (2015).[109] In the 2018 matter, Melo was ordered to pay a TZS3 million (USD1,300) fine or serve a one-year imprisonment term; however, Melo was released on a 'Conditional Discharge' directing him not to commit a similar offence within one year.[110] Melo's advocates filed a notice of appeal on 8 April contesting the second conviction.

Recommendations

Based on the findings in the report, ARTICLE EA proposes that, at a minimum, the six Eastern Africa countries should adopt the following measures to promote human rights in the digital environment, with the full and effective participation of civil society and other concerned stakeholders:

- Governments should comply with their international, regional, and national freedom of expression and other human rights obligations under international law and standards

- On freedom of expression, governments should refrain from criminalising free speech and ensure that domestic legislation, regulation, and policies imposing criminal restrictions on the right to freedom of expression are repealed and/or amended as follows:

  - **Tanzania** – Repeal the Electronic and Postal Communications (Online Content) Regulations 2020, in its entirety.
  - **Kenya** – Repeal Sections 22 and 23, Computer Misuse and Cybercrimes Act 2018.
  - **Uganda** – Repeal Section 171 of the Penal Code.
  - **Ethiopia** – Repeal the Proclamation on Hate Speech and Disinformation, in its entirety.
  - **Rwanda** – Repeal Articles 22 and 60 of the ICT Law and amend the definition of a 'professional journalist' under Article 2(19) Media Law to recognise citizen journalists and freelance journalists, in line with the UN definition of journalism.
  - **South Sudan** – Repeal Sections 75 and 289 of the Penal Code criminalising the publication or communication of false statements prejudicial to South Sudan and criminalising defamation.

- Governments should also promote societal resilience to 'misinformation', 'disinformation', and 'hate speech' by developing and implementing nationwide civic education and empowerment programmes, alongside multi-stakeholder groups, including CSOs and media actors.

- On **accessibility and affordability** of the Internet and digital technologies, governments should proactively promote the public's right to know by regularly publishing comprehensive annual reports on universal access/service funding mechanisms.

- On **privacy and data protection**, governments should refrain from adopting and using Covid-19 applications without appropriate human rights safeguards, including sunset clauses.

- Furthermore, judiciaries should promote human rights protections in the digital environment by enabling rather than watering down digital anonymity protections.

Endnotes

[1] The police and other investigative agencies have been requesting individuals to appear before them for questioning and/or other investigative reasons.

[2] These mechanisms are referred to differently in the six countries as follows: Rwanda – Universal Access Fund (or UAF, Rwanda); Kenya – Universal Service Fund (or USF); South Sudan – Universal Service and Access Fund (or USAF); Tanzania – Universal Communications Service Access Fund (or UCSAF); Uganda – Rural Communications Development Fund (or RCDF); Ethiopia – Universal Access Fund (or UAF, Ethiopia).

[3] In 2018, the Uganda Communications Commission (UCC) noted that only 15% of persons with disabilities (PWD) (household members) had access to the Internet, whereas a majority (85%) of PWD household members either had no access to the Internet or the individual PWD interviewed did not know. See UCC, *Access and Usage of Information and Communications Technologies (ICTs) by People With Disabilities (PWDs) in Uganda*, December 2018, pp. 46–47.

[4] Office of the United Nations High Commissioner for Human Rights (OHCHR), International Human Rights Law.

[5] Through its adoption in a resolution of the UN General Assembly, the Universal Declaration of Human Rights is not strictly binding on states. However, many of its provisions are regarded as having acquired legal force as customary international law since its adoption in 1948. See *Filartiga v Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).

[6] International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, UN Treaty Series, vol. 999, p. 171.

[7] The African Commission on Human and Peoples' Rights' (ACHPR) African Charter on Human and Peoples' Rights, 1981, came into effect on 25 January 2005.

[8] Human Rights Committee (HR Committee), *General Comment No. 34 on Article 19: Freedoms of Opinion and Expression*, CCPR/C/GC/34, 12 September 2011, para 11.

[9] ACHPR, *Declaration of Principles on Freedom of Expression and Access to Information in Africa*, November 2019, Principle 37.

