Module 1

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

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 1

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

- **Human rights have become firmly entrenched in international law since the adoption of the seminal Universal Declaration of Human Rights in 1948.**
- **Since then, international human rights law has become increasingly influential in domestic courts and has set a global standard for the protection of human rights.**
- **Freedom of expression is one such right that has benefitted from this trend, but it is increasingly under threat from the dramatic changes to the media and information eco-system occasioned by the rise of the internet.**
- **African regional instruments, if properly understood and utilised, constitute a powerful tool in the arsenal of defenders of freedom of expression.**

INTRODUCTION

Since at least the formation of the United Nations (UN) and the construction of a human rights regime founded in international law in 1948, the right to freedom of expression became universally acknowledged. An example of this universal acknowledgement is found in the case of *Madanhire and Another v Attorney General* from the Zimbabwean Constitutional Court, where the Court stated that:

> "There can be no doubt that the freedom of expression, coupled with the corollary right to receive and impart information, is a core value of any democratic society deserving of the utmost legal protection. As such, it is prominently recognised and entrenched in virtually every international and regional human rights instrument."[1]

Because the principle of freedom of expression is explicit in so many treaties, soft law instruments, and widely acknowledged in domestic and regional law, it has come to be regarded as a principle of customary international law.[2] Nevertheless, today's rapidly evolving world is presenting new and unprecedented threats to the full realisation of the right to freedom of expression for many around the world, especially journalists and the media.

---

[1] Zimbabwean Constitutional Court, Constitutional Application No. CCZ 78/12, para. 7 (2014) (accessible at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2015/03/Madanhire-v.-Attorney-General-CCZ-214.pdf).

[2] See article 38 of the Statute of the International Court of Justice (1948) (accessible at https://legal.un.org/avl/pdf/ha/sicj/icj_statute_e.pdf) which documents the four recognised sources of international law.

In order for African defenders of freedom of expression to adequately address these new challenges, it is crucial to have a firm understanding of freedom of expression in international and regional law. This module seeks to provide an overview of the key principles related to freedom of expression in international law, as well as in African regional instruments, and provide a foundation for understanding how to use these principles in the new digitally-connected world.

KEY PRINCIPLES OF INTERNATIONAL LAW

Human rights in international law

Human rights are inherent to all persons and dictate the minimum standard that must be applied to all people. They are enshrined in both national and international law and all persons are entitled to enjoy such rights without discrimination. When fully realised, human rights reflect the minimum standards to enable persons to live with dignity, freedom, equality, justice and peace.

The cornerstones of human rights are that they are inalienable and therefore cannot be taken away; interconnected and therefore dependant on one another; and indivisible, meaning that they cannot be treated in isolation. Not all rights are absolute, and some rights may be subject to certain limitations and restrictions in order to balance competing rights and interests.

Human rights under international law are generally considered to be rooted in the Universal Declaration of Human Rights (UDHR), which was agreed to by the United Nations in 1948 following the end of World War II. The UDHR is not a binding treaty in itself, but countries can be bound by those UDHR principles that have acquired the status of customary international law. The UDHR has further been the catalyst to creating other binding legal instruments, most notably the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR). Together, these three instruments constitute what is known as the International Bill of Rights. Since their adoption, additional thematic treaties have been developed to address certain topics:

- The International Convention on the Elimination of All Forms of Racial Discrimination;
- The Convention on the Elimination of All Forms of Discrimination against Women;
- The Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment;
- The Convention on the Rights of the Child;
- The International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families;
- The Convention on the Rights of Persons with Disabilities; and
- The International Convention for the Protection of All Persons from Enforced Disappearance.

In Africa, the African Charter on Human and Peoples' Rights (African Charter) is the primary treaty governing human rights on the continent. States are the primary duty-bearers for the realisation of human rights, which encompasses both negative and positive duties. With negative duties, states must avoid violating the rights of individuals and communities within

their territories and protect them against violations by others. On the other hand, the obligation to fulfil human rights requires states to take positive steps to enable the full enjoyment of these rights. By ratifying treaties, states commit to put in place domestic measures, such as legislation, to give effect to their treaty obligations.

Applying international law in a domestic context

International and regional human rights law not only sets a standard for domestic law to follow, but is in many cases binding on states. However, the exact way in which international law obligations are implemented domestically varies around the world.

The ICCPR creates a binding obligation on states. Regional human rights standards are also particularly influential, especially since there is near-universal ratification of the African Charter by African states.[3]

The way in which international law applies domestically is largely determined by whether a state applies monist or dualist principles:

- **Monist** states are those where international law is automatically part of the domestic legal framework. However, their exact status — whether above or on par with a state's constitution or domestic law — varies.
- **Dualist** states are those where international treaty obligations only become domestic law once they have been enacted by the legislature. Until this has happened, courts are not expected to comply with these obligations in a domestic case, although there are states wherein some parts of international law may be automatically applied or used as a tool to interpret domestic law.

