Module 2

Restricting Access and Content

Advanced Modules on Digital Rights and Freedom of Expression Online in Sub-Saharan Africa

MEDIA DEFENCE

ISBN 978-0-9935214-1-6

Published by Media Defence: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in February 2024

TABLE OF CONTENTS

MODULE 2

RESTRICTING ACCESS AND CONTENT

The objectives of this module are:

- **To provide an overview of the current mechanisms through which access to the internet and access to content is restricted;**
- **To outline the fundamental international and regional legal principles relating to access;**
- **To unpack the different rights affected by such restrictions;**
- **To set out the limitations of implicated rights and explore the justifiability of the measures adopted by states; and**
- **To identify practical ways to deal with restrictions.**

INTRODUCTION

The internet was created to facilitate the free flow of information;[1] it now allows people to instantaneously access information and services, to communicate, and to share knowledge and ideas. The internet offers an array of opportunities for the realisation of human rights and has, in many instances, been a catalyst for the empowerment of marginalised members of society. It is common cause that the internet is an enabling space for the advancement of the right to freedom of expression, the right of access to information, the right of freedom of assembly, the right to freedom of opinion, thought and belief, the right to be free from discrimination in all forms, the right to education, the right to culture and language, and the right of access to socio-economic services.

Access to the internet is a crucial component of social, economic, and human development, particularly in the African context. The Declaration of Principles of Freedom of Expression and Access to Information in Africa (African Declaration), adopted by the African Commission on Human and Peoples' Rights (ACHPR) in 2019, calls for states to facilitate the rights to freedom of expression and access to information online and to provide the means to exercise these rights.[2] It further highlights that universal, equitable, affordable, and meaningful access to the

[1] Internet Society, 'Brief History of the Internet' (1997) (accessible here).
[2] ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2019) (accessible here).

internet is necessary for the realisation of freedom of expression, access to information and the exercise of other human rights.

However, a range of restrictions to internet access are eroding the right to freedom of expression and associated rights.[3] Suppressive tactics by governments and private actors cause significant challenges in accessing information online. As will become apparent, the unjustifiable restriction of access to the internet is a violation of human rights. This module outlines some of the prevalent harms to access and provides guidance on how to secure fundamental rights and freedoms in the digital age. In doing so, this module focuses on internet shutdowns, the ways in which access to content may be unjustifiably limited through blocking and filtering, the implications of social media taxes, and the harms of distributed denial of service (DDoS) attacks.

INTERNET SHUTDOWNS

Overview of internet shutdowns

An internet shutdown typically involves the deliberate disruption of internet or electronic communications, to the extent that they become either partially or fully inaccessible or unusable. Internet shutdowns often target a particular population or a specific location with the objective of exerting control over the free flow of information in that area, but they have also sometimes affected entire countries. Internet shutdowns, which are sometimes referred to as a "blackout" or "kill switch," include full and localised shutdowns, bandwidth throttling, and service-based blocking of two-way communication platforms.[4]

Internet shutdowns on the rise

Internet shutdowns are unfortunately on the rise*:* in 2022 the #KeepItOn coalition documented at least 187 internet shutdowns in 35 countries around the world, compared to 76 in 2016.[5] These figures highlight the rise of this new trend in which governments seek to silence dissenting voices, control information and curb freedom of expression.

A clear example of this can be seen in Zimbabwe, which experienced internet shutdowns in 2022,[6] despite an interim court ruling in 2019 ordering that internet services be restored after a similar shutdown.[7] Further, there were reports of the quality of internet access being degraded ahead of the 2023 elections.[8] Of additional concern is the protracted duration of

[3] See Tim Berners-Lee, 'I Invented the web. Here are three things we need to change to save it' (2017) (accessible here).
[4] See Access Now, 'What is an internet shutdown?' (2019) (accessible here) and Media Defence, 'Training Manual on Digital Rights and Freedom of Expression Online'. See further Access Now, 'Launching STOP: the #KeepItOn internet shutdown tracker' (2017) (accessible here) and Indian Council for Research on International Economic Relations, 'The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India' (2018) (accessible here).
[5] Access Now, '#KeepItOn' (accessible here).
[6] Access Now, 'Zimbabwe elections 2023: voters need internet access' (2023) (accessible here).
[7] Access Now, 'Zimbabwe orders a three-day, country-wide internet shutdown' (2019) (accessible here).
[8] Reliefweb, 'Zimbabwe: Elections marred by arbitrary arrests and fears of internet shutdown" (2023) (accessible here).

the shutdowns. At the time of this module's latest update, there have been ongoing shutdowns in the Tigray region of Ethiopia for more than 3 years.[9]

The #KeepItOn coalition is actively monitoring links between elections set to take place in 2024 and has concerningly pinpointed at least 23 countries where there is a significant risk of internet shutdowns occurring during election periods.[10] Mauritania, Togo, Chad, Tanzania, Somaliland, Guinea Bissau, Ghana, Algeria, and South Sudan are on the watchlist for 2024.

Internet shutdowns are used by states to limit opposition and disarm dissent and are often used during critical periods such as elections or times of mass protest. They pose severe threats to people's rights and are contrary to international human rights standards.

International and regional responses

Over the last decade, the exponential growth in access to the internet has led to the corresponding development of international norms and standards regarding the use of the internet and the various rights it invokes. In the context of internet shutdowns, the rights to freedom of expression, access to information, and association and assembly rights contained in articles 19 and 21 of the International Covenant on Civil and Political Rights (ICCPR) are primarily implicated.

International guidance on this issue goes some time back. In 2011, the United Nations Special Rapporteur on Freedom of Expression (UNSR on FreeEx) reported to the United Nations General Assembly that:

> "the Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression, as guaranteed by article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."[11]

In 2012, the UN Human Rights Council (UNHRC) unanimously adopted a Resolution to protect the free speech of individuals on the internet. This Resolution was the first of its kind and notably called upon states to "promote and facilitate access to the Internet." It affirmed that:

> "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."[12]

In recent years there have been more explicit statements concerning internet shutdowns:

[9] Access Now, 'Who is shutting down the internet in 2023? A mid-year update' (2023) (accessible here).
[10] Access Now, '2024 elections and internet shutdown watch' (2024) (accessible here).
[11] UNHRC, 'Report of UNSR of FreeEx' (2011) (accessible here).
[12] UNHRC, 'The promotion, protection and enjoyment of human rights on the internet: Resolution' (2012) (accessible here).

- In 2016, the UNHRC expressed deep concern regarding "measures aiming to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law."[13]
- In 2017, the UNSR on FreeEx reported that "Internet and telecommunications shutdowns involve measures to intentionally prevent or disrupt access to or dissemination of information online in violation of human rights law,"[14] explaining further that shutdowns "ordered covertly or without an obvious legal basis violate the requirement of Article 19(3) of the [ICCPR] that restrictions be 'provided by law'."
- In 2018, the UNHRC expressed its deep concern "at measures in violation of international human rights law that aim to or that intentionally prevent or disrupt access to or dissemination of information online."[15]
- In 2019, the UNSR on FreeEx reiterated that internet shutdowns are clearly inconsistent with article 19(3) of the ICCPR.[16]
- In 2020, the UNHRC strongly condemned the use of internet shutdowns "to intentionally and arbitrarily prevent or disrupt access to or dissemination of information online."[17]
- In June 2022, the UN High Commissioner for Human Rights presented a report to the UN General Assembly highlighting the severe human rights impacts of internet shutdowns, including the fact that they "very rarely meet the fundamental requirements of necessity and proportionality," and providing a set of recommendations for ending shutdowns, including calling on states to refrain from the full range of internet shutdowns.[18]
- In October 2022 the UNSR on FreeEx presented a report concerning the protection of freedom of expression during armed conflict, noting that internet shutdowns undermine human rights and are not legitimate warfare tactics.[19]
- In 2023, UN experts raised alarm on internet shutdowns in Gaza that are disrupting essential communications and reporting on the conflict.[20]
- In the 2023 Report to the UNHRC, the UNSR on FreeEx noted that internet shutdowns continue to occur with severe impacts on freedom of expression and peaceful assembly as well as on economic and social rights such as education, health, and essential online services like financial services.[21] The report highlighted that the intentional disruption of access to the internet constitutes a disproportionate interference with the right to freedom of expression and has been considered by various UN human rights mechanisms and regional courts to be a violation of international human rights law.

---

[13] UNHRC, 'The promotion, protection and enjoyment of human rights on the internet: draft resolution' (2016) (accessible here).
[14] UNHRC, 'Report on UNSR on FreeEx' (2017) (accessible here).
[15] UNHRC, 'Resolution adopted by the Human Rights Council on 5 July 2018' (2018) (accessible here).
[16] UN General Assembly, 'Promotion and protection of the right to freedom of opinion and expression' (2019) (accessible here).
[17] ARTICLE 19, 'HRCC: Un resolution on freedom of opinion and expression' (2020) (accessible here).
[18] UNHRC, 'Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights – Report of the Office of the United Nations High Commissioner for Human Rights' (2022) (accessible here).
[19] UN Office of the High Commissioner, 'Protect freedom of expression as a vital survival right of civilians in armed conflict: UN expert' (2023) (accessible here).
[20] UN Office of the High Commissioner, 'Gaza is running out of time UN experts warn, demanding a ceasefire to prevent genocide' (2023) (accessible here).
[21] UNHRC, 'UNSR on FreeEx: Report on sustainable development and freedom of expression: why voice matters' (2023) (accessible here).

