*Module 2*

# *Summary Modules on Litigating Digital Rights and Freedom of Expression Online*

MEDIA DEFENCE

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

**Originally published in November 2022**
**Revised in April 2024**

## TABLE OF CONTENTS

**1. INTRODUCTION ..... 1**

**2. WHAT ARE DIGITAL RIGHTS? ..... 2**

**3. WHAT IS AN INTERNET INTERMEDIARY? ..... 4**

*3.1. Laws on the limitation of intermediary liability* ..... 5

**4. THE BORDERLESS ENJOYMENT OF FREEDOM OF EXPRESSION ..... 6**

**5. THE RIGHT TO FREEDOM OF EXPRESSION ONLINE ..... 8**

**6. CONCLUSION ..... 9**

# MODULE 2

# INTRODUCTION TO DIGITAL RIGHTS

- **Digital rights — which include the right to freedom of expression, privacy and access to information — are the same fundamental human rights as those enjoyed offline but adapted to a new age of technology.**

- **In understanding digital rights, it is also important to understand the role of internet intermediaries, a range of actors who play a critical role in protecting or undermining freedom of speech and associated digital rights online.**

- **Freedom of expression online is uniquely powerful because of its borderless nature, but it has created new legal questions and consequences.**

- **Human rights defenders must engage with the new challenges online and act to protect and promote digital rights in the rapidly evolving online world.**

## 1. INTRODUCTION

Digital rights are human rights in the digital realm. The term 'digital rights' speaks to questions about how the same rights that are fundamental to all humans — such as freedom of expression, privacy, and access to information — are exercised and protected in the era of the internet, social media, and technology.

There is a tension between human rights and freedoms and the rise in restrictions of access to online spaces, which is continuing with increased political polarisation and the growing powers of non-state actors. While many countries have made progress in regulating the digital sphere, including passing data protection laws to protect privacy online, some regulations, such as laws criminalising hate speech and fake news, for example, are abused in order to silence and stifle criticism and freedom of expression online. Protecting and developing online spaces where human rights can be respected and promoted requires effective responses to oppressive regulations and innovative solutions.

Understanding digital rights is crucial to being able to protect fundamental human rights in any domain, as very little of our lives today is immune from the forces of technology and the internet, which have reshaped how humans communicate, participate in public life, and behave. The COVID-19 pandemic has only enhanced our dependence on the digital realm and has exposed some of the emerging challenges in this regard, such as mis- and disinformation and online gender-based violence. Digital rights are the rights that apply in these spaces, including the particular nuances which come with the application of human rights online.

This module seeks to provide an overview of digital rights and the trends affecting freedom of expression online in Africa.

## 2. WHAT ARE DIGITAL RIGHTS?

It is now firmly entrenched by both the African Commission on Human and Peoples' Rights[1] (ACHPR) and the United Nations[2] (UN) that the same rights that people have offline must also be protected online, in particular the right to freedom of expression. As stipulated in article 19(2) of the International Covenant on Civil and Political Rights (ICCPR), the right to freedom of expression applies regardless of frontiers and through any media of one's choice.

However, how established principles of freedom of expression should be applied to online content and communications is in many ways still being determined. For example:

- How to regulate content moderation without infringing on freedom of speech?
- How to balance the use of new technologies for security or surveillance without compromising civil liberties and the ability to dissent?
- How should states regulate the re-tweeting or resharing of hate speech?
- What about regulations for defamatory statements from anonymous or encrypted accounts? How should states ensure cybersecurity, particularly given the rise of artificial intelligence technologies (AI), without being overly oppressive?

These challenges are actively being grappled with by policymakers and courts around the world.

**Examples of digital rights issues**

To give an idea of the range and complexity of the issues included in the umbrella term 'digital rights,' here are some examples:

- **Access to the internet:** Although an express right to the internet has not, as yet, been recognised in any international treaty or similar instrument, there has been much debate about whether the internet should be considered a human right.[3] Nevertheless, there is an increasing recognition that access to the internet is indispensable to the enjoyment of an array of fundamental rights.