States with common law systems are invariably dualist, and while States with civil law systems are more likely to be monist, many are not. Because the application of international law is so varied and complicated, practitioners must evaluate the specific context in a given country to understand how to apply international and regional law most effectively.

THE RIGHT TO FREEDOM OF EXPRESSION UNDER INTERNATIONAL LAW

Freedom of expression under international law

The rights contained under article 19 of the ICCPR comprise three core tenets: the right to hold opinions without interference (freedom of opinion); the right to seek and receive information (access to information); and the right to impart information (freedom of expression).

The UN Human Rights Committee's (UNHRCtte) General Comment No. 34 on the ICCPR notes that the right to freedom of expression includes, for example, political discourse, commentary on one's own affairs and on public affairs, canvassing, discussion of human

[3] African Commission on Human and Peoples' Rights, 'Ratification Table – African Charter on Human and Peoples' Rights' (accessible at: https://www.achpr.org/ratificationtable?id=49).

rights, journalism, cultural and artistic expression, teaching, and religious discourse.[4] It also embraces expression that may be regarded by some as deeply offensive.[5] The right covers communications that are both verbal and non-verbal, and all modes of expression, including audio-visual, electronic and internet-based modes of communication.[6]

In terms of article 19(3) of the ICCPR, the right to freedom of expression contained in article 19(2) may be subject to certain restrictions:

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (*ordre public*), or of public health or morals."

With respect to a limitation on the right to freedom of expression under article 19(2) of the ICCPR, a three-part test is used to assess whether such a limitation is justified: (i) the limitation must be provided for in law; (ii) it must pursue a legitimate aim; and (iii) it must be necessary for a legitimate purpose.[7] This test applies similarly to limitations of the right to freedom of expression under other legal instruments, including the African Charter.

Freedom of expression online

Article 19(2) of the ICCPR stipulates that the right to freedom of expression applies regardless of frontiers and through any media of one's choice. General Comment No. 34 further explains that article 19(2) includes internet-based modes of communication.[8]

In a 2016 resolution, the UN Human Rights Council (UNHRC) affirmed that:[9]

> "[T]he 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

---

[4] OHCHR, General Comment No. 34 at para 11. (2011) (accessible at: https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf).
[5] *Ibid* at para 11. For further discussion on this, see Nani Jansen Reventlow, 'The right to 'offend, shock or disturb', or the importance of protecting unpleasant speech' in Perspectives on harmful speech online: A collection of essays, Berkman Klein Center for Internet & Society, 2016 at pp 7-9 (accessible at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746096).
[6] *Ibid* General Comment No. 34 at para 12.
[7] For a fuller discussion on how freedom of expression may be legitimately limited, see the training manual published by Media Defence on the principles of freedom of expression under international law: Richard Carver, 'Training manual on international and comparative media and freedom of expression law' at pp 14-16 (2018) accessible at: https://www.mediadefence.org/sites/default/files/resources/files/MLDI.FoEManual.Version1.1.pdf). For more on proportionality see the 2002 decision of *Attorney-General v 'Mopa* in the Lesotho Court of Appeal (accessible at: https://lesotholii.org/ls/judgment/high-court/2002/3) and *Zimbabwe Lawyers for Human Rights & Associated Newspapers of Zimbabwe v Zimbabwe* in the ACHPR (2009) (accessible at: https://africanlii.org/afu/judgment/african-commission-human-and-peoples-rights/2009/98)
[8] General Comment No. 34 above at n 4 at para 12.
[9] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/32/L.20 (2016) at para 1 (accessible at: https://digitallibrary.un.org/record/845728?ln=en).

> 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."

In 2016, the African Commission on Human and Peoples' Rights (ACHPR) affirmed the UNHRC's declaration and called on states to respect and to take legislative and other measures to guarantee, respect and protect citizens' rights to freedom of information and expression through access to internet services.[10]

While freedom of expression is clearly protected by a considerable body of treaty law, it can also be regarded as a principle of customary international law, given how frequently the principle is enunciated in treaties, as well as other soft law instruments.[11] Most human rights treaties, including those dedicated to the protection of the rights of specific groups — such as women, children and people with disabilities — also make explicit mention of freedom of expression.[12]

Freedom of expression in the digital age

In recent years, freedom of expression has been under attack from a variety of new and challenging sources. First, the rise of social media and new media platforms has in many places decimated the revenue model for independent media, leaving many media houses weakened or bankrupt and unable to play their crucial role of holding power to account. Secondly, the rise of the internet has upended the traditional information eco-system in various ways. This has resulted in a backlash from governments seeking to regulate growing cybercrimes and a flood of misinformation, often to the detriment of freedom of expression and legitimate dissent.[13] Nigeria and Ethiopia are just two examples of this rising trend.[14]

The importance of protecting freedom of expression in this new digital age is emphasised by the new ACHPR Declaration on Freedom of Expression and Access to Information in Africa, published in April 2020. The Declaration differs from the 2002 Declaration in the following notable ways:

- It emphasises the importance of access to information by dedicating an entire section to the subject, where the 2002 Declaration mentioned it only in the Preamble.