Decisive regional law on access to the internet

In her 2023 report, the UNSR on FreeEx most notably cites the case of *SERAP v Federal Republic of Nigeria* (2022) in the Community Court of Justice of the Economic Community of West African States (ECOWAS Court), which held that the Nigerian government had violated the right to freedom of expression, access to information, and of the media by suspending the operations of social media platform Twitter in the country. Also of note is the fact that the UNSR of FreeEx submitted an *amicus curiae* brief in that matter, which clearly set out the international law position, and is available for review here.

In an African context, the 2019 Declaration of Principles on Freedom of Expression in Africa provides that:[22]

> "States shall not interfere with the right of individuals to seek, receive and impart information through any means of communication and digital technologies, through measures such as the removal, blocking or filtering of content, unless such interference is justifiable and compatible with international human rights law and standards.
>
> States shall not engage in or condone any disruption of access to the internet and other digital technologies for segments of the public or an entire population."

African bodies have also explicitly expressed their condemnation of internet shutdowns:

- In 2019, the ACHPR's Special Rapporteur on Freedom of Expression and Access to Information expressed concern about the continuing trend of internet shutdowns in Africa and noted that shutdowns violate the right to freedom of expression and access to information contrary to Article 9 of the African Charter on Human and People's Rights.[23]
- In 2020, the ACHPR Special Rapporteur again expressed his concern about internet shutdowns in Africa, stressing the importance of internet access for containing the spread of COVID-19 and enabling journalists to verify the information and update the public on measures governments were taking to deal with the virus.[24]
- In 2023 the ACHPR Special Rapporteur, together with other regional and international Special Rapporteurs, issued a joint declaration on Media Freedom and Democracy in which they implore States to refrain from imposing internet shutdowns and thereby prevent access to information, undermining journalistic work, and abet the perpetration of human rights violations.[25]

[22] African Declaration above n 2.
[23] ACHPR, 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa' (2019) (accessible here).
[24] ACHPR, 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Importance of Access to the Internet in Respondent to the COVID-19' (2020) (accessible here).
[25] ACHPR, 'Joint Declaration on Media Freedom and Democracy' (2023) (accessible here).

The above standards make it clear that internet shutdowns result in rights violations, and these reports and resolutions are important for establishing the rights-based framework relating to internet shutdowns. The practicality of litigating against states requires a nuanced understanding of the international human rights standards of **legality**, **necessity**, and **proportionality** and when there can be reasonable and justifiable limitations on fundamental human rights, particularly the right to freedom of expression.

Legality, necessity, and proportionality

Central to litigating internet shutdowns is establishing that the measure violates the right to freedom of expression and access to information, among others, such as the right to health and education. As discussed above, internet shutdowns violate the full enjoyment of the right to freedom of expression. However, since freedom of expression is not an absolute right, it may be limited in certain circumstances, but only when, according to international human rights law, the limitation is "provided by law" and "necessary" to ensure "respect of the rights or reputation of others" or for "the protection of national security or of public order (*ordre public*), or of public health or morals."[26]

States often rely on this exception of "national security" or "public order" to justify internet shutdowns. When litigating the issue of internet shutdowns, it is important to conduct a thorough limitations analysis in order to illustrate to a court that a right has been infringed and that the limitation does not meet the threshold of Article 19(3) of the ICCPR.

Note on the limitation of freedom of expression

Article 19(3) of the ICCPR sets out the grounds upon which the right to seek, receive, and impart information and ideas on the internet may be limited. The restriction must be:

1. **Provided by law.**
2. **Be necessary for**:
   - Respect for the rights of others.
   - The protection of national security or of public order (*ordre public*), or of public health or morals.
     - ➔ These are understood as the "legitimate grounds for restrictions."

The UNHRC, through General Comment 34, has given further scope to the understanding of Article 19(3):[27]

The restrictions must be **provided by law**:[28]

[26] Article 19 of the International Covenant on Civil and Political Rights (accessible here).
[27] UNHRC, 'General Comment 34: Article 19 Freedoms of opinion and expression' (2011) (accessible here).
[28] The UNSR FreeEx 2019 Report explains that "The restriction must be provided by laws that are precise, public and transparent; it must avoid providing authorities with unbounded discretion, and appropriate notice must be given to those whose speech is being regulated. Rules should be subject to

- The law must be clear (be formulated with sufficient precision to enable an individual to regulate their conduct accordingly) and accessible, and apply equally to everyone.
- The law must also be consistent with international human rights law.
- It must provide sufficient guidance on remedies and procedures for challenging non-compliance with the law.
- It is for the state to demonstrate the legal basis for any restrictions imposed on freedom of expression.

Directions or instructions from state departments or actors are insufficient to meet this legality threshold.

The restriction must be **necessary**:

- It must respect the rights or reputations of others. The UNHRC explains that for example, it may be legitimate to restrict freedom of expression to protect the right to vote. The UNHRC cautions that restrictions must be constructed with care: while it may be permissible to protect voters from forms of expression that constitute intimidation or coercion, such restrictions must not impede political debate, including, for example, calls for the boycotting of a non-compulsory vote.
- It must be aimed at the protection of national security or of public order (*ordre public*), or of public health or morals. Here the UNHRC explains that restrictive laws used for the pursuit of national security cannot be used to suppress or withhold from the public information of legitimate public interest if it does not harm national security. Journalists, researchers, environmental activists, human rights defenders, or others cannot be prosecuted for having disseminated such information if it does not harm national security. Relying on the justification of national security to stifle advocacy and activism is prohibited and merely alleging the justification of national security is insufficient.

The UNHRC explains further that the above grounds must conform to the strict tests of **necessity** and **proportionality:**[29]

- Restrictions must be "necessary" for a legitimate purpose.
- Restrictions must not be overbroad. The UNHRC emphasised that restrictive measures must conform to the principle of proportionality:
    - They must be appropriate to achieve their protective function.
    - They must be the least intrusive instrument amongst those which might achieve their protective function.
    - They must be proportionate to the interest to be protected.

public comment and regular legislative or administrative processes. Procedural safeguards, especially those guaranteed by independent courts or tribunals, should protect rights." See UN General Assembly above n 16.

[29] The UNHRC explains: "Fundamentally, any restriction or limitation must not undermine or jeopardise the right to freedom of expression itself. Additionally, restrictions must be consistent with other rights found in the ICCPR and the fundamental principles found in the UDHR." See UNHRC, 'General Comment 34 above n 27.

- The principle of proportionality must be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law.

Internet shutdowns are seldom proportionate and are generally viewed as a "disproportionate restriction on the right to freedom of expression, and have serious repercussions for the protection of other human rights."

If a state cannot fulfil these requirements, then the restriction amounts to an unjustifiable and disproportionate limitation of the right. Echoing this and responding to the internet shutdown crisis in Kashmir in 2019, several UN Special Rapporteurs recorded that "[t]he shutdown of the internet and telecommunication networks, without justification from the Government, are inconsistent with the fundamental norms of necessity and proportionality."[30]

Recent examples of litigation relating to internet shutdowns

Despite these clear standards, states continue to claim that measures taken to restrict the internet are necessary and proportionate to ensure national security or public order, or both. Fortunately, there have been instances in which courts have handed down decisions providing that these justifications do not warrant internet shutdowns and where the threat of litigation itself has proved successful.

Domestic Courts

Cameroon

In 2017, a case was brought before the Constitutional Council in Cameroon which challenged the state's decision state to shut down the internet in the South West and North West of the country — the majority English-speaking regions — following language-related protests.[31] Civil society actors filed a challenge demanding that the state restore access to the internet in these regions,[32] after which access to the internet was restored without the need for a judicial determination.[33] As stated by Access Now, this showed that "simply filing the lawsuit can get results, like increased transparency and responsiveness from telcos or the state."[34]

[30] UN Office of the High Commissioner, 'UN rights experts urge India to end communications shutdown in Kashmir' (2019) (accessible here).
[31] Al Jazeera, 'Cameroon internet shutdowns cost Anglophones millions' (2018) (accessible here).
[32] Media Defence, 'Media Defence and Veritas Law Bring Case Before the Constitutional Council of Cameroon Challenging Internet Shutdown,' (2017) (accessible here).
[33] Media Defence along with Veritas Law were the applicants challenging the internet shutdown. Media Defence stated: "The case that has been brought highlights that open and accessible internet communications are essential to ensuring the right to freedom of expression. Disruption of online services, whether through website blocking or internet shutdowns, amounts to a serious violation of that fundamental right. The government of Cameroon is obliged under domestic and international legal obligations to protect freedom of expression, including ensuring that it remains accessible and that people are able to use it freely and without interference."
[34] AccessNow, 'Judges raise the gavel to #KeepItOn around the world,' (2019) (accessible here).

