Module 2

INTRODUCTION TO DIGITAL RIGHTS

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

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

December 2020

TABLE OF CONTENTS

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.**
- **It is crucial that human rights defenders engage with the new challenges posed online and act to protect and promote digital rights in the rapidly evolving online world.**

INTRODUCTION

Digital rights are human rights in the digital realm. The term 'digital rights' speaks to questions around how the same rights that have always been 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. Protecting and developing online spaces where human rights can be respected and promoted requires effective responses to oppressive regulations, and innovative solutions.

Additionally, 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 that have reshaped how humans communicate, participate and behave. 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.

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, do bloggers and citizen journalists count as journalists and should they be afforded the same protections with regards to freedom of expression? How should states regulate the re-tweeting or resharing of hate speech? What about regulations for defamatory statements from anonymous accounts? 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. In Africa, there is a growing trend of implementing 'social media taxes,' making internet access even more unaffordable in a region that already has the highest financial barriers to access in the world.[4] Following the implementation of a social media tax in Uganda in 2018, internet penetration dropped by five million users within the space of just three months.[5]
- **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 are generally considered a form of prior restraint to freedom of expression as it restricts internet users from expressing themselves through these services and websites before the

[1] ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', ACHPR/Res.362(LIX) (2016) (accessible at: https://www.achpr.org/sessions/resolutions?id=374).
[2] UN Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet' A/HRC/32/L.20 (2016) at para 1 (accessible at: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf).
[3] For more see Juan Carlos Lara, 'Internet access and economic, social and cultural rights', Association for Progressive Communications, (2015) at pp 10-11 (accessible at: https://www.apc.org/en/pubs/internet-access-and-economic-social-and-cultural-r).
[4] Web Foundation, 'New research explores impact of social media taxes in East and Southern Africa' (2019) (accessible at: https://webfoundation.org/2019/06/new-research-explores-impact-of-social-media-taxes-in-east-and-southern-africa/).
[5] CIPESA, 'Social Media Tax Cuts Ugandan Internet Users by Five Million, Penetration Down From 47% to 35%' (2019) (accessible at: https://cipesa.org/2019/01/%EF%BB%BFsocial-media-tax-cuts-ugandan-internet-users-by-five-million-penetration-down-from-47-to-35/).

expression actually occurs. The ICCPR has been interpreted as providing for an absolute prohibition on such measures.[6] 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.[7]

- **The freedom to choose among information sources.** The 2017 Report of the UN Special Rapporteur on freedom of expression 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.[8] This concept is known as network neutrality, the principle that all internet data should be treated equally without undue interference.[9] In Africa, there has been significant debate about access to zero-rated content, which is applications or websites the usage of which a mobile operator does not count towards a user's monthly data allotment, rendering it 'free.'[10] This is a practice commonly used by social media platforms. On the one hand, zero-rating provides access to the internet for persons who might not otherwise have been able to do so, but on the other hand, can lead to unfair competition, and can distort users' perceptions by only allowing access to particular sites.[11]
- **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.[12] 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 variety of new ways, such as biometric data collection and facial recognition technology.[13] In January 2020, a High Court in Kenya handed down a judgment finding that a new national biometric identity

[6] 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 at p 398 (1987) (accessible at: https://brill.com/view/title/9771).

[7] ECOWAS Community Court of Justice, Suit No. ECW/CCJ/APP/61/18 (2020) (accessible at: http://prod.courtecowas.org/wp-content/uploads/2020/09/JUD_ECW_CCJ_JUD_09_20.pdf).

[8] UN Special Rapporteur on Freedom of Expression, Report A/HRC/38/35 on the Role of Digital Access Providers at para.\ 23 (2017) (accessible at: https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2017ReporttoHRC.aspx).

[9] For more on net neutrality, see pp 2-9 of Module 5 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online (accessible at: https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-5-trends-in-censorship-by-private-actors/).

[10] Research ICT Africa, 'Zero-rated internet services: What is to be done?' (2020) (accessible at: https://www.researchictafrica.net/docs/Facebook%20zerorating%20Final_Web.pdf).

[11] For a discussion on zero-rating in Africa, see Research ICT Africa, 'Much ado about nothing? Zero-rating in the African context', (2016) (accessible at: https://www.researchictafrica.net/publications/Other_publications/2016_RIA_Zero-Rating_Policy_Paper_-_Much_ado_about_nothing.pdf).

[12] Data Protection Africa, 'Trends' (accessible at: https://dataprotection.africa/trends/).