[10] ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', ACHPR/Res.362, (2016) (accessible at: https://www.achpr.org/sessions/resolutions?id=374).
[11] Carver above at n 7 at p. 5.
[12] *Ibid* at p 5.
[13] For more see Washington Post, 'There's a worrying rise in journalists being arrested for 'fake news' around the world' (2019) (accessible at: https://www.washingtonpost.com/world/2019/12/12/theres-worrying-rise-journalists-being-arrested-fake-news-around-world/) and Freedom House, 'The Rise of Digital Authoritarianism: Fake news, data collection and the challenge to democracy' (2018) (accessible at: https://freedomhouse.org/article/rise-digital-authoritarianism-fake-news-data-collection-and-challenge-democracy).
[14] Al Jazeera 'Nigerians raise alarm over controversial Social Media Bill' (2019) (accessible at: https://www.aljazeera.com/news/2019/12/18/nigerians-raise-alarm-over-controversial-social-media-bill) and Al Jazeera, 'Ethiopia passes controversial law curbing 'hate speech' (2020) (accessible at https://www.aljazeera.com/news/2020/02/ethiopia-passes-controversial-law-curbing-hate-speech-200213132808083.html).

- It calls on States to "recognise that universal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression [and] access to information."[15]
- The Declaration "articulates State obligations with respect to internet intermediaries, noting that States must ensure that internet intermediaries provide access to the internet in a non-discriminatory manner and that the use of algorithms or other artificial intelligence uses do not infringe on international human rights standards;"[16]
- It provides guidance on requests to remove online content.[17]
- It addresses the protection of personal information and communication surveillance and requires States to adopt laws regulating the processing of personal information.[18]

WHO CONSTITUTES A JOURNALIST?

A particular challenge that arises in the context of digital rights is the changing roles of journalists and publishers online. Journalists are vitally important protagonists when discussing digital rights and freedom of expression because they investigate and criticise the actions of the state and other powerful actors as part of the exercise of their functions. The particular role that the media plays in achieving an open and democratic society, and the special protections that this deservedly engages, have frequently been emphasised by the courts. Of course, the media industry has also experienced dramatic and rapid change as a result of the rise of the internet and social media, thus defending press freedom has become more complicated and needs to be tailored to the new and evolving dynamics of the media eco-system.

Nevertheless, General Comment No. 34[19] expressly provides that journalism is a function shared by a wide range of actors, from professional full-time reporters and analysts to bloggers and others who engage in forms of self-publication in print and on the internet. Thus, journalistic protections should be construed broadly to apply to both professional and citizen journalists who are disseminating information in the public interest, so as not to unduly constrain freedom of expression.

In 2013, the UN Special Rapporteur on freedom of expression stated that[20] "[n]ew technologies have provided unprecedented access to means of global communication, and have therefore introduced new means of reporting on news and events around the world."

---

[15] ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa', Principle 37(2) (2019) (accessible at: https://www.achpr.org/legalinstruments/detail?id=69).
[16] International Justice Resource Center, 'New ACHPR Declaration on Freedom of Expression & Access to Information' (2020) (accessible at: https://ijrcenter.org/2020/04/22/new-achpr-declaration-on-freedom-of-expression-access-to-information/).
[17] ACHPR above at n 15 at Principle 39(4).
[18] *Ibid* at Principle 42.
[19] General Comment No. 34 above at n 4.
[20] Report of the UNSR on Freedom of Expression to the UN General Assembly (UNGA), A/65/284, at para 21 (2013) (accessible at: https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf).

The report notes that, although citizen journalists are not trained professional journalists, it is nevertheless an important form of journalism as it can contribute to a richer diversity of views and opinions, and can provide an immediate, insider's view of a conflict or catastrophe.

In interpreting the ICCPR in relation to freedom of the press, General Comment No. 34 states:[21]

> "The Covenant embraces a right whereby the media may receive information on the basis of which it can carry out its function. The free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential. This implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion. The public also has a corresponding right to receive media output… As a means to protect the rights of media users, including members of ethnic and linguistic minorities, to receive a wide range of information and ideas, States parties should take particular care to encourage an independent and diverse media."