- **Interferences to access to the internet.** Despite the above, restrictions on accessing the internet through internet shutdowns, the disruption of online networks and social media sites, and the blocking and filtering of content continue to be used. The ICCPR

[1] ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', (2016) (accessible here) and ACHPR, 'Declaration on Principles of Freedom of Expression and Access to Information in Africa,' (2019) (accessible here).
[2] UNHRC, 'The promotion, protection and enjoyment of human rights on the Internet' (2016) (accessible here) at para 1.
[3] For more see Juan Carlos Lara, 'Internet access and economic, social and cultural rights', Association for Progressive Communications, (2015) (accessible here) at pp 10-11.

has been interpreted as providing an absolute prohibition on measures such as these which constitute prior restraint.[4]

- **Access to information and freedom of expression to combat climate change:** A 2023 report by the UN Special Rapporteur on Freedom of Expression (UNSR on FreeEx) explores the linkages between the right to freedom of expression and to information and sustainable development. The report notes that more is needed to ensure that the voices of the most disadvantaged and vulnerable are heard and calls for renewed political commitment to uphold freedom of expression as an enabler of sustainable development.[5] The Committee on the Rights of the Child issued a General Comment on children's rights and the environment with a special focus on climate change in which it recognised the importance of access to accurate and reliable environmental information and that the digital environment can enhance children's ability to participate and express views on environmental matters.[6]

- **The freedom to choose among information sources:** The 2017 Report of the UNSR on FreeEx notes that in the digital age, the freedom to choose among information sources is meaningful only when internet content and applications of all kinds are transmitted without undue discrimination or interference by non-state actors, including providers.[7] This concept is known as network neutrality, the principle that all internet data should be treated equally without undue interference.[8] In Africa, there has been significant debate about 'zero-rating', a process in which a mobile operator does not count the usage of certain applications or websites towards a user's monthly data allotment, rendering it 'free.'[9]

- **The right to privacy.** Exercising privacy online is increasingly difficult in a world in which we leave a digital footprint with every action we take online. While data protection laws are on the rise across the world, including Africa, they are of widely varying degrees of comprehensiveness and effectiveness, as well as enforcement.[10] Government-driven mass surveillance is also on the rise as a result of the development of technology that enables the interception of communications in a

[4] This has been inferred from the *travaux préparatoires* of the ICCPR that prior restraints are absolutely prohibited under article 19 of the ICCPR. See Marc J Bossuyt, 'Guide to the "Travaux Preparatoires" of the International Covenant on Civil and Political Rights', *Martinus Nijhoff* (1987) (accessible here) at p 398.
In a landmark case setting this precedent, in June 2020, the Economic Community of West African States (ECOWAS) Community Court of Justice ruled that the internet shutdown implemented by the Togolese government in 2017 was illegal (accessible here).
[5] UNHRC, 'UN Special Rapporteur on Freedom of Expression - Sustainable Development and Freedom of Expression (2023) (accessible here).
[6] CRC, 'General comment No. 26 (2023) on children's rights and the environment, with a special focus on climate change' (2023) (accessible here).
[7] UNHRC, 'UN Special Rapporteur on Freedom of Expression, Report on the Role of Digital Access Providers' (2017) (accessible here) at para 23.
[8] For more on net neutrality, Module 5 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online (accessible here) at pp 2-9.
[9] Research ICT Africa, 'Zero-rated internet services: What is to be done?' (2020) (accessible here).
[10] Data Protection Africa, 'Trends' (accessible here).

variety of new ways, such as biometric data collection and facial recognition technology.[11]

- **The use of AI to spread disinformation:** The spreading of false, inaccurate or misleading information is one of the most significant threats to freedom of expression tools have become increasingly sophisticated and widely accessible, spurring an escalation of disinformation tactics.[12] On the other hand, AI can be extremely effective at identifying disinformation,[13] making its regulation complicated.