[10] HR Committee, *Velichkin v Belarus*, Comm. No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

[11] UN Human Rights Council, *Resolution 20/8 on the promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/20/8, 16 July 2012.

[12] General Comment No. 34, para 43.

[13] OHCHR, *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework* (The Ruggie Principles), A/HRC/17/31, 21 March 2011, Annex. The UN HRC endorsed the Guiding Principles in HRC Resolution 17/4, A/HRC/RES/17/14, 16 June 2011.

[14] UN HRC, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Frank La Rue, 16 May 2011, A/HRC/17/27, paras 75–76.

[15] UN HRC, A/HRC/17/27, paras 75–76.

[16] OHCHR, *Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/66/290, 10 August 2011, para 18.

[17] OHCHR, A/66/290, para 22.

[18] UN HRC, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/38/35, 6 April 2018.

[19] The *Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda*, adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe's Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression, and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information on 3 March 2017.

[20] ACHPR, *Declaration of Principles*, Principle 5.

[21] ACHPR, *Declaration of Principles*, Principle 5.

[22] UN HRC, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, David Kaye, A/HRC/29/32, 22 May 2015, para 56.

[23] UN HRC, A/HRC/17/27, paras 53–55.

[24] HR Committee, *General Comment No. 16*, 32nd Session, 1988, UN Doc. HRI/GEN/1/Rev.1 (Vol. I), 8 April 1988, para 3.

[25] HR Committee, HRI/GEN/1/Rev.1, para 8.

[26] UN General Assembly, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, Martin Scheinin, A/HRC/13/37, 28 December 2009, para 17.

[27] UN General Assembly, A/HRC/13/37, para 2.

[28] UN HRC, A/HRC/17/27, para 59.

[29] UN General Assembly, *The Right to Privacy in the Digital Age*, Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014, A/HRC/27/37, paras 23.

[30] ACHPR, *Declaration of Principles*, Preamble.

[31] The African Declaration on Internet Rights and Freedoms, prepared by members of the African Declaration group, is a Pan-African initiative to promote human rights standards and principles of openness in Internet policy formulation and implementation on the continent, 2019.

[32] ACHPR, *Declaration of Principles*, Principle 37.

[33] African Declaration on Internet Rights and Freedoms, Principle 2.

[34] UN HRC, A/HRC/17/27, para 60.

[35] UN HRC, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/38/L.10/Rev.1 38/7, 4 July 2018.

[36] East Africa Radio, 'Waziri Mkuu aagiza hili kupambana na Corona' [video], 21 March 2020.

[37] Faustine Nduguilile [DocFaustine], Tweet on 20 March 2020.

[38] Bob Karashani, 'Posting 'rumours' on social media could land you in Tanzania jail,' *The EastAfrican*, 10 August 2020.

[39] On 20 March, it is reported that Idris Sultan, Doctor Universe, and Isihaka Mwinyimvua were arrested and charged for publishing content online. Sultan was charged for publishing online content on his online TV show, *Loko Motion*, without a licence from the TCRA, in contravention of regulations. See Tevin Sherah, 'Tanzanian comedian Idris Sultan out on Sh368,000 bond,' *The Standard*, April 2020.

[40] On 1 April, Awadhi Lugoya was arrested and charged under the Regulations 2018 for allegedly creating a Facebook account, 'Coronavirus Tanzania'. On 6 April, Afrikana Mlay was interrogated in Kilimanjaro for allegedly publishing false Covid-19 information online and publishing 'unofficial' statistics on Twitter, Instagram, and WhatsApp and appeared in court on 9 April. On 9 April, Mariamu Jumanne Sanane, a university student, was arrested in Shinyanga for allegedly publishing and disseminating false Covid-19 information via WhatsApp and publishing false statistics. See 'TRUE: A Tanzanian man has been arrested on charges of opening a Facebook account to spread Covid-19 misinformation,' PesaCheck, 7 April 2020; 'Tanzanian man held for allegedly spreading false information on Covid-19,' Xinhua, 6 April 2020; and 'Tanzanian university student arrested over spreading Covid-19 rumor,' China.org.cn, 11 April 2020.