Recently, the High Court of South Africa provided a resounding defence of freedom of the press in their role of providing access to information for the public and enabling freedom of expression in the 2019 case of *amaBhungane v Minister of Justice*.[22] In defending the right of journalists to protect the confidentiality of their sources and to be safe from surveillance, the judgment stated:

> "Despite much lauding of the role of the media and the express guarantee of freedom of expression and of the media, in particular, in section 16(1)(a) of the Constitution, there has been a reluctance to take the next step needed to recognise journalists as a special class of persons whose intrinsic working methods warrant especial protection, such as lawyers enjoy.[23]
>
> In a country that is as wracked by corruption in both our public institutions and in our private institutions as ours is, and where the unearthing of wrongdoing is significantly the work of investigative journalists, in an otherwise, seemingly, empty field, it is hypocritical to both laud the press and ignore their special needs to be an effective prop of the democratic process."[24]

UNITED NATIONS

The United Nations was the first international entity to enshrine the right to freedom of expression in international law in 1948 with the Universal Declaration of Human Rights. Article 19 states: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." This was the foundation of what later

[21] General Comment No. 34 above at n 4.
[22] High Court of South Africa in Pretoria, Case No. 25978/2017, (2019) (accessible at: http://www.saflii.org/za/cases/ZAGPPHC/2019/384.html).
[23] High Court of South Africa Case No. 25978/2017 at para.130 (accessible at: http://www.saflii.org/za/cases/ZAGPPHC/2019/384.html).
[24] *Ibid* at para 131.

became article 19 of the ICCPR, and was further elaborated on in General Comment No. 34 by the UNHRCtte.[25]

The ICCPR is not the only treaty within the United Nations framework to address the right to freedom of expression. For instance:

- Article 15(3) of the ICESCR specifically refers to the freedom required for scientific research and creative activity, providing that: "The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity."
- Articles 12 and 13 of the UN Convention on the Rights of the Child (CRC) contain extensive protections relating to the right to freedom of expression enjoyed by children in articles 12 and 13.
- Article 21 of the United Nations Convention on the Rights of Persons with Disabilities (CRPD) contains extensive protections relating to freedom of expression and access to information of persons with disabilities in article 21.

It is therefore clear that the right to freedom of expression is firmly entrenched within the United Nations system, both as an important right on its own, as well as a crucial enabling right. For example, as stated in General Comment No. 25, in the context of the right to participate in public affairs, voting rights and the right of equal access to public service, it was noted that:

> "Citizens can also take part in the conduct of public affairs by exerting influence through public debate and dialogue with their representatives or through their capacity to organize themselves. This participation is supported by ensuring freedom of expression, assembly and association."[26]

AFRICAN REGIONAL INSTRUMENTS

A number of regional instruments guarantee the right to freedom of expression in Africa. For example, article 9 of the African Charter provides for it as follows:

> "1. Every individual shall have the right to receive information.
> 2. Every individual shall have the right to express and disseminate his opinions within the law."[27]

Oversight and interpretation of the African Charter is the sole domain of the African Commission on Human and Peoples' Rights (ACHPR), which was established in 1987. A protocol to the African Charter was adopted in 1998 which created an African Court on Human and Peoples' Rights (ACtHPR), and which came into effect in 2005.[28]

It should be noted that reference to "within the law" in article 9(2) the African Charter should not be seen as permitting states to enact laws that violate the right to freedom of expression.

---

[25] General Comment No. 34 above at n 4 at para 11.
[26] UNHRCtte General Comment No. 25 at para 8 (1996) (accessible at: https://www.equalrightstrust.org/ertdocumentbank/general%20comment%2025.pdf).
[27] African Charter on Human and Peoples' Rights (1981) (accessible at: https://www.achpr.org/legalinstruments/detail?id=49).
[28] *Ibid.*

The ACHPR made clear in *Constitutional Rights Project v Nigeria*[29] that "[g]overnment[s] should avoid restricting rights, and take special care with regard to those rights protected by constitutional or international human rights law. No situation justifies the wholesale violation of human rights."

The right to freedom of expression is further underscored in the Declaration of Principles on Freedom of Expression in Africa (revised in 2019),[30] and the ACHPR Guidelines on Freedom of Association and Assembly in Africa.[31]

There are also a number of sub-regional instruments that engage the right to freedom of expression, such as the Treaty Establishing the East African Community (EAC)[32], the Revised Treaty of the Economic Community of West African States (ECOWAS), and the Protocol on Culture, Information and Sport of the Southern African Development Community (SADC).