- **Gendered disinformation:** The UNSR on FreeEx has noted a concerning trend of journalists facing intensified smear campaigns, particularly evident on social media platforms.[14] She highlighted the insidious nature of gendered disinformation, which not only spreads falsehoods but also employs emotionally charged and culturally contextualized content to undermine the credibility and competence of women. These campaigns often resort to sexualization and attacks on the character, integrity, appearance, and intelligence of women journalists, aiming to discredit their reporting and deter them from their professional pursuits. In the African context, such campaigns frequently leverage anti-colonial narratives to undermine women's rights activists and gender rights defenders, falsely associating them with opposition to the decolonial project and aligning them with Western forces.

## 3. WHAT IS AN INTERNET INTERMEDIARY?

Internet intermediaries play an important role in protecting freedom of expression and access to information online. An internet intermediary is an entity which provides services that enable people to use the internet, falling into two categories:

- conduits, which are technical providers of internet access or transmission services; and
- hosts, which are providers of content services, such as online platforms (e.g. websites), caching providers and storage services.[15]

Examples of internet intermediaries are:

- Network operators, such as MTN, Econet and Safaricom.
- Network infrastructure providers, such as Cisco, Huawei, Ericsson and Dark Fibre Africa.

[11] For more, see Module 1 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online (accessible here) T page 11. In January 2020, a High Court in Kenya handed down a judgment finding that a new national biometric identity system could not be rolled out until a comprehensive data protection framework was in place (accessible here).
[12] Freedom House 'The Repressive Power of Artificial Intelligence' (2023) (accessible here).
[13] Fatima C. Carrilo Santos 'Artificial Intelligence in Automated Detection of Disinformation: A Thematic Analysis' *Journalism and Media* (2023) (accessible here).
[14] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on Gendered Disinformation' (2023) (accessible here).
[15] Association for Progressive Communications, 'Frequently asked questions on internet intermediary liability' (2014) (accessible here).

- Internet access providers, such as Comcast, MWeb and AccessKenya.
- Internet service providers, such as Liquid Telecommunications South Africa, iBurst, Orange, and Vox Telecom.
- Social networks, such as Facebook, Twitter and LinkedIn.

One of the most challenging questions relating to internet intermediaries is whether they constitute publishers in the traditional sense of the word. Is an Internet Service Provider (ISP) liable for the content it hosts on behalf of others? Increasingly, courts are finding that an ISP does not "publish" more than the supplier of newsprint, or the manufacturer of broadcasting equipment does. As pointed out by the UNSR on FreeEx in 2011:

> "Holding intermediaries liable for the content disseminated or created by their users severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads to self-protective and over-broad private censorship, often without transparency and the due process of the law."[16]

On the other hand, the increasing power and influence of multinational technology companies have sparked calls for greater transparency and accountability over their internal operations and the decisions they make that have significant effects on the exercise of the rights to freedom of expression and access to information around the world, such as decisions to remove specific content, ban particular users from their platforms, or to allow and promote political advertising.

The **EU** has been at the forefront of regulating internet intermediaries through the Digital Services Act, which sets out obligations for digital services that act as intermediaries in their role of connecting consumers with goods, services and content, including measures for the removal of illegal content and transparency requirements.[17]

### *3.1. Laws on the limitation of intermediary liability*

Some countries in Africa have laws providing for the limitation of intermediary liability, such as **Ghana** and **Uganda**.[18] To protect themselves from liability even in cases where such legislation does not exist, intermediaries often develop terms and conditions that specify their responsibilities and those of their customers.[19] However, it has been noted that intermediaries do not always adhere to their own terms and conditions as has been seen in the removal of violent and sexualised hate speech targeting women.[20]

[16] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (2011) (accessible here).
[17] European Commission, 'Digital Services Act' (2023) (accessible here).
[18] See Ghana's Electronic Transactions Act of 2008 (accessible here) at Article 92 and Uganda's Electronic Transactions Act of 2011 (accessible here) at Section 29.
[19] CIPESA, 'State of Internet Freedom in Africa 2017' (2017) (accessible here) at p 23.
[20] Global Witness 'Violent and sexualised hate speech targeting women approved for publication by social media platforms' (2023) (accessible here).