In a subsequent legal challenge brought before the Supreme Court of Cameroon, sitting as the Constitutional Council of Cameroon, seeking a declaratory judgment on the internet shutdown, the court dismissed the application for lack of *locus standi*, noting that the Constitution does not empower civil society organisations to file matters before it.[35]

Zimbabwe

In January 2019, an urgent chamber application was filed by Zimbabwe Lawyers for Human Rights (ZLHR) and the Media Institute of Southern Africa-Zimbabwe Chapter (MISA-Zimbabwe) challenging the ongoing internet shutdowns in Zimbabwe at that time, which were reportedly imposed in response to mass political protests and to provide cover for security forces to implement a violent crackdown.[36] The High Court granted an interim order that the implicated mobile operator must immediately and unconditionally resume full services and thus ensure access to the internet.[37] The Court's ruling was mainly based on the absence of a legal provision enabling the shutdown.

While this resulted in the eventual restoration of access, internet shutdowns in Zimbabwe have persisted in the intervening years. For example, there were internet shutdowns again in 2022[38] and once more in 2023 ahead of elections in the country.[39]

Zambia

In August 2021, internet access was shut down during the Zambian general elections. The incumbent president ostensibly conducted this shutdown "in an effort to maintain peace and during the voting period." This led a Zambian NGO, Chapter One Foundation, to approach the High Court to review the Zambian Information and Communications Technology Authority's decision to interrupt internet access.[40]

The parties ultimately came to an agreement, which was made an order of court by the High Court, whereby the Zambian Information and Communications Technology Authority:

> "would not do any act or make any omission outside of their legal regulatory authority which may inhibit or interrupt the flow of an uninhibited access to information on all available telecommunication platforms under their control and/or regulation where the interest of consumers and their consumer and constitutional rights are threatened."

[35] *Cameroon v. Ministry of Posts and Telecommunications and Others* (2018) (accessible here).
[36] Zimbabwe Lawyers for Human Rights, 'Zim Court Hears Challenge of Internet Blockade' (2019) (accessible here).
[37] Bloomburg, 'Zimbabwe Lawyers Sue Mobile Operators Over Internet Shutdown' (2019) (accessible here).
[38] Access Now, 'Zimbabwe elections 2023: voters need internet access' (2023) (accessible here).
[39] Reliefweb, 'Zimbabwe: Elections marred by arbitrary arrests and fears of internet shutdown' (2023) (accessible here).
[40] *Chapter One Foundation v. Zambian Information and Communications Technology Authority* (2021) (accessible here).

Further, and importantly for government accountability, the Information and Communications Technology Authority agreed to inform the public as to the cause of any internet disruption within 36 hours of the event.

Sudan

After an internet shutdown in the country in 2019, a Sudanese lawyer launched a legal challenge that successfully resulted in an order for the service provider to restore his access.[41] However, the order did not extend beyond his single SIM card due to his filing the suit in his personal capacity as a customer. This was then followed by a class action suit which eventually resulted in the court ordering multiple service providers to restore access for all customers, as well as provide apologies to their customers.

In a subsequent lawsuit brought in 2021 against another shutdown, the Sudanese Consumer Protection Organisation succeeded in securing an order for all internet service providers (ISPs) to restore access for all subscribers.[42] When the Telecommunication and Post Regulatory Authority (TPRA) insisted on maintaining the shutdown despite the court order on the grounds of national security, the court issued a warrant of arrest for the chief executives of the ISPs which finally resulted in access being restored.

Uganda

Unfortunately, some domestic legal challenges have not proven successful. In 2021 the Ugandan Constitutional Court dismissed an application challenging the government's disruption of internet as well as mobile money services in the country during the 2016 general elections. The court held that the shutdown was permissible by law and involved no constitutional issues.[43]

Regional courts

Nigeria

In 2021, the federal government suspended social media site Twitter after it removed content posted by President Muhammadu Buhari which threatened to punish regional secessionists.[44] The ban was in place for seven months before Twitter agreed to several of the government's demands, including opening a local office in Nigeria.

The ban was subsequently challenged in the ECOWAS Court in a case brought by the Socio-Economic Rights and Accountability Project (SERAP) and joined with other similar cases. The Court held that access to Twitter was a "derivative right" that was "complementary to the enjoyment of the right to freedom of expression." As such, any derogation from that right must

[41] CIPESA, 'Litigating Internet Disruptions in Africa: Lessons from Sudan,' (2022) (accessible here).
[42] Id.
[43] The Independent, 'Constitutional court dismisses petition challenging internet, mobile money shutdown during elections,' (2021) (accessible here). See also the brief on the Columbia Case Law Database here.
[44] Al Jazeera, 'Nigeria ends its Twitter ban after seven months' (2022) (accessible here).

be lawfully justified by either an existing law or an order of the Court, something which the government had failed to show.

Consequently, the Court held that the ban violated the right to freedom of expression, access to information and the media as set out in Article 9 of the African Charter on Human and People's Rights (ACHPR) and Article 19 of the ICCPR. It further ordered the government to prevent such a repetition. Media Defence and Mojirayo Ogunlana-Nkanga represented the applicants.[45]

Guinea

In 2020, the Guinean government disrupted access to the internet and banned demonstrations as well as arrested demonstrators, journalists, and civil society activists amidst protests concerning the President's amendment of the Constitution that would effectively allow him to remain in power. Consequently, an NGO brought a case to the ECOWAS Court on the basis that the government had violated their right to freedom of expression and right to information.[46] The Applicants argued that the government's actions in shutting down the internet violated Article 9 of the African Charter, Paragraph 19 of the ICCPR, and Paragraph 66 of the ECOWAS Revised Treaty.

The Court noted that the aim of the right to information is to enable citizens to participate usefully in the democratic process and in decisions concerning their future. Access to information is considered the foundation of democracy. It held that the right to information is an extension of freedom of the press and freedom of expression and that any unjustified measure which aims to suspend or restrict free access to information constitutes a violation of the right to information. As such, the government's actions in interrupting access to the internet without justification constituted a violation of the right to information.

Similarly, the Court held that the right to freedom of expression is an essential right which guarantees the exercise of freedom of the press and is a necessary and indispensable element of any democratic society. Importantly, the Court found that states not only have an obligation to refrain from interfering with this right, but they also must adopt all necessary measures to give effect to it. It emphasised that any restriction or limitation to the right to freedom of expression is only justified if it is provided by law, serves a legitimate interest, is necessary and proportionate, and respects the rights of others, the collective security, morality, and the common interest. The government did not meet these requirements and, as such, they were found to have violated the Applicants' right to freedom of expression. Guinea was ordered to take all necessary measures to ensure that these violations do not occur in the future and to adopt and implement laws, regulations, and safeguards to fulfil its obligations regarding the right to freedom of expression under international human rights instruments.

Togo

In 2017, the Togolese government enacted an internet shutdown in response to protests over President Faure Gnassingbé's efforts to pursue a fourth term in power. Seven local CSOs,

[45] *SERAP v. Federal Republic of Nigeria* (2022) (accessible here).
[46] *Association des Blogueurs de Guinée and Others v. State of Guinea* (2023) (accessible here).

including Amnesty International Togo and an individual blogger-activist, applied to the ECOWAS Court arguing a violation of Article 9 of the African Charter, as well as that the shutdown prevented their ability to carry out their work and damaged their reputation and finances.[47]

The government justified the shutdown in terms of national security, claiming that there was a spread of hate speech and incitement online which risked a civil war. As described by the Global Freedom of Expression Database at Columbia University:

> "The Court found that access to the internet is a "derivative right" as it "enhances the exercise of freedom of expression." As such, internet access is "a right that requires protection of the law" and any interference with it "must be provided for by the law specifying the grounds for such interference." [p. 11] As there was no national law upon which the right to internet access could be derogated from, the Court concluded that the internet was not shut down in accordance with the law and the Togolese government had violated Article 9 of the African Charter on Human and Peoples' Rights. The Court subsequently ordered the Respondent State of Togo to take measures to guarantee the "non-occurrence" of a future similar situation, implement laws to meet their obligations with the right to freedom of expression and compensate each applicant to the sum of 2,000,000 CFA (approx. 3,500 USD)."

The Court also established that non-natural persons, including CSOs, can bring claims to protect their right to freedom of expression in the ECOWAS Court.[48]

Benin: a case study on the importance of procedure

In 2019 the government of Benin shut down internet access on the day of legislative elections. This sparked several individuals to bring a case to the African Court of Human and Peoples' Rights (African Court), where they argued that the shutdown violated their right to freedom of opinion and expression in terms of Article 19 of the UDHR.[49] In 2023, the court delivered its judgment, ultimately dismissing the case as the Applicants did not meet admissibility requirements. This judgement serves as an important reminder of the importance of complying with procedure in litigation.