Other regional bodies also provide useful guidance on how to interpret the right to freedom of expression. For example, the European Court of Human Rights has published a Case-Law Guide[33] providing insight into the decisions of the Court pertaining to article 10 of the European Convention on Human Rights, which deals with freedom of expression. Likewise, the Inter-American Court of Human Rights provides a jurisprudence booklet on freedom of expression.[34]

CONCLUSION

The right to freedom of expression is firmly established in international and regional human rights law, which has proven instrumental in ensuring binding domestic and regional judgments against states seeking to violate this fundamental and touchstone right. However, the right is increasingly being challenged in new ways as a result of the dramatic changes wrought upon the world by the growth of the internet and technology, particularly for journalists and the media. Leveraging the international law and jurisprudence that exists to continue to protect this fundamental right in a rapidly evolving world is more important than ever.

---

[29] ACHPR, Communication No. 102/93 (1998) at paras 57-58 (accessible at: https://www.achpr.org/sessions/descions?id=100).
[30] ACHPR above at n 15.
[31] ACHPR, Guidelines on Freedom of Association and Assembly in Africa (accessible at https://www.achpr.org/presspublic/publication?id=22).
[32] See, for instance, *Burundi Journalists' Union v The Attorney General of the Republic of Burundi*, Reference No. 7 of 2013 (2015) (accessible at: https://www.eacj.org/?cases=burundi-journalists-union-vs-the-attorney-general-of-the-republic-of-burundi).
[33] European Court of Human Rights, 'Guide on Article 10 of the European Convention on Human Rights' (2020) (accessible at: https://www.echr.coe.int/Documents/Guide_Art_10_ENG.pdf). For more, see also the ECHR's Factsheets on Access to the Internet and Freedom to Receive and Impact Information and Ideas (accessible at: https://www.echr.coe.int/Documents/FS_Access_Internet_ENG.pdf), on Hate Speech (accessible at: https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf), on the Protection of Journalistic Sources (accessible at: https://www.echr.coe.int/Documents/FS_Journalistic_sources_ENG.pdf), and on the Protection of Reputation (accessible at: https://www.echr.coe.int/Documents/FS_Reputation_ENG.pdf).
[34] Inter-American Court of Human Rights, 'Cuadernillo de Jurisprudencia de la Corte Interamericana de Derechos Humanos nº 16: libertad de pensamiento y de expresión' (accessisble at: https://www.corteidh.or.cr/sitios/libros/todos/docs/cuadernillo16.pdf in Spanish).

Module 2

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

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[35] (ACHPR) and the United Nations[36] (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.[37] 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.[38] 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.[39]

---

[35] 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).
[36] 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).
[37] 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).
[38] 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/).
[39] 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/).

- **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 expression actually occurs. The ICCPR has been interpreted as providing for an absolute prohibition on such measures.[40] 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.[41]
- **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.[42] This concept is known as network neutrality, the principle that all internet data should be treated equally without undue interference.[43] 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.'[44] 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.[45]
- **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.[46] 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

---

[40] 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).

[41] 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).

[42] 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).

[43] 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/).

[44] 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).

[45] 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).

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

biometric data collection and facial recognition technology.[47] 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.[48]

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.[49]

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,

[47] 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/).

[48] Kenyan High Court at Nairobi , Consolidated Petitions No. 56, 58 & 59. (2020) (accessible at: http://kenyalaw.org/caselaw/cases/view/189189/).

[49] 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).

> because it leads to self-protective and over-broad private censorship, often without transparency and the due process of the law."[50]

Some countries in Africa have laws providing for the limitation of intermediary liability, such as Ghana and Uganda.[51] 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.[52] Other countries in Africa have laws that explicitly make intermediaries liable for their actions regarding content posted using their services.[53] The High Court of Tanzania ruled in 2017 in *Jamii Media v The Attorney General of Tanzania and Another*[54] 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.[55]

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.[56] 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.[57] 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.[58] This, clearly, has serious consequences for freedom of expression online.

---

[50] 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).
[51] 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).
[52] CIPESA, 'State of Internet Freedom in Africa 2017,' at p 23 (2017) (accessible at: https://cipesa.org/?wpfb_dl=254).
[53] 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.
[54] 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).
[55] 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/).
[56] 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).
[57] CIPESA above n 18 at pp. 24.
[58] 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/).

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 messages of solidarity had been reshared by celebrities, politicians, activists and concerned citizens around the world.[59]

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*,[60] 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

[59] BBC, 'End Sars protests: Growing list of celebrities pledge support for demonstrators' (2020) (accessible at: https://www.bbc.com/news/world-africa-54629449).
[60] High Court of South Africa, Gauteng Division, Case no. 13349/2019, (2019) (Accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2019/157.pdf).

their own).[61] 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.[62]

Challenges to freedom of expression online

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

- 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.[63]
- The rapid growth in misinformation on online platforms leading to backlash from states, who attempt to regulate it with broad 'fake news' regulations.[64]
- 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.[65]
- 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.