[13] For more, see page 11 of Module 1 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online (accessible at: https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-1-general-overview-of-trends-in-digital-rights-globally-and-expected-developments/).

system could not be rolled out until a comprehensive data protection framework was in place.[14]

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: (i) conduits, which are technical providers of internet access or transmission services; and (ii) 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.
- 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. As pointed out by the UN Special Rapporteur on Freedom of Expression 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]

Some countries in Africa have laws providing for the limitation of intermediary liability, such as Ghana and Uganda.[17] To protect themselves from liability even in cases where such legislation does not exist, intermediaries often develop terms and conditions that specify their

[14] Kenyan High Court at Nairobi , Consolidated Petitions No. 56, 58 & 59. (2020) (accessible at: http://kenyalaw.org/caselaw/cases/view/189189/).
[15] Association for Progressive Communications, 'Frequently asked questions on internet intermediary liability' (2014) (accessible at: https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-internetintermed).
[16] OHCHR, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (2011) (accessible at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf).
[17] See article 92 of Ghana's Electronic Transactions Act of 2008 (accessible at: https://www.researchictafrica.net/countries/ghana/Electronic_Transactions_Act_no_772:2008.pdf) and Section 29 of Uganda's Electronic Transactions Act of 2011 (accessible at: https://www.ug-cert.ug/files/downloads/Electronic%20Transactions%20Act%20(Act%20No.%208%20of%202011).pdf).

responsibilities and those of their customers.[18] Other countries in Africa have laws that explicitly make intermediaries liable for their actions regarding content posted using their services.[19] The High Court of Tanzania ruled in 2017 in *Jamii Media v The Attorney General of Tanzania and Another*[20] 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.[21]

Additionally, 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 lack transparency and public scrutiny.[22] 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.[23] 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.[24] This, clearly, has serious consequences for freedom of expression online.

THE BORDERLESS ENJOYMENT OF FREEDOM OF EXPRESSION

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

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

In October 2020, young Nigerians took to the street 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

[18] CIPESA, 'State of Internet Freedom in Africa 2017,' at p 23 (2017) (accessible at: https://cipesa.org/?wpfb_dl=254).
[19] 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.
[20] High Court of Tanzania, Miscellaneous Civil Cause No. 9 of 2016 (2017) (accessible at: https://thrdc.or.tz/wp-content/uploads/2019/09/JAMII-MEDIA-Judgment-20-Mar-2017.pdf).
[21] CIPESA, 'Tanzania Court Deals a Blow to Intermediary Liability Rules' (2017) (accessible at: https://cipesa.org/2017/04/tanzania-court-deals-a-blow-to-intermediary-liability-rules/).
[22] Association for Progressive Communications, 'Policing the internet: Intermediary liability in Africa' (2020) (accessible at: https://www.apc.org/en/project/policing-internet-intermediary-liability-africa-0).
[23] CIPESA above n 18 at pp. 24.
[24] Quartz Africa, 'Zimbabwe's internet blackout shows how powerless major telcos are against governments' (2019) accessible at: https://qz.com/africa/1526754/zimbabwe-shutdown-econet-blames-government-whatsapp-still-off/).

messages of solidarity had been reshared by celebrities, politicians, activists and concerned citizens around the world.[25]

Before the internet, this would have been next to impossible. The borderless nature of the internet can lead to international pressure being put on states for rights violations, global campaigns being developed and supported, and a rigorous marketplace of ideas being fostered.

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 very difficult to remove it. In the 2019 case of *Manuel v Economic Freedom Fighters and Others*,[26] 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).[27] This is a particular challenge for finding effective remedies to claims of defamation, hate speech, or the right to be forgotten.

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.[28]

Challenges to freedom of expression online

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

[25] BBC, 'End Sars protests: Growing list of celebrities pledge support for demonstrators' (2020) (accessible at: https://www.bbc.com/news/world-africa-54629449).
[26] High Court of South Africa, Gauteng Division, Case no. 13349/2019, (2019) (Accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2019/157.pdf).
[27] ALT Advisory, Avani Singh, 'Social media and defamation online: Guidance from Manuel v EFF', (2019) (accessible at: https://altadvisory.africa/2019/05/31/social-media-and-defamation-online-guidance-from-manuel-v-eff/).
[28] UN Human Rights Council, 'General Comment no. 34 at para. 12 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).

- The blocking, filtering, and removal of content, often executed by internet intermediaries on behalf of 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.[29]
- The rapid growth in misinformation on online platforms leading to backlash from states, who attempt to regulate it with broad 'fake news' regulations.[30]
- 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.
- Enabling free and equal access to the internet, including overcoming the challenges of unaffordability while preventing against the distortion that can be created by zero-rating.[31]
- 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.

CONCLUSION

Digital rights is 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 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.

[29] For more see Module 7 in this series from Media Defence on 'Cybercrimes.'
[30] For more see Module 8 in this series from Media Defence on 'False news, misinformation and propaganda'.
[31] For more see Module 3 in this series from Media Defence on 'Access to the internet'.