[47] Global Freedom of Expression: Columbia University, 'Amnesty International Togo and Ors v. The Togolese Republic,' (2020) (accessible here).
[48] Id. Access Now, which intervened in the case as a friend of the court along with a group of other CSOs, stated: "The ECOWAS Togo decision is generally consistent with existing international law, such as Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and the UN Human Rights Committee (UNHRC)'s General Comment No. 34 on Article 19 ICCPR, which state that no internet restrictions are permissible unless they are provided by law. However, the court did not address the necessity and proportionality requirements outlined in General Comment No. 34, including that any restrictions on the freedom of expression, such as internet shutdowns, "must be the least intrusive instrument amongst those which might achieve their protective function." This is the key question that should be asked whenever a government is contemplating shutting down an entire internet network or service: would a less harmful step be effective? Nevertheless, the court did order the government of Togo to enact the law protecting freedom of expression that would be consistent with international human rights instruments in the future. This means that the Togolese government should enact legislation protecting its citizens' rights from any disproportionate restrictions on their expression."
[49] *Adelakoun and Others v Republic of Benin* (2023) (accessible here).

Notably, the Court held that the Applicants did not exhaust all local remedies available to them before approaching the Court, and failed to provide sufficient evidence showing that local remedies were unavailable or ineffective. Therefore, the Court found the application to be inadmissible.

Tips to consider when litigating internet shutdowns

Several resources are available providing guidelines and tips on how to litigation internet shutdowns in Africa, dealing with practical issues such as the documentation of evidence and procedural steps:

- Michael Gyan Nyarko & Tomiwa Ilori, "Litigating Internet Shutdowns in Africa: A Guide on Approaching the African Commission on Human and Peoples' Rights and the African Court on Human and Peoples' Rights."
- Dunia Mekonnen Tegegn (CIPESA), "Advancing Strategic Litigation on Internet Shutdown Cases in Africa: Promises and Pitfalls."

For election-related shutdowns, Access Now's election toolkit provides guidance on how to prevent and respond to internet shutdowns.

A guide from the Southern African Litigation Centre also highlights the legal considerations for legal action on internet shutdowns in various courts in the region:

- **The parties**: consider the impact of the shutdown and whether it is necessary to identify specific categories of applicants and respondents. Identify who is responsible for ordering the shutdown and who implemented it.
- **The procedure and the relief**: consider if the case requires urgent litigation and interdicts, injunctions, or judicial reviews. Consider the type of precedent the case will set.
- **The law**: consider whether there are existing laws that prescribe blockage orders. If there are, consider whether the government has complied with them and consider if the laws themselves are in accordance with human rights standards.
- **The rights**: consider which rights were violated and consider responses to government justifications.

The growing number of shutdowns internationally and in Africa is of grave concern. Fortunately, there is a simultaneous growth of activism and litigation that is working towards curbing these continued rights violations, and progress has been made in recent years in developing domestic and regional jurisprudence condemning such shutdowns, as well as in the publication of international law instruments and guidance that can be referenced to show the firm international human rights law position on the subject. However, until states refrain from blanket bans over access to the internet through shutdowns, there will be a continued need for strategic litigation, activism, and advocacy.

CENSORSHIP, BLOCKING AND FILTERING

Overview of censoring, blocking, and filtering of content

Access to information is a central tenet of the internet. However, efforts to restrict access have developed in step with improved infrastructure and technology that should enable access. Technical measures are being implemented in many jurisdictions by state and non-state actors to limit, influence, monitor, and control people's access to content on the internet. These measures include censoring, blocking, filtering, and monitoring content. While these measures may not be as extreme as complete internet shutdowns, they still hinder the full enjoyment of the right to freedom of expression and have the potential to severely distort and disrupt people's access to information online.

Censorship and blocking	**Filtering**
Typically refers to the prevention of access to specific websites, domains, IP addresses, protocols, or services included on a blacklist.[50] Justifications for blocking often include the need to prevent access to illegal content or to content that is a threat to public order or is objectionable to a particular audience.[51]	Generally, refers to restricting or limiting access to information (or related services) that is either illegal in a particular jurisdiction, is considered a threat to public order, or is objectionable to a particular audience. Filtering can relate to the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols, or keywords, or based on their perceived connection to content deemed inappropriate or unlawful.
Note: The distinction between these concepts may appear to be semantic, but there is arguably a difference in scale and perspective. However, the key commonality is that they both limit access to content on the internet.[52]	

At a more granular level, ARTICLE 19 outlines several ways in which access to content can be restricted:[53]

- URL blocking, which blocks a specific web page;
- IP address blocking, which prevents connection to a host;
- Blocking of entire domain names through DNS tampering;
- Blacklisting, which compiles a list of URLs to be filtered, while whitelisted URLs are not subject to blocking or filtering; and

[50] ARTICLE 19, 'Freedom of Expression Unfiltered: How blocking and filtering affect free speech' (2016) at 7 (accessible here).
[51] Internet Society, 'Internet Society Perspectives on Internet Content Blocking: An Overview' (2017) (accessible here).
[52] Id. See further Barnes, 'Technical Considerations for Internet Service Blocking and Filtering' (2013) (accessible here).
[53] ARTICLE 19 above n 7 at 9.

- Keyword blocking, which is generally used to enable the blocking of specific categories of content.

The rise of disinformation has also contributed to an increase in blocking and filtering with states trying to mitigate the spread of false information, and, in some instances, legally permitting blocking and filtering to prohibit and punish the dissemination of false or inaccurate statements.

Applicable international human rights standards

The same general considerations relating to access, online rights and freedom of expression discussed above are applicable here, save for specific considerations relating to filtering and blocking. In 2011, in a Joint Statement on Freedom of Expression and the Internet, a collective of Special Rapporteurs and experts stated the following in relation to filtering and blocking:[54]

- Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure — analogous to banning a newspaper or broadcaster — and can only be justified in accordance with international standards, for example, where necessary to protect children against sexual abuse.
- Content filtering systems which are imposed by a government or commercial service provider, and which are not end-user controlled are a form of prior restraint and are not justifiable as a restriction on freedom of expression.
- Products designed to facilitate end-user filtering should be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering.

In a 2016 Report, the UNSR on FreeEx explained that:[55]

> "States often block and filter content with the assistance of the private sector. Internet service providers may block access to specific keywords, web pages or entire websites. On platforms that host content, the type of filtering technique depends on the nature of the platform and the content in question. Domain name registrars may refuse to register those that match a government blacklist; social media companies may remove postings or suspend accounts; search engines may take down search results that link to illegal content. The method of restriction required by Governments or employed by companies can raise both necessity and proportionality concerns, depending on the validity of the rationale cited for the removal and the risk of removal of legal or protected expression.
>
> Ambiguities in State regulation coupled with onerous intermediary liability obligations could result in excessive filtering. Even if content regulations were validly enacted and enforced, users may still experience unnecessary access restrictions. For example, content filtering in one jurisdiction may affect the digital expression of users in other jurisdictions. While companies may configure filters to apply only to a particular jurisdiction or region, there have been instances where they were nevertheless passed on to other networks or areas of the platform."

[54] OAS, 'Joint Declaration on Freedom of Expression' (2011) (accessible here).
[55] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2016) (accessible here).

In a case in the European Court of Human Rights (ECtHR) in which access to a lawful website was obstructed as a result of blocking measures applied to an illegal website, the Court stated that:

> "When exceptional circumstances justify the blocking of illegal content, a State agency making the blocking order must ensure that the measure strictly targets the illegal content and has no arbitrary or excessive effects, irrespective of the manner of its implementation. Any indiscriminate blocking measure which interferes with lawful content or websites as a collateral effect of a measure aimed at illegal content or websites amounts to arbitrary interference with the rights of owners of such websites."[56]

Despite these clear prohibitions on blocking and filtering, African states have increasingly used these mechanisms to prevent access to information during elections and to quell protests and cover up human rights violations.