[41] On 29 May, it is reported that Zitto Kabwe was found guilty of sedition and incitement and ordered to refrain from writing any seditious material, which could result in Kabwe being sentenced for the offence. See 'Tanzanian court finds opposition leader guilty of sedition, sets him free,' Reuters, 29 May 2020; H. Jumanne, 'Zitto Kabwe sentenced to serve one-year ban not writing seditious statements,' *The Citizen*, 29 May 2020.

[42] Under the Third Schedule, Schedule 10, 'content that is false, untrue, misleading [or] which is likely to mislead or deceive the public' is prohibited, unless it is clearly pre-stated that the content is a satire, parody or fiction; and where it is preceded by a statement that the content is not factual.' See ARTICLE 19, *Tanzania: New Content Regulations Criminalise Free Speech Online*, 31 August 2020.

[43] Joseph Ndunda, 'Robert Alai to spend weekend in custody over 'fake' coronavirus post,' Nairobi News, 20 March 2020.

[44] Kenya Law, *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties) [2020] eKLR*.

[45] Paul Ogemba, 'Win for Senate in supremacy war as court declares 23 laws unconstitutional,' *The Standard*, 30 October 2020.

[46] On 15 March, Elijah Muthui Kitonyo was arrested and threatened with charges under Section 23 of the Computer Misuse and Cybercrimes Act 2018 for allegedly publishing false Covid-19 information on Twitter that was 'calculated or results in panic'. No formal charges were imposed and he was later released. On 25 March, Cyprian Nyakundi was charged under Section 23 of the Computer Misuse and Cybercrimes Act 2018 for 'publishing false information on the Covid-19 pandemic'. On 24 March, Dagoretti South MP John Kiarie presented himself to Dagoretti Division Police Headquarters following a Directorate of Criminal Investigations (DCI) summons over a Covid-19 Twitter thread. Kiarie was not formally charged and his posts were not taken down, but he posted explanatory messages after being released. See DCI Kenya [DCI_Kenya], Tweet of 15 March 2020; Cyrus Ombati, 'Blogger Cyprian Nyakundi arrested over coronavirus post,' *The Standard*, 25 March 2020; Tonny Ndungu, 'MP John Kiarie grilled at DCI office over fake coronavirus tweet,' Citizen Digital, 29 March 2020.

[47] On 18 August, Milton Were (blogger/freelance journalist) and Jack Okinyi (editor) were arrested by the DCI. The Office of the Director of Public Prosecutions rejected the charge sheet raised against Were and Okinyi using Section 23 of the Computer Misuse and Cybercrimes Act 2018. The charge sheet claimed that both had created and posted an article which was 'false and likely to discredit the reputation' of a named individual. On 20 August, Charles Guchuki Ndiang'ui was arrested in connection to a website – currently unavailable – which detailed the extent of corruption in Kenya under the current President's leadership. See ARTICLE 19, *Kenya: ARTICLE 19 Eastern Africa calls for unconditional release of Milton Were and Jack Okinyi*, 25 August 2020; Nelson Havi [NelsonHavi], Tweet of 21 August 2020.

[48] ARTICLE 19, *Kenya: ARTICLE 19 Eastern Africa calls for unconditional release of Milton Were and Jack Okinyi*, 25 August 2020.

[49] Hilary Kimuyu, 'Blogger Alai charged for publishing 'alarming' claims on coronavirus,' Nairobi News, 23 March 2020.

[50] UCC [UCC_Official], 'Public Advisory Notice on Circulation of Fake Information,' 22 March 2020.

[51] See, e.g., ARTICLE 19, *Uganda: Oral Statement Calls for Action in Implementation in UN Universal Periodic Review*, 16 March 2017.

[52] Abu-Bakarr Jalloh, 'Stella Nyanzi, critic of Uganda's President Yoweri Museveni, released from jail,' DW, 20 February 2020.