[61] 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/).
[62] UN Human Rights Council, 'General Comment no. 34 at para. 12 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).
[63] For more see Module 7 in this series from Media Defence on 'Cybercrimes.'
[64] For more see Module 8 in this series from Media Defence on 'False news, misinformation and propaganda'.
[65] For more see Module 3 in this series from Media Defence on 'Access to the internet'.

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.

Module 3

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

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 3

ACCESS TO THE INTERNET

- **An express right to the internet has not been recognised in international law. However, it is widely accepted that access to the internet enables a variety of other fundamental rights.**

- **Practices such as internet shutdowns and blocking and filtering of content often violate the rights to freedom of expression and do not constitute a justifiable limitation.**

- **National security is frequently relied upon as the justification for an interference with access to the internet, as well as other interferences with the right to freedom of expression. While national security is listed as one of the legitimate aims for derogation from the right to freedom of expression in appropriate circumstances, it is often used by states to quell dissent and cover up state abuses.**

- **'Net neutrality' refers to the principle that all internet data should be treated equally without undue interference, and the concept promotes the widest possible access to information on the internet.**

- **Intermediary liability occurs where governments or private litigants can hold technological intermediaries, such as internet service providers (ISPs) and websites, liable for unlawful or harmful content created by users of those services. Such liability has a chilling effect on freedom of expression online.**

IS THERE A RIGHT TO THE INTERNET UNDER INTERNATIONAL LAW?

An express right to the internet has not yet been recognised in any international treaty or similar instrument. This has been the source of much debate, and the arguments for and against whether the right of access to the internet are numerous.

Arguments in favour of access to the internet as a human right[66]	**Arguments against access to the internet as a human right**
• **Necessity**. There is a certain consensus on not only the usefulness of the internet but its crucial role as an "indispensable tool" for human rights and development in the current century. • **Implied existence under current international human rights law**. The full exercise of freedom of expression, participation in cultural life and enjoyment of scientific benefits requires access to the internet. Current standards of living include participation in the broader community in different ways, eg. through the connection to the internet. • **Inevitability**. Several countries including Greece, Estonia, Finland, Spain, Costa Rica and France have asserted or recognised some right of access in their constitutions, legal codes, or judicial rulings. These are most easily accessed online. • **Inseparability**. Technological progress changes how people enjoy their rights and governments should address the link between those rights and their current methods of enjoyment. • **Progression**. The notion of rights themselves has the ability to change, as social contexts change. The growing importance of the internet in changing social contexts makes it necessary to ensure access to it.	• **No international treaty directly creates a right of access to the internet, although some countries, mostly in Europe, have domestic legislation that does**. In simple terms, it is not a human right if the international community has not recognised it as such in a binding instrument, and there is no discussion of a new treaty to do so in any forum. • **Analogy to other forms of media**. There is no right to the telephone, the television, the printed press (either for publishing or receiving it) or any other similar medium that has imposed a duty on states to provide it to its citizens and cover its costs. • **Universality**. Access to the internet is not an economic right that can be construed from article 11 of the ICESCR and article 25 of the UDHR, for they are representative of standards of living that cannot be considered on the same scale for countries in much different stages of development. • **Nature as a right**. Even if there is a legal consideration of access, it is established not as much as an individual right but as an obligation for states. • **Means to an end.** Access to the internet consists of technology, which is a tool, not a right itself.

[66] Juan Carlos Lara, 'Internet access and economic, social and cultural rights', Association for Progressive Communications (September 2015) at p 10-11 (accessible at: https://www.apc.org/sites/default/files/APC_ESCR_Access_Juan%20Carlos%20Lara_September2015%20%281%29_0.pdf). See, also, The 2019 Report of the UN Secretary-General's High level panel on Digital Cooperation noted that "universal human rights apply equally online as offline – freedom of expression and assembly, for example, are no less important in cyberspace than in cyberspace than in the town square" at p 16 (accessible at: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf). In *Delfi v Estonia* the European Court of Human Rights held that the internet provided an unprecedented platform for the exercise of the right to freedom of expression (accessible at: https://globalfreedomofexpression.columbia.edu/cases/delfi-as-v-estonia/).