Blocking and filtering during elections

Blocking and filtering of content has increasingly been used to prevent access to information over election periods. In 2023, NetBlocks reported that Gabon had blocked access to social media platforms on the day of presidential and legislative elections. These blocks were lifted four days later after military officers announced that they had taken power in the country.[57] Similarly, Zambia,[58] Uganda,[59] and Cameroon have also experienced social media restrictions just before or after election processes.[60] In 2023, access to social media networks was blocked just before the polls closed in the Mozambican local elections. This made it impossible to access information about the closing of the polls and the vote count.[61]

Filtering and blocking to dampen protests and cover up human rights violations

Ethiopia: In 2023, the government cut off access to social media and communications platforms in the Amhara region without explanation for over 100 days.[62] Ethiopia has repeatedly made use of blocking and filtering mechanisms in the recent past: between 2012 and 2018 hundreds of websites were blocked, including the websites of LGBTQI+

[56] European Court of Human Rights, *Vladimir Kharitonov v. Russia* (application No. 10795/14), (2020), para. 46 (accessible here).
[57] Netblocks, 'Internet cut in Gabon on election day'(2023) (accessible here).
[58] Netblocks, 'Social media and messaging apps restricted in Zambia on election day' (2021) (accessible here).
[59] Netblocks, 'Social media and messaging restricted, internet shut down for Uganda elections' (2021) (accessible here).
[60] Netblocks, 'Facebook and WhatsApp restricted in Cameroon on eve of election results' (2018) (accessible here).
[61] Club of Mozambique, 'CIP Mozambique Elections: Internet cut, counting starts' (2023) (accessible here).
[62] Access Now, '#KeepItOn in conflict: the human impact of internet shutdown in Amhara region, Ethiopia' (2023) (accessible here).

organisations, media outlets and CSOs like the Electronic Frontier Foundation.[63] In 2017, during a spate of anti-government protests, Facebook, Twitter, WhatsApp, and Dropbox were frequently blocked. While the 2018 change in regime resulted in over 250 websites becoming unblocked, politically motivated blocking and filtering have nevertheless continued in the country.[64] In 2023, authorities continued to block access to social media platforms in response to tension and protests in several areas of the country.[65]

Zimbabwe: In 2022, the opposition Citizens' Coalition for Change reported that the ruling party was blocking access to social media during a political rally ahead of the general elections.[66]

Eswatini: In 2021, the government suspended access to Facebook, WhatsApp, and Twitter claiming the platforms were being used to "spread misinformation," contributing to violence around the country.[67] However, this and other internet disruptions at the time were reported to have been actually ordered to thwart pro-democracy protests and reports about police brutality.[68]

In addition to blocking and filtering by states, the UNSR on FreeEx noted in 2022 that the digital platforms, through which most of the content on the internet is accessed, are under increased pressure from governments "to take down, delist, de-index, block and filter content, including journalistic content, leading to a form of opaque, privatized censorship."[69]

Blocking and filtering remain a contemporary concern. While in limited instances there may be justifiable limitations, generally such measures constitute an unjustifiable infringement and are often carried out with limited guidance to the public and limited or no regulation or oversight.[70]

Unjustifiable limitations

As discussed above, and as with all limitations of the right to freedom of expression, restrictions are only permissible if they are provided by **law**, pursuant to a legitimate aim and conform to the strict tests of **necessity** and **proportionality**. In terms of "blanket" or "generic" bans, the 2011 UNHRC General Comment stated that "generic bans on the operation of certain sites and systems are not compatible" with Article 19 of the ICCPR. Where restrictions constitute "generic" bans, they will generally amount to an infringement of the right to freedom of expression.[71]

[63] Access Now, 'Ethiopia: Verifying the unblocking of websites,' (2018) (accessible here).
[64] Freedom House, 'Freedom on the net 2021: Ethiopia' (2021) (accessible here).
[65] Freedom House, 'Freedom on the net 2023: Ethiopia' (2023) (accessible here).
[66] Zimbabwe Independent, 'Cyberspace the new Zim political battlefield,' (2022) (accessible here).
[67] MISA, 'Eswatini shuts down internet as protests rock monarchy' (2021) (accessible here).
[68] Access Now, 'Eswatini authorities shut down internet to quell protests, ask people to email grievances' (2021) (accessible here).
[69] UNHRC, 'Report of the UNSR on FreeEx on Reinforcing media freedom and the safety of journalists in the digital age,' (2022) (accessible here).
[70] UNICEF 'Children's Rights and Business in a Digital World: Freedom of Expression, Association, Access to Information and Participation (2017) at 11 (accessible here).
[71] UNHRC, 'General Comment 34 above n 27

Justifiable limitations: children's rights

There may be circumstances in which measures such as blocking and filtering of content are justifiable. The protection of children's rights may be one such example. Blocking and filtering techniques can be developed and utilised to prevent the proliferation of and exposure to damaging material and to protect children from harmful and illegal content.

Despite this important purpose, UNICEF has noted that there are inherent concerns around blocking and filtering, including a lack of transparency; the unscrupulous nature of filters; the lack of evidence to show where and when they have been deployed; and the threat of legitimate content being limited.[72]

In addition, UN General Comment 25 on children's rights in relation to the digital environment makes it clear that filtering and blocking must be treated cautiously so as not to infringe on children's rights to access to information, freedom of expression, freedom of thought, conscience and religion, and right to privacy.[73] This illustrates that even when there might appear to be a legitimate purpose, rights can be unduly limited if the elements of legality, necessity and proportionality are not thoroughly and independently tested.

In digital rights litigation, practitioners will do well to test all tenets of the limitations analysis before determining the appropriateness or otherwise of an imposed restriction. The ECtHR, in its 2012 decision of *Ahmet Yıldırım v. Turkey*,[74] provides guidance on the limitations analysis in relation to blocking and filtering.

Case note: *Ahmet Yıldırım v. Turkey*

The applicant owned and ran a website on which he published his academic work and views on various topics. In 2009, the Denzili Criminal Court in Turkey ordered the blocking of the website as a preventative measure in the context of criminal proceedings against the site's owner, who was accused of insulting the memory of Atatürk. The Court subsequently ordered the blocking of all access to *Google Sites*, a website hosting platform, as this was the only means of blocking the offending website. The Applicant unsuccessfully tried to have the blocking order removed and applied to the ECtHR submitting that the blocking of *Google Sites* amounted to indirect censorship.

The ECtHR held that the impugned measure amounted to a restriction stemming from a preventive order blocking access to a website. The ECtHR found that the impugned measure produced arbitrary effects and could not be said to have been aimed solely at blocking access to the offending website, since it consisted in the wholesale blocking of all websites hosted by *Google Sites*.

[72] UNICEF 'Children's Rights and Business in a Digital World: Freedom of Expression, Association, Access to Information and Participation (2017) at 12 (accessible here).
[73] UN Committee on the Rights of the Child, 'General comment No.25 (2021) on Children's Rights in Relation to the Digital Environment' (2021) (accessible here).
[74] *Ahmet Yildirim v. Turkey* (2013) (accessible here).

The ECtHR reasoned that specific legal provisions are necessary, as general provisions and clauses governing civil and criminal responsibility do not constitute a valid basis for ordering internet blocking. Relying on General Comment 34, the Joint Declaration on Freedom of Expression and the Internet and the 2011 UNSR FreeEx Report, the ECtHR went further, stating:

> "In any case, blocking access to the Internet, or parts of the Internet, for whole populations or segments of the public, can never be justified, including in the interests of justice, public order, or national security. Thus, any indiscriminate blocking measure which interferes with lawful content, sites, or platforms as a collateral effect of a measure aimed at illegal content or an illegal site or platform fails *per se* the "adequacy" test, in so far as it lacks a "rational connection," that is, a plausible instrumental relationship between the interference and the social need pursued. By the same token, blocking orders imposed on sites and platforms which remain valid indefinitely or for long periods are tantamount to inadmissible forms of prior restraint, in other words, to pure censorship."

Furthermore, the ECtHR held that the judicial review procedures concerning the blocking of websites in Turkey are insufficient to meet the criteria for avoiding abuse, as Turkish domestic law does not provide for any safeguards to ensure that a blocking order in respect of a specific website is not used as a means of blocking access in general. Accordingly, the ECtHR found there had been a violation of the right to freedom of expression.

In another case in the Turkish Constitutional Court in 2021, it was found that blocking access to news articles on account of a violation of reputation and personal rights unjustifiably infringed the right to freedom of expression and, again, that the domestic law which permitted the blocking provided no opportunity to realistically challenge the decision and no procedural safeguards against excessive and arbitrary internet-blocking measures.[75]

Similar considerations relating to ligation in respect of internet shutdowns are applicable in the context of blocking and filtering. However, there are further practical considerations that might be of use to potential litigators and activists.

Tips for measuring internet restrictions

The Open Observatory of Network Interference is a useful, free resource that detects censorship and traffic manipulation on the internet. Their software can help measure:

- Blocking of websites;
- Blocking of instant messaging apps (WhatsApp, Facebook Messenger, Signal, and Telegram);
- Blocking of censorship circumvention tools (such as Tor);
- Blocking of Virtual Private Networks (VPNs);

[75] Global Freedom of Expression, 'The Case of Keskin Kalem Yayıncılık v. Ticaret A.Ş.,' (2021) (accessible here).

- Presence of systems (middleboxes) in your network that might be responsible for censorship and/or surveillance; and
- Speed and performance of your network.

This tool can be a helpful way to collect data that can be used as evidence of restrictions to access.

The Association for Progressive Communications (APC) has also developed a facilitated training activity in the form of a game for people to better understand internet shutdowns blocking and filtering, as well as ways to circumvent such measures. This game can be used by all, whether in person or online, to better understand and navigate restrictions.