[53] On 28 March, Pastor Augustine Yiga was arrested and charged for allegedly broadcasting his belief that Covid-19 does not exist in Uganda and Africa. The prosecution claimed that this constituted a 'negligent act likely to spread infection of disease'. On 20 April, Kakwenza Rukirabashaija was charged under Section 171 of the Penal Code (CAP 120) for allegedly 'doing an act likely to spread the infection of disease' on Facebook. This charge was dismissed on 25 August by Magistrate Yunus Ndiwalana. See Conrad Ahabwe, 'COVID-19 CRISIS: Court rejects Pastor Yiga's bail application again, remands him again,' PML Daily, 16 April 2020; Kenneth Kazibwe, 'Court dismisses case against critical book writer, Kakwenza,' Nile Post, 25 August 2020.

[54] On 13 April, Adam Obec, a Kampala Capital City Authority (KCCA) staff member, was arrested for allegedly 'spreading false information regarding coronavirus'. It is unclear whether Obec was formally charged and what legislation, if any, was used. On 20 April, TV anchor, Samson Kasumba, was arrested by plain-clothes officers in Kampala as he left the NBS TV station for alleged seditious activities (Sections 39 & 40, Penal Code). See Kenneth Kazibwe, 'KCCA payroll officer arrested for spreading fake news on first Covid-19

death in Uganda,' *Nile Post*, 13 April 2020; Samson Kasumba, 'Samson Kasumba: "Six months later, I'm still waiting to be charged in court",' Nile Post, 17 October 2020.

[55] Amnesty International, *Uganda: Activist arrested for criticising the president: Kakwenza Rukirabashaija*, 20 April 2020.

[56] RMC [RMC_Rwanda] Tweet of 13 April 2020.

[57] RMC, Tweet of 13 April 2020.

[58] Law No. 02/2013 of 08/02/2013 Regulating Media.

[59] Law No. 24/2016 of 18/06/2016 Governing Information and Communication Technologies, Official Gazette No. 26 of 27/06/2016. This law replaced Law No. 44/2001 of 30/11/2001 governing telecommunications, Law No. 18/2010 of 12/05/2010 relating to electronic messages, electronic signature and electronic transactions, and Decree-Law No. 43/76 of 01/12/1976 on the organisation of the postal service.

[60] ARTICLE 19, *Rwanda: ARTICLE 19 and Access Now contribute to Universal Periodic Review process*, 16 July 2020.

[61] These vague terms, which are present under Article 60 of the ICT Law, include 'false, grossly offensive, indecent, obscene [and] menacing'. The same provision further prohibits the '[persistent use of] public electronic communications network for purposes of causing annoyance, inconvenience, or needless anxiety'. The RURA is mandated to 'make and publish instructions for the implementation of this Article', including the applicable sanctions, but no rules have been issued yet. Law No. 24/2016 of 18/06/2016 Governing Information and Communication Technologies, Official Gazette No. 26 of 27/06/2016.

[62] Law No. 02/2013 of 08/02/2013 Regulating Media, Official Gazette No. 10 of 11 March 2013.

[63] CCPR/C/GC/34, para 44.

[64] On 8 April, bloggers Valentin Muhirwa and David Byiringiro were arrested in relation to their collection of information for a YouTube news channel associated with Afrimax TV. Human Rights Watch, 'Rwanda: Lockdown Arrests, Abuses Surge,' 24 April 2020.

[65] Office of the Prime Minister – Ethiopia, Facebook update from 29 March 2020.

[66] Federal Negarit Gazette of the Federal Democratic Republic of Ethiopia, Proclamation No. 1185/2020 Hate Speech and Disinformation Prevention and Suppression Proclamation, 23 March 2020.

[67] ARTICLE 19, *Ethiopia: Analysis of Draft Law on Hate Speech and False Information*, 28 November 2019.

[68] The Ethiopian Human Rights Commission is only tasked with 'conducting public education awareness campaigns to combat hate speech'. Federal Negarit Gazette of the Federal Democratic Republic of Ethiopia, Article 8(6) of the Proclamation.

[69] ARTICLE 19, *'Hate Speech' Explained: A Toolkit*, 23 December 2019.

[70] Proclamation No. 1185/2020.