• **Public support**. Worldwide surveys show a single predominant attitude towards access to the internet: that it should be recognised as a right.[67]	• **Access to the internet is not absolutely necessary for participation in a political community**. A big part of the world's population is without internet access. It is only when such participation already exists and is taken away that it gets attention. • **Inflation**. Claiming that an interest is a basic, fundamental or human right, without considering the conditions under which it can really be realised, inflates the number of rights, diminishing the forcefulness of core traditional human rights. • **Flexibility of existing human rights**. It is not necessary to "create" new rights aside from those already recognised, but to ensure their exercise and enjoyment in changing technological contexts. • **Side effects**. Digital inclusion policies carry concerns regarding the true beneficiary. On one hand, access policies will benefit those users with devices with the ability to access the internet, therefore exacerbating inequalities. On the other hand, lack of control by governments would lead to the need for investment in private telecommunications companies, therefore granting them economic benefit before citizens.

There is an increasing recognition of access to the internet being indispensable to the enjoyment of an array of fundamental rights. The corollary is that those without access to the internet are deprived of the full enjoyment of those rights, which, in many instances, can exacerbate already existing socio-economic divisions. For instance, a lack of access to the internet can impede an individual's ability to obtain key information, facilitate trade, search for jobs, or consume goods and services.

Access entails two distinct but interrelated dimensions: (i) the ability to see and disseminate content online; and (ii) the ability to use the physical infrastructure to enable access to such

[67] The Internet Society, 'Global Internet User Survey 2012' (2012) (accessible at: https://wayback.archive-it.org/9367/20170907075228/https://www.internetsociety.org/sites/default/files/rep-GIUS2012global-201211-en.pdf).

online content. In 2003, UNESCO was among the first international bodies to call on states to take steps to realise a right of access to the internet. In this regard, it stated that:[68]

> "Member States and international organizations should promote access to the Internet as a service of public interest through the adoption of appropriate policies in order to enhance the process of empowering citizenship and civil society, and by encouraging proper implementation of, and support to, such policies in developing countries, with due consideration of the needs of rural communities.
> …
> Member States should recognize and enact the right of universal online access to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or economic situation."

In 2012, the United Nations Human Rights Council (UNHRC) passed an important resolution that "[called] upon all States to facilitate access to the Internet and international cooperation aimed at the development of media and information communications facilities in all countries".[69]

This has been expanded upon in the United Nation's Sustainable Development Goals (SDGs), which recognise that "[t]he spread of information and communications technology and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies".[70] The SDGs further call on states to enhance the use of Information Communication Technologies (ICTs) and other enabling technologies to promote the empowerment of women,[71] and to strive to provide universal and affordable access to the internet in least developed countries by 2020.[72]

The 2016 UN Resolution on the Internet, adopted by the UN Human Rights Council, recognises that the internet can accelerate progress towards development, including in achieving the SDGs, and affirms the importance of applying a rights-based approach in

---

[68] UNESCO, 'Recommendation concerning the promotion and use of multilingualism and universal access to cyberspace' at paras 7 and 15 (accessible at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Eng%20-%20Recommendation%20concerning%20the%20Promotion%20and%20Use%20of%20Multilingualism%20and%20Universal%20Access%20to%20Cyberspace.pdf).

[69] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/20/L.13, 29 June 2012 at para 2 (accessible at: https://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc). This was expanded upon further the following year in UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/Res/26/13, 14 July 2014 (accessible at: https://hrlibrary.umn.edu/hrcouncil_res26-13.pdf).

[70] UNGA, 'Transforming our world: The 2030 agenda for sustainable development', A/Res/70/1, 21 October 2015 at para 15 (accessible at https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E).

[71] *Id*. at goal 5(b) at p 18.

[72] *Id.* at goal 9(c) at p21.

providing and expanding access to the internet.[73] Notably, it affirms the importance of applying a comprehensive rights-based approach in providing and in expanding access to the internet,[74] and calls on states to consider formulating and adopting national internet-related public policies with the objective of universal access and the enjoyment of human rights at their core.[75]

Notwithstanding whether the internet is seen as a self-standing right or an enabling tool to facilitate the realisation of other rights, the groundwork has firmly been laid for the need to realise universal access to the internet. States are concomitantly required to take steps to achieve universal access. However, in reality, universal access to the internet is far from being realised. This is due to a confluence of factors, including a lack of financial resources to be able to access the internet, inadequate locally-relevant content, insufficient levels of digital literacy, and a lack of political will to make this a priority.

In *Kalda v Estonia*, the European Court of Human Rights (ECtHR) held that the applicant's right to freedom of expression had been violated through a prison's refusal to grant him access to internet websites containing legal information, as this had breached his right to receive information.[76] The ECtHR noted that when a state is willing to allow prisoners access to the internet, as with the case in question, it had to give reasons for refusing access to specific sites.[77]

INTERFERENCES WITH ACCESS TO THE INTERNET

Some of the ways in which access to the internet is interfered with is through internet shutdowns, the disruption of online networks and social media sites, and the blocking and filtering of content. Such interferences can pose severe restrictions on the enjoyment of the right to freedom of expression, as well as the enjoyment of a range of other rights and services (including mobile banking, online trade and the ability to access government services via the internet).