Other countries in Africa have laws that explicitly make intermediaries liable for their actions regarding content posted using their services.[21] The High Court of **Tanzania** ruled in 2017 in *Jamii Media v The Attorney General of Tanzania*[22] that government requests for the disclosure of user information from an internet intermediary were justified, and that the law governing such disclosures was not unconstitutional, despite a lack of regulations to govern the enforcement of the Act.[23]

In addition, internet intermediaries are increasingly being used by states to police the internet through direct requests to take down content or interfere with internet access, decisions which are often made outside of formal legal and regulatory frameworks and which lack transparency and public scrutiny.[24]

- The **Democratic Republic of Congo**, for example, states in article 50 of the Framework Law No. 013/2002 on Telecommunications that the refusal to grant the request of the authority may lead to the temporary or definitive withdrawal of the operating license or to other penalties.[25]

- After protests against the government in **Zimbabwe** in early 2019, the head of a major telecommunications provider, Econet, was candid in explaining to customers that limitations in network access were a direct response to a directive from the Zimbabwean government.[26] This, clearly, has serious consequences for freedom of expression online.

In 2020, the ECOWAS Community Court issued a pivotal decision for the right of freedom of expression in **Togo and other West African States**, as it held that internet shutdowns that had occurred in Togo violated this right and that the government's national security arguments did not justify internet shutdowns.[27]

## 4. THE BORDERLESS ENJOYMENT OF FREEDOM OF EXPRESSION

The particular opportunity that freedom of expression online presents is that the right can be enjoyed regardless of physical borders. People can speak, share ideas, coordinate and mobilise across the globe on a significant and unprecedented scale.

[21] For example, article 30 of Burundi's Law 100/97 of 2014 on electronic telecommunications provides that operators of electronic communications are fully responsible for fighting fraud on their domains and article 53 of the Law No 1/15 of 2015 regulating the media, provides that media organisations are responsible for any articles published on their portals, even where the person published anonymously.
[22] *Jamii Media v The Attorney General of Tanzania and Another* (2017) (accessible here).
[23] CIPESA, 'Tanzania Court Deals a Blow to Intermediary Liability Rules' (2017) (accessible here).
[24] Association for Progressive Communications, 'Policing the internet: Intermediary liability in Africa' (2020) (accessible here).
[25] See above n 18 at pp 24.
[26] Quartz Africa, 'Zimbabwe's internet blackout shows how powerless major telcos are against governments' (2019) (accessible here).
[27] Access Now 'ECOWAS Togo Court Decision: Internet Access is a Right that Requires Protection of the Law' (2023) (accessible here).

**The internet as a tool for change: the case of #EndSARS**

In October 2020, young **Nigerians** took to the streets to protest against the notorious brutality of the Special Anti-Robbery Squad (SARS), a special unit of the Nigerian police renowned for harassing, kidnapping, extorting, and brutalising particularly young Nigerians. Within days, the protest's hashtag, #EndSARS, had spread like wildfire on social media and messages of solidarity had been reshared by celebrities, politicians, activists, and concerned citizens around the world.[28]

The #EndSARS protests can be compared with the incitement of destructive and violent protests that took place in KwaZulu Natal in **South Africa** in 2021, which was sparked by the imprisonment of former President Jacob Zuma for contempt of court. Online platforms were used to co-ordinate looting and violent attacks, leading to much destruction around the country. In 2023, one of the instigators- who incited violence via WhatsApp- was sentenced to 12 years imprisonment for his role in instigating the unlawful protests.[29]

Before the internet, both protests would have been next to impossible. The borderless nature of the internet can lead to international pressure being put on states for rights violations, the development of and support for global campaigns, the fostering of a rigorous marketplace of ideas, as well as increased incitement of violence.

However, the internet also gives rise to particular challenges that need to be addressed. Through the internet, the ability to publish immediately and reach an expansive audience can create difficulties from a legal perspective, such as establishing the true identity of an online speaker, establishing founding jurisdiction for a multi-national claim, or achieving accountability for wrongdoing that has spread rapidly online, such as the non-consensual dissemination of intimate images.