[71] Between March and April, broadcast journalist Yayesew Shimelis was charged for various crimes, ranging from the spread of alarming and false information about the Covid-19 pandemic under Article 485 of the Criminal Code, to a violation of anti-terror laws, to the spread of disinformation, in contravention of Articles 5 and 7(4) of the Proclamation. This arrest is alleged to have taken place after Shimelis' YouTube post noting that the government had 'ordered the preparation of 200,000 burial places'. According to the government, Shimelis currently has two charges raised against him, including the false information charges (lodged by the Addis Ababa Police Commission) and the terrorism charge (lodged by the Federal Police Commission). The government claims that the first case is 'adjourned for trial', whereas 'investigations' under the second charge have been 'suspended for the time being due to lack of sufficient evidence'. On 4 April, Elizabeth Kebede was arrested, imprisoned overnight in Addis Ababa, and transported to the Harari region on accusations of 'spreading false Covid-19 information on social media'. Kebede's ordeal stemmed from an alleged Facebook post which 'claimed that an infected person had sat down with two high ranking officials of the Harari region'. As of 11 November, reports indicate that Kebede had not been formally charged because the 'Federal Attorney General of the FDRE [Federal Democratic Republic of Ethiopia] and the Federal Police are still conducting investigations.' See Committee to Protect Journalists, 'Ethiopian journalist Yayesew Shimelis's charges changed to terrorism,' IFEX, 22 April 2020.

[72] The report estimated that mobile broadband penetration in 2018 stood as follows: Kenya (35%), Ethiopia (16%), Uganda (14%), Tanzania (13%), Rwanda (11%), and South Sudan (5%). Additionally, the report estimated that 4G mobile broadband penetration rates in 2018 stood as follows: Uganda (9%), Kenya (8%), Tanzania (6%), Ethiopia (1%), Rwanda (1%), and South Sudan (0%). See Broadband Commission Working Group on Broadband for All, 'Connecting Africa Through Broadband: A strategy for doubling connectivity by 2021 and reaching universal access by 2030,' October 2019, Figures 4.1 & 4.2, pp. 60 & 61.

[73] Kenya's government affirmed the existence of a 'wide "digital divide" in the access to connectivity services in the country.' See Communications Authority of Kenya, 'Digital Economy Blueprint: Powering Kenya's Transformation,' 2019, p. 49. In 2018, the UCC noted that only 15% of persons with disabilities (PWD) (household members) had access to the Internet, whereas a majority (85%) of PWD household members either had no access to the Internet or the individual PWD interviewed did not know. See UCC, 'Access and Usage of Information and Communications Technologies (ICTs) by People With Disabilities (PWDs) in Uganda,' December 2018, pp. 46–47.

[74] Broadband Commission Working Group on Broadband for All, *Connecting Africa Through Broadband,* p. 47.

[75] Ministry of Information, Communication Technology, and Postal Services, *Universal Service and Access Fund Secretariat – Six Months Report*, April 2020.

[76] Rwanda RURA, *Annual Report 2018–2019*, 22 October 2019, pp. 38–39; Kenya – Communications Authority of Kenya, *Annual Report for the Financial Year 2018–2019*, p. 20; Tanzania – UCSAF, *Project Report – January 2020*, pp. 1 & 11 ; South Sudan – Ministry of Information, Communication Technology and Postal Services, *Universal Service and Access Fund Secretariat – Six Months Report*, April 2020.

[77] Regulation 28(1) of the UCSAF's Regulations (2009) requires the fund to 'maintain a register of universal service provision which shall include the following: a) Designated service providers; b) A list of licensees contributing to the fund; and c) A list of information required by the fund when determining designated universal service providers.' See UCSAF, UCSAF Public Register.

[78] UCC, *RCDF Operational Guidelines 2017/18–2021/22 (RCDF III)*, pp. 29.

[79] Ethiopia has postponed its August 2020 elections by at least nine months (they are now likely to take place in March 2021) due to Covid-19 concerns and is facing a looming constitutional crisis as a result of the Ethiopian parliament's extension in mid-June of Prime Minister Abiy Ahmed's stay in office, as well as parliament's own term lapse in October. See 'Ethiopian parliament allows PM Abiy to stay in office beyond term,' Al Jazeera, 10 June 2020; Zecharias Zelalem, 'Ethiopia's decision to delay its election for Covid will have consequences for its democratic goals,' QuartzAfrica, 18 June 2020.