Activists and litigators should remain vigilant for the occurrence of blocking and filtering given its sometimes covert and nuanced nature, and, where necessary, apply the principles of legality, proportionality, and necessity to establish when the restriction of content amounts to a rights violation. As international pressure against full-scale internet shutdowns mounts, litigators should be cognisant that blocking and filtering may increase as a popular measure to restrict the free flow of information.

SOCIAL MEDIA TAXES, LICENSES, AND REGISTRATION

Overview of social media taxes

Social media taxes, as the name indicates, refer to the trend of placing additional taxes on users on the use of social media. For some time, this was a popular approach among African governments seeking to cash in on the growing usage of international social media platforms. In recent years, such taxes have become less common, with some converting into other forms of online usage taxes and others being removed entirely.

Uganda's experience with social media taxes has been most controversial, with the introduction of the Excise Duty (Amendment) Act 2018.[76] This Act envisaged 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." Taxing over-the-top services (OTTs) was supposedly intended to create a level playing field among telecommunications service providers and to favour local content over international content. However, in practice, service providers transferred the cost of the tax to users, resulting in increased costs to access the internet.

Impacts of social media taxes

The Uganda example clearly illustrated that taxes "disproportionately and negatively impact the ability of users in Uganda to gain affordable access to the internet, and thus unduly restrict their right to freedom of expression."[77] The Ugandan Tax Authority reported that

[76] Uganda, 'Excise Duty (Amendment) Act, 2018' (2018) (accessible here).
[77] ARTICLE 19 'Eastern Africa new tax and licensing rules for social media threaten freedom of expression' (2018) (accessible here).

within a year of the tax being introduced, it had only received 17% of the anticipated revenue. Reportedly, many social media users relied on virtual private networks (VPNs) to avoid the financial implications of the tax, and research has found that the tax "actually lowered domestic tax revenue and reduced Internet use."[78]

Further, "since mobile money is disproportionately used by lower-income households and individuals (informal sector, women, youth, etc), mobile money taxes have implications on the attainment of financial inclusion and wider socio-economic development goals."[79]

Uganda subsequently abandoned the OTT tax but later introduced a new 12% excise tax on internet bundles that are reportedly disproportionately affecting women, exacerbating the gender digital divide.[80] Tanzania and Zambia have also initiated such schemes, along with attempts in a host of other countries in East and Southern Africa.[81] Some taxes have taken a slightly different form, such as Ghana which implemented a 1.5% levy on electronic money transfers.[82] This trend sparked concern among digital rights activists and individual users alike.

Kenya also attempted to implement a Digital Service Tax in 2020 with the passing of the Finance Act, 2020. However, after a legal challenge, the High Court nullified the Act on the grounds that the Senate had not participated in its passing.[83]

Human rights implications of social media taxes

Such taxes have clear rights-based implications. The additional financial burden curbs people's access and enjoyment of online content and may also diminish their ability to access information and exchange ideas. When the Uganda tax was introduced, Human Rights Watch expressed concern that the proposed tax is "just another way for authorities to stifle free speech," explaining that "[t]axing anyone to use social media is an affront to their basic human rights."[84] Research ICT Africa has pointed out that "in some countries these taxes are… a tactic for repressive governments to control freedom of speech where dissent coincides with the largest band of Internet users, who are often between 18 to 35 years of age."[85]

The international human rights framework on access to the internet and the promotion of the right to freedom of expression has been discussed, in detail, above. The same principles apply here, save for the addition of a brief review of the African human rights system.

[78] Research ICT Africa, 'COVID-19 exposes the contradictions of social media taxes in Africa,' (2021) (accessible here).
[79] Id.
[80] Global Dev, 'Taxation, gender, and internet access: lessons from Uganda,' (2023) (accessible here).
[81] Id.
[82] The Economist, 'African governments hope digital taxes will fill a budget hole,' (2022) (accessible here).
[83] Internews, 'The Impact of Digital Media Regulation – an East African Case Study,' (2021) (accessible here).
[84] Human Rights Watch 'Uganda's Troubling Social Media Tax: New Law Restricts Right to Free Speech and Information on Social Media' (2018) (accessible here).
[85] Research ICT Africa above n 78.

In 2019, the ACHPR adopted the Declaration of Principles on Freedom of Expression and Access to Information in Africa.[86] The Declaration affirms that "the same rights that people have offline should be protected online and in accordance with international human rights law and standards" and that these rights apply "through any medium." It recognises the importance of the internet in advancing human and people's rights in Africa, particularly the right to freedom of information and expression.

The Declaration explicitly addresses the issue of social media taxes under Principle 38(3) on Non-interference, which states that:[87]

> "States shall only adopt economic measures, including taxes, levies and duties, on internet and information and communication technology service end-users that do not undermine universal, equitable, affordable and meaningful access to the internet and that are justifiable and compatible with international human rights law and standards."

A positive shift in tax burdens

In contrast to the burden of social media taxes placed on internet users on the continent, there is growing support for the notion that international digital platforms, particularly social media companies, should be taxed in the countries in which they operate and generate revenues, including those in Africa. In 2023, the Organisation for Economic Co-operation and Development (OECD) secured agreement from 138 countries on a landmark initiative that would enable major reform to the international tax system to more fairly tax digital platforms in the jurisdictions in which they earn revenue.[88] This is seen as a fairer, more equitable, and rational way of boosting tax revenues in countries seeking to benefit from the rise of digital technologies without hindering the expansion of access to the internet to those with limited ability to pay.

Licenses and registrations

Another tactic frequently used by states on the continent is the implementation of laws and regulations that require bloggers, social media users, and independent journalists to register or obtain licenses in order to publish online. In addition to implicating their individual rights to freedom of expression, it must be emphasised that these types of internet users fulfil an important role in our contemporary society by disseminating information and enabling discussion, and many international standards and guidelines on freedom of expression online provide legal standards that protect bloggers and journalists alike.[89] Requiring these users to

[86] African Declaration above n 2.
[87] Id.
[88] OECD, '138 countries and jurisdictions agree historic milestone to implement global tax deal,' (2023) (accessible here).
[89] The UN's General Comment No 34 includes bloggers in its assessment of journalism, stating that any restriction on the operation of websites, blogs or any other internet-based systems are not compatible with the right to freedom of expression. See General Comment 34 above n 27.

obtain licenses or become registered to share content may inhibit their ability to disseminate information and constitute unjustified restrictions on these rights.

In 2018, the ACHPR expressed concern regarding the growing trend of states in East Africa in particular adopting stringent regulations on the internet and internet platforms that included various forms of taxes and licenses.[90] The ACHPR noted particular concern over the following developments:

- The Electronic and Postal Communications (Online Content) Regulations 2018 in Tanzania, introduced licensing requirements for bloggers that required them to pay up to 2,100,000 Tanzanian Shillings (around USD900) for licences.
- The Excise Duty (Amendment) Bill 2018 in Uganda, which requires users of OTTs, such as social media platforms, to pay UGX200 (USD0.05), per user, per day of access.
- The directive issued by the Kenya Film and Classification Board on 14 May 2018 requires licences for anyone posting videos for public exhibition or distribution online on their social media accounts.
- The 5% levy on telecommunications was proposed by the Nigerian government in 2022, which was halted after Communications and Digital Economy Minister Isa Pantami argued that the sector was already over-taxed in the face of rising costs.[91]

The ACHPR further stated:

> "These regulations may negatively impact the ability of users to gain affordable access to the Internet, which goes against States' commitment to protect the right of every individual to receive information, as well as the right to express and disseminate one's opinion within the law which is provided under Article 9 of the African Charter on Human and Peoples' Rights."

There are several examples of countries in SSA that have or have attempted to, implement such license or registration regulations.

Kenya

The Kenyan Film and Classification Board requires citizens to obtain a license to be able to post videos intended for public exhibition or sale.[92] The Board has explained that it seeks to protect national security from illegal filming activities, as well as provide an additional stream of revenue. License costs amount to KShs 12,000 (USD 74) and KSh 5,000 (USD 31) for every video produced under 40 minutes and Sh1,000 (USD 6) for every video uploaded, with stiff penalties for non-compliance.[93]

The additional cost raises concerns about the ability of video producers to operate, including concerns that this could have far-reaching consequences for freedom of expression online. It

[90] APC, 'Concern on the growing trend of stringent regulation of the internet in East African states' (2018) (accessible here).
[91] Premium Times, 'Why I oppose new 5% tax on phone calls, data- Pantami' (2022) (accessible here).
[92] ARTICLE 19, 'Kenya: Censorship by film classification board limiting free expression' (2018) (accessible here).
[93] Rödl & Partner, 'Kenya's Film Board: Licensing of Online Content,' (2018) (accessible here).

remains unclear whether the regulations apply to all video producers posting on social media,[94] but the KFCB has confirmed that it applies to videos recorded using mobile phones and published on social media.[95] UNESCO, in a 2022 assessment of media development in Kenya, likewise recommended that the government withdraw the regulation due to its potential impacts on the public's access to information.[96]

Potential developments to monitor in Kenya

In 2019, a private members' Bill, the Information and Communication (Amendment) Bill, sought to introduce regulations relating to the licensing of social media platforms and the sharing of information by licensed persons.[97] The Bill would create obligations on social media users, require the registration of bloggers, and allow the Communications Authority to develop a bloggers' code of conduct. Although the Bill appears to have languished since its introduction in 2019, such legislative efforts raise serious concerns for freedom of expression on the internet. As of 2024, the Bill has not yet passed and has since gone through several iterations.