Moreover, once content has been published online, it can sometimes be difficult to remove. In the 2019 case of *Manuel v Economic Freedom Fighters*,[30] a **South African** High Court ordered the defendants to delete statements that were deemed defamatory from their social media accounts within 24 hours. However, the deletion of a tweet on Twitter does not necessarily remove it from all platforms, as there are other ways in which the content may have been distributed that are not addressed by the deletion (such as retweets in which persons added a comment of their own).[31] This is a particular challenge for finding effective remedies to claims of defamation, hate speech, or the right to be forgotten.

[28] BBC, 'End Sars protests: Growing list of celebrities pledge support for demonstrators' (2020) (accessible here).
[29] South African Government News Agency 'July unrest instigator Mdumiseni Zuma slapped with 12 year jail sentence' (2023) (accessible here).
[30] *Manuel v Economic Freedom Fighters and Others* (2019) (accessible here).
[31] ALT Advisory, Avani Singh, 'Social media and defamation online: Guidance from Manuel v EFF', (2019) (accessible here).

## 5. THE RIGHT TO FREEDOM OF EXPRESSION ONLINE

International law is clear that the right to freedom of expression exists as much online as it does offline, though there are challenges in implementing this principle in practice. For example, article 19(2) of the ICCPR is explicit that the right to freedom of expression applies "regardless of frontiers," and the United Nations Human Rights Council (UNHRC) General Comment No. 34 further clarifies that this includes internet-based modes of communication.[32]

### Challenges to freedom of expression online

Some examples of new challenges to exercising freedom of expression online include:

- The blocking, filtering, and removal of content, often executed by internet intermediaries on behalf of the government outside of regulatory or legislative provisions, and with little transparency or accountability.
- Online content regulation through overly broad and vague cybercrimes legislation intending to counter genuinely criminal activity online, such as child pornography, but often misused by governments to stifle criticism and free speech.[33]
- The rapid growth in mis- and disinformation on online platforms led to backlash from states, who attempted to regulate it with broad 'fake news' regulations.[34]
- Defining and protecting journalists and the media in an environment now saturated with bloggers and social media writers, and defending them from online harassment, particularly women who are disproportionately subject to online harms.[35]
- Enabling free and equal access to the internet, including overcoming the challenges of unaffordability while preventing potential distortions and filtering of content.[36]
- Tackling the spread of hate speech on online platforms without placing undue responsibility on private actors to proactively limit content on their platforms.
- Protecting the public from invasive uses of private data and protecting anonymous communications, while simultaneously enabling accountability for illegal behaviour online, such as child sexual abuse material (CSAM).
- The use of automated systems, including those using artificial intelligence (AI), to filter and monitor online speech and to make decisions about the removal of content, as well as to make automated decisions about users of digital tools in ways that are potentially biased and discriminatory.

[32] UN Human Rights Council 'General Comment no. 34' (2011) (accessible here) at para 12.
[33] For more see Module 7 in this series from Media Defence on 'Cybercrimes'.
[34] For more see Module 8 in this series from Media Defence on 'False news, misinformation and propaganda'.
[35] See *Isaac Olamikan & Anor v. Federal Republic of Nigeria* an ECOWAS decision that addresses the development of online media and highlights the influential role of influencers and content creators in shaping public opinion, noting that social media offers an unrestricted platform for information dissemination and expression.
[36] For more see Module 3 in this series from Media Defence on 'Access to the internet'.

## 6. CONCLUSION

Digital rights are an emergent and dynamic field. Protecting digital rights involves a host of new actors that did not exist in previous generations of the media, such as internet intermediaries. The internet is an incredibly powerful tool for social progress and the fuller realisation of human rights, but it also gives rise to particular challenges. Nevertheless, international law is clear that the same rights that apply offline also apply online, and while those challenges might be immense, the benefits of getting it right — a free and fair internet accessible to all — are too important not to take digital rights seriously.