[80] '"Hundreds dead" as conflict in Ethiopia's Tigray worsens,' Al Jazeera, 9 November 2020.

[81] ARTICLE 19, *Ethiopia: Killing of protesters must be investigated*, 2 July 2020.

[82] Addis Getachew, 'Ethiopia restores Internet partially after weeklong ban,' Anadolu Agency, 9 July 2020.

[83] Tesfa-Alem Tekle, 'Month-long Internet shutdown cost Ethiopia over $100m: NetBlocks,' *The EastAfrican,* 27 July 2020.

[84] NetBlocks Cost of Shutdown Tool (COST).

[85] 'Critics decry Magufuli's "unprecedented" win, rivals' elimination,' Al Jazeera, 9 November 2020.

[86] 'Internet disrupted in Tanzania on eve of general elections,' NetBlocks, 27 October 2020.

[87] Twitter Public Policy, [Tweet] of 27 October 2020.

[88] TCRA, Directive on Temporal Suspension of Bulk Messaging and Bulk Voice Calling Services, 21 October 2020.

[89] Ambassador Donald J. Wright [USAmbTanzania], [Tweet], 2 November 2020.

[90] Davis Ayega, 'Kassait to be sworn in as Data Commissioner after House approval,' Capital News, 6 November 2020. Elias Okwara, 'Kenya appoints its first ever data protection commissioner,' IAPP, 1 December 2020.

[91] Ministry of ICT & National Guidance, *Data Protection and Privacy Regulation, 2020*.

[92] Republic of Rwanda, Office of the Prime Minister, Statement on Cabinet Decisions of 27 October 2020.

[93] 'Kenya reveals digital tracing system,' Geneva Internet Platform, 13 July 2020.

[94] Frankline Sunday, 'NTSA plans mandatory cashless fare payment,' *The Standard*, 3 June 2020.

[95] Joseph Muraya, 'Kenya: 3 Tech Firms Develop Mobile Application to Support Covid-19 Contact Tracing,' allAfrica, 12 April 2020.

[96] Mary Wambui, 'Kenya: Hope as Three Kenyans Develop App for Contact Tracing,' allAfrica, 17 June 2020.

[97] Moses K. Gahigi, 'Rwanda Opts for Digital Tools in Covid-19 Contact Tracing,' allAfrica, 2 May 2020.

[98] Arafat Mugambo, 'Rwanda Deploys Robots in Treating Covid-19 Patients,' allAfrica, 12 May 2020.

[99] Kelvin Atuhaire, 'Ugandans Develop App for Covid-19 Contact Tracing,' allAfrica, 23 May 2020.

[100] Chas Kissick, Elliot Setzer, and Jacob Schu, 'What Ever Happened to Digital Contact Tracing?,' LawFare, 21 July 2020.

[101] Christine Maema, 'South Sudan confirms 72 more Covid-19 cases,' CGTN Africa, 12 June 2020.

[102] JSI, 'Ethiopia's Digital Health Response to Covid-19,' 14 May 2020.

[103] Simon Marks, 'Ethiopian Diaspora Champions Digital Apps in Fight Against Covid,' VOA News, 3 June 2020.

[104] ARTICLE 19, *Coronavirus apps and human rights: what you need to know*, 13 May 2020.

[105] In 2018, Melo was acquitted (Case No. 457) for allegedly failing to comply with an order to 'disclose of data in his possession' under Section 22(2) of the Cybercrimes Act (2015). The third case relates to Melo's 'management of a domain not registered in Tanzania under Section 79(c) of the Electronic and Postal Communications Act (2010)'. This matter was determined in November 2020. See Paradigm Initiative, *Case Study: Maxence Melo and the Right to Privacy*, 27 October 2019.

[106] Paradigm Initiative, *Case Study*.

[107] Committee to Protect Journalists, 'Tanzanian court convicts Maxence Melo of obstructing investigation, levies fine,' 9 April 2020.

[108] Case references: Criminal Case No. 456 & 458 of 2016.

[109] Section 22 of the Cybercrimes Act (2015).

[110] Case reference: Criminal Case No. 458 of 2016.