Tanzania

Tanzania has also introduced licensing requirements which attach additional fees to social media. The Electronic and Postal Communications (Online Content) Regulations, 2020 introduced new online content regulations.[98] Bloggers, in particular, are required to pay unreasonably high fees in order to obtain a license. Among other concerns with the regulations, the licensing requirement has been heavily criticised for being incompatible with the right to freedom of expression. APC argued that:

> "Tanzania's new excise duty in the form of online content licence fees fundamentally threatens universal access to and affordability of the internet. Consequently, it clearly constitutes a limitation on the right to freedom of expression. Further, it is unjustifiable when measured against the arguments that could be made by the Tanzanian government in support of the increase, such as the need to ensure appropriate excise duty levels in order to ensure the fiscal sustainability of the state in meeting the developmental and other socioeconomic rights of its inhabitants."[99]

Tanzania: Attempts to oppose the Regulations

- In 2018, ARTICLE 19 argued that the Tanzania Regulations were defective and wholly at odds with international standards on freedom of expression,

[94] ARTICLE 19 above n. 92.
[95] Innovation Village, 'Kenyans to Register with Kenya Film and Classification Board Before Posting Videos for Public Consumption,' (2018) (accessible here).
[96] UNESCO, 'Assessment of Media Development in Kenya,' (2022) (accessible here) at p. 41.
[97] Republic of Kenya, 'The Kenya Information and Communication (Amendment) Bill, 2019' (2019) (accessible here).
[98] United Republic of Tanzania, 'The Electronic and Postal Communications (Online Content) Regulations, 2020' (2020) (accessible here).
[99] APC, 'Human rights impacts of taxing popular internet services' (accessible here) at 12.

recommending that they be withdrawn entirely.[100] After subsequent amendments were made to the Regulations in 2020, ARTICLE 19 again found that several issues with the 2018 Regulations had not been addressed while others had been made worse, including a failure to limit the sweeping powers of the Authority and a failure to provide appropriate due process safeguards in the licensing process.[101]

- In April 2018, civil society activists obtained a temporary court injunction against the regulations from Tanzania's High Court pending another hearing to decide the case.[102]
- In May 2018, however, the injunction was overturned.[103] As a result, owners of social media platforms are required to register and comply with the regulations.

Lesotho

In 2020, Lesotho proposed the Lesotho Communications Authority (Internet Broadcasting) Rules which sought to require all social media users with over 100 followers to register as "internet broadcasters" and comply with the rules governing broadcast media houses.[104] In addition, the government was criticised for failing to publish the outcomes of the public consultation process for the development of the Rules.[105] As of 2024, it appears that the Rules have not yet been approved.[106]

Zambia

In 2021, Zambia's Independent Broadcasting Authority likewise issued rules requiring online television stations to obtain a broadcasting license and criminalising online broadcasting without such a license.[107] It is also notable that Zambia introduced a daily levy on internet voice calls in 2018 which was subsequently withdrawn after backlash from consumers and digital rights groups, in addition to another abandoned attempt in 2010 to introduce a 17,5% excise tax on airtime and the provision of bandwidth to end users.[108]

This trend of introducing social media taxes and licensing and registration regulations in Africa warrants concern, notably the implication that states' obligations to respect, protect and promote the right to freedom of expression can be traded off in pursuit of economic gain. The

[100] ARTICLE 19, 'Tanzania: Electronic and Postal Communications (Online Content) Regulations 2018,' (2018) (accessible here).
[101] ARTICLE 19, 'Tanzania: Online Content Regulations 2020 extremely problematic in context of COVID-19 pandemic' (2021) (accessible here).
[102] Reuters, 'Tanzania bloggers win temporary court order against state crackdown' (2018) (accessible here).
[103] Reuters, 'Tanzania government wins court case to impose online regulations' (2018) (accessible here).
[104] CIPESA, 'Towards an Accessible and Affordable Internet in Africa Key Challenges Ahead' (2021) (accessible here).
[105] Internet Freedom Project, Lesotho, 'Digital Rights in Lesotho,' (2022) (accessible here) at p. 12.
[106] Lesotho Communications Authority, (accessible here).
[107] CIPESA above n. 104 at p 4.
[108] Id.

ACHPR, civil society actors, and affected individuals should continue to speak out against these trends. Litigation, policy reform and advocacy strategies need to be urgently adopted to re-route the current trajectory away from increased reliance by states on social media taxes, as well as from burdensome obligations on bloggers and journalists.

DISTRIBUTED DENIAL-OF-SERVICE ATTACKS

Overview of DDoS attacks

The UNSR on FreeEx defines a DDoS attack as a cyber-attack that seeks to undermine or compromise the functioning of a computer-based system.[109] The UNSR notes further that a DDoS attack can have the same effect as an internet shutdown. This increasingly common online phenomenon uses a large number of computers to target websites and online services and overwhelms them with more traffic than they can handle, rendering them temporarily inoperable.[110]

DDoS Attacks and critical moments

The 2019 UNSR Research Paper on Freedom of Expression and Elections in the Digital Age found that:

> "During elections, State actors have historically denied access to unfavourable views and information concerning incumbent officeholders … One common practice involves the use of Distributed Denial of Service ("DDoS") attacks, [which] have targeted the websites of political parties, journalists and media outlets, and human rights defenders and civil society organizations. Perpetrators have also targeted the websites of States' election commissions, which publicize critical information such as changes to ballot locations. DDoS attacks are also potentially a cover for coordinated hacks on voter registration and other electoral databases and other attempts to steal the data of voters, candidates and public officials. Given that online media have become the primary resource of news and information for many voters, and the integration of electronic systems into electoral processes, DDoS attacks are likely to increase in magnitude and frequency. Furthermore, in the Internet of Things era, the growing number of connected devices makes them attractive targets for DDoS attacks."[111]

Given their similarity to internet shutdowns, DDoS attacks, whether committed by a state or non-state actor, infringe the right to freedom of expression. They are usually well hidden, covert, and illicit in nature, and, accordingly, fall foul of the "provided by law" requirement of Article 19(3) of the ICCPR. They completely disable access to online content, usually during a critical time — such as an election. As a result, the UNSR Research Paper further emphasised that DDoS attacks "whether committed by State actors or their agents, are incompatible with Article 19 of the ICCPR" and are "almost always unnecessary and disproportionate measures under Article 19(3)."

[109] UNHRC, 'Report of UNSR of FreeEx' above n 11.
[110] See further Media Defence above n 3 at 23.
[111] UNHRC, 'UNSR on FreeEx Report on Freedom of Expression and Elections in the Digital Age' (2019) (accessible here).

These challenges extend to other regions as well. The Inter-American Commission on Human Rights reported in 2013 that DDoS attacks can be extremely disruptive to the exercise of the right to freedom of expression, and, as a result, states are obligated to investigate and properly redress such attacks.[112] The principles mentioned above and sentiments relating to access and freedom of expression are implicated by DDoS attacks. The UN Guiding Principles on Business and Human Rights can also be relied on when trying to prevent and mitigate DDoS attacks by non-state actors, including the safeguarding of systems infrastructure.

Examples of DDoS attacks

In 2023, the World Economic Forum reported that Google and Amazon had fought off the largest DDoS attack in history, 7.5 times larger than the previous biggest attack.[113] The prevalence of such attacks had also increased by a third in the first half of 2023 in comparison to the same time the previous year.[114] DDoS attacks are affecting states across the world, regardless of their social policies or economic status:

- In 2023, Kenya's e-Citizen platform was attacked, leaving citizens of the country unable to access essential services such as buying electricity tokens and making payments via a mobile transactions system.[115]
- Spain had numerous private and public websites impacted by a wave of DDoS attacks in 2023 amid an ongoing European Union (EU) summit. The attacks affected Granada, the city in which the summit was being held, transportation services and tourism portals.[116]
- In 2019, the South African financial sector fell victim to a string of DDoS attacks.[117] DDoS attacks rose by 30% in 2023 from 2022 in the country. Further, the size of the average DDoS attack in the country rose by 50%.[118]
- In 2018, it was reported that a website of a Mexican political opposition party was rendered inoperable by a DDoS attack. The attack occurred during a debate between presidential candidates in the lead-up to the elections.[119]

Be it politically, socially, or economically motivated, DDoS attacks are a serious threat to freedom of expression as well as the public's ability to access information. Nefarious state and non-state actors are becoming increasingly skilled and sophisticated, posing new challenges for states to overcome in order to ensure they fulfil their positive obligations to protect and promote freedom of expression. Mitigating DDoS attacks in future will require multidisciplinary

[112] IACHR, 'Freedom of expression and the internet,' (2013) (accessible here).
[113] World Economic Forum, 'Biggest-ever DDoS attack threatens companies worldwide, and other cybersecurity news to know this month,' (2023) (accessible here).
[114] Marcus Law, 'Global events driving rise in DDoS attacks, says Netscout' Cyber Magazine (2023) (accessible here).
[115] Matthew Gooding, 'Anonymous Sudan DDoS cyberattacks cripple Kenya's new e-Citizen digital infrastructure' Tech Monitor (2023) (accessible here).
[116] SC Media, 'DDoS attacks hit Spain amid EU summit' (2023) (accessible here).
[117] Times Live, 'Almost certain that organised criminal group behind wave of cyberattacks in SA' (2019) (accessible here).
[118] SEACOM, 'What tools do South African enterprises need to combat DDoS attacks?' (2023) (accessible here).
[119] Reuters, 'Cyber attack on Mexico campaign site triggers election nerves' (2018) (accessible here).

teams of litigators and technologists working jointly to protect and promote freedom of expression.

ACCOUNTABILITY OF PRIVATE PLATFORMS FOR CONTENT MODERATION

Overview of Content Moderation

As internet and social media companies have become increasingly influential in the digital age, questions have arisen about the accountability mechanisms in place for these actors who hold extraordinary power over the ability of the general public to exercise their rights to freedom of expression and access to information. The content moderation policies of these tech giants effectively block and filter the content not only that individuals can post, but also that other users can access. As a result, attention is now mounting over how these companies make their decisions about removing or deprioritising content, and the transparency and accountability mechanisms in place to ensure that they comply with human rights law and standards.

Critics argue that users in African countries, in particular, lack the influence over and access to these big multinational companies to be able to understand how content moderation may be affecting their freedom of expression and to act where content is removed (or where illegal content remains up).

Various cases have recently reached the courts in this regard:

- In Germany, the Federal Court of Justice ruled in 2021 that Facebook's terms of service on deleting user posts and blocking accounts for violations of its Community Standards were invalid because they did not make provision for informing users about decisions to remove their content and to grant them an opportunity to respond, followed by a new decision.[120]
- In France, the Paris Court of Appeal ordered Twitter to provide information on the measures the company was taking to fight online hate speech in a case brought by organisations who had found, in their research, that Twitter only removed under 12% of tweets that were reported to them.[121]
- In another case involving Facebook, the Republic of The Gambia initiated proceedings in the United States requesting Facebook to release public and private communications and documents about content that Facebook had deleted following the genocide in Myanmar.[122] The Gambia had previously initiated proceedings in the International Court of Justice against Myanmar claiming a breach of its obligations under international law for its alleged crime of genocide against the Rohingyas. The Gambia thus sought information from Facebook on content that it had removed which may have contributed to or exacerbated the violence against the Rohingyas, given Facebook's dominant position as an almost sole news provider in that country at the time. The US District Court held that Facebook must disclose the requested materials.

[120] Global Freedom of Expression, 'The Case on Facebook's Terms of Service' (2021) (accessible here).
[121] *UEJF v. Twitter* (2022) (accessible here).
[122] *The Gambia v. Facebook* (2021) (accessible here).

In an effort to address public concerns over its content moderation practices, Meta has instituted the Oversight Board, a semi-independent body of experts that reviews content moderation decisions to ensure the protection of the right to freedom of expression. While it has made some influential decisions, it has been criticised for only reviewing a very small proportion of total decisions made, being too slow in making recommendations, and having little real influence over Meta's policies.[123]

In a recent example affecting Africa, the Oversight Board upheld Meta's decision to remove a post alleging the involvement of ethnic Tigrayan civilians in atrocities in Ethiopia's Amhara region in 2021. The Board held that the post violated Facebook's prohibition on unverified rumours under its Violence and Incitement Community Standard, and therefore must be removed.[124]

Meta and Kenyan content moderators' labour dispute

Employees of Sama, a Meta subcontractor responsible for removing violent and hateful publications from Facebook, filed a complaint against their employer and Meta as their principal in 2023 claiming they had been unfairly dismissed by Sama.[125] This followed ongoing complaints by the content moderators that they were insufficiently compensated and protected from the risks to which they were exposed and the damages caused to their mental health as a consequence of the moderation of content for Facebook.[126]

In August 2023 the parties agreed to negotiate to reach an amicable solution. However, in October 2023 negotiations broke down amidst accusations that Meta and Sama "were making very little attempt to address the core issues" and "were not being genuine."[127] As of 2024, it is expected that this matter will proceed to litigation.

Non-Consensual Dissemination of Intimate Images

In recent years, the issue of the Non-Consensual Sharing of Intimate Images (NCII) has become increasingly prominent as a result of the unfortunate proliferation of this form of online gender-based violence. In many cases, content is shared in order to blackmail, threaten, or harass internet users, predominantly women and gender minorities. It is vital that the rights of the victims/survivors to privacy and reputation are protected by enabling such content to be rapidly and permanently removed. While this is one of the narrow circumstances in which the removal of content is not only justified but absolutely critical to protecting human rights, it is still important to maintain appropriate checks and balances over the technology companies that make decisions regarding the removal or blocking of content.

[123] See, for example, here and here.
[124] Global Freedom of Expression, 'Oversight Board Case of Alleged Crimes in Raya Kobo' (2021) (accessible here).
[125] The Guardian, 'Meta's settlement talks with Kenyan content moderators break down' (2023) (accessible here).
[126] Id.
[127] Id.

Case law on NCII

A body of case law is gradually building up that provides guidance on how courts are interpreting this issue around the world:

- In 2023, the High Court of Delhi in India ordered intermediaries to remove all offending content from their platform in cases of NCII and not just the specific links provided by victims. The Court highlighted the damage caused by NCII and how victims being required to search the internet for new uploads for the purpose of requesting their removal can cause further trauma.[128] In an earlier case, the same Court ordered the immediate removal of content not only from the website on which it had been published, without consent but also ordered search engines to de-index the content from their search results, stressing the need for "immediate and efficacious" remedies for victims of such cases.[129]

- The Constitutional Court of Ecuador dealt with a case in 2021 in which pictures of the victim/survivor had been sent to their parents without the victim's consent. The Court also found in favour of the right to privacy and held, in the words of the Columbia Global Freedom of Expression database, that "the storage and sharing of sexual photos without the consent of the victim were a violation of her constitutional rights to personal data protection, reputation, and intimacy" and that "intimate images were personal data sent exclusively to the defendant's partner and required previous consent to be processed by anyone else."[130]
- In 2016, the High Court of Kenya determined a case involving the non-consensual distribution of the petitioner's nude photographs by an ex-boyfriend, resulting in her dethronement as Miss World Kenya 2015.[131] The Court held that the victim/survivor had a legitimate expectation of privacy, that she did not waive her right to protection of privacy by taking nude photographs, and did not consent to their dissemination to third parties, and as such, her right to privacy under Article 31 of the Constitution of Kenya had been violated.

Some countries are also incorporating provisions criminalising NCII in domestic law. For example, South Africa's Cybercrimes Act, passed into law in 2020, criminalises the disclosure of data messages that contain intimate images of a person without the latter's consent.[132] While such provisions are welcomed for the recourse they provide to victims of online gender-based violence, concerns have also been raised about the potential for infringements on the right to freedom of expression if such provisions are vague, broad, or open to abuse. It is, therefore, crucial, that protections for privacy are carefully balanced against potential intrusions into freedom of expression in the online space. Litigation by civil society can play

[128] *Mrs X v. Union of India* (2023) (accessible here).
[129] *X v. Union of India* (2021) (accessible here).
[130] Global Freedom of Expression, 'The Case of Nonconsensual Pornography Sent to Victim's Parents' (2021) (accessible here).
[131] *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* (2016) (accessible here).
[132] South Africa, 'Cybercrimes Act 19 of 2020' (2020) (accessible here).

an important role in appropriately defining this balance and ensuring the advancement of digital rights for all.

The power and opacity of the tech giants raise real questions about the legitimacy of content moderation decisions that are made daily and how they affect the information environment around the world. Litigation is a powerful way to seek greater transparency and accountability from these actors and to achieve a more rights-respecting balance between the various rights implicated by different types of content online.

CONCLUSION

The internet is a key site of struggle for the advancement of human rights in the modern age. Restricting access to the internet, either through internet shutdowns, blocking and filtering, imposing regulatory restrictions, or through DDoS attacks, limits people's fundamental human rights. The promotion, protection, and enjoyment of human rights on the internet is well established as a norm under international human rights law, and restricting access to the internet, by states or non-state actors, violates human rights and can only be justified under very narrow circumstances.

It is comforting to observe that despite the rise of restrictive conduct, the international community, civil society actors and individuals are fighting to advance freedom of expression and digital rights. Fortunately, there are strong legal foundations that allow for progressive and dynamic solutions to these contemporary challenges.