The act of disrupting or blocking access to internet services and websites amounts to a form of prior restraint. Prior restraints are State actions that prohibit speech or other forms of expression before they can take place.[78] Due to the profound chilling effect prior restraint can have on the exercise of the right to freedom of expression, the International Covenant on Civil

---

[73] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/Res/32/13, 18 July 2016 at para 2 (accessible at: https://www.refworld.org/docid/57e916464.html).

[74] *Id*. at para 5.

[75] *Id.* at para 12.

[76] Application No. 17429, 19 January 2016 (accessible at: https://hudoc.echr.coe.int/eng?i=001-160270).

[77] *Id*. at para 53. In the subsequent decision of *Jankovskis v Lithuania*, Application No. 21575/08, 17 January 2017 (accessible at: https://hudoc.echr.coe.int/eng?i=001-170354), also in relation to a prisoner who had been refused access to a website containing education-related information, the ECtHR again upheld the applicant's claim of a violation of the right to freedom of expression.

[78] Council of Europe, 'Prior Restrains and Freedom Of Expression: The Necessity of Embedding Procedural Safeguards in Domestic System' (May 2018), (accessible at: https://rm.coe.int/factsheet-prior-restraints-rev25may2018/16808ae88c).

and Political Rights (ICCPR) has been interpreted as effectively providing for the prohibition of most forms of prior restraint on speech.[79] The American Convention on Human Rights contains a similar prohibition.[80] It is therefore imperative that, in order for any such measure to be permissible, it must be able to comply with the three-part limitations test detailed in Module 1.

WHAT IS AN INTERNET SHUTDOWN?

An internet shutdown may be defined as an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.[81] In other words, this arises when someone, be it the government or a private sector actor, intentionally disrupts the internet, a telecommunications network or an internet service, arguably to control or curb what people say or do.[82] This is sometimes also referred to as a 'kill switch'.

In some instances, this may entail there being a total network outage, whereby access to the internet is shutdown in its entirety. In other circumstances, this may also arise when access to mobile communications, websites or social media and messaging applications is blocked, throttled or rendered effectively unusable.[83] Shutdowns may affect an entire country, towns or regions within a country, or even multiple countries, and have been seen to range from several hours to several months.[84]

It should be noted that in order to conduct shutdowns governments typically require the action of private actors that operate networks or facilitate network traffic.[85] As noted by the United Nations Special Rapporteur (UNSR) on freedom of expression, large-scale attacks on network infrastructure committed by private parties, such as distributed denial-of-service (known as 'DDoS') attacks, may also have shutdown effects.

ECOWAS Court finds internet shutdown illegal

---

[79] 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) at p 398.

[80] Article 13: "1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice. 2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure: a. respect for the rights or reputations of others; or b. the protection of national security, public order, or public health or morals."

[81] Access Now, 'What is an internet shutdown?' (accessible at: https://www.accessnow.org/keepiton/?ignorelocale).

[82] *Id*.

[83] Report of the UNSR on Freedom of Expression to the UNGA, A/HRC/35/22, 30 March 2017 (2017 Report of the UNSR on freedom of expression) at para 8 (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement).

[84] *Id*.

[85] *Id*.

In a landmark case confirming that internet shutdowns constitute a form of prior restraint, in June 2020, the Economic Community of West African States (ECOWAS) Community Court of Justice ruled that the internet shutdowns implemented by the Togolese government in 2017 were illegal.[86]

WHAT IS THE BLOCKING AND FILTERING OF CONTENT?

Although a less drastic measure than a complete internet shutdown, the blocking and filtering of content online can also hinder the full enjoyment of the right to freedom of expression.

Blocking/filtering has been defined as follows:

> "[T]he difference between "filtering" and "blocking" is a matter of scale and perspective.
> - Filtering is commonly associated with the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords, or on the basis of their perceived connection to content deemed inappropriate or unlawful;
> - Blocking, by contrast, usually refers to preventing access to specific websites, domains, IP addresses, protocols or services included on a blacklist."[87]

For example, in March 2020 social media sites were blocked in Guinea during a referendum;[88] and in October that same year, a general shutdown of the internet ensued during the General Election.[89] Even after the general connection was re-established, users reported that certain sites, specifically Facebook, remained blocked for a few more weeks. Guinea is unfortunately far from the only African country to implement such techniques in recent years.[90]

WHAT IS NETWORK NEUTRALITY?

Network neutrality — or "net neutrality" — refers to the principle that all internet data should be treated equally without undue interference, and promotes the widest possible access to information on the internet.[91] In other words, ISPs should treat all data that travels over their networks fairly, without improper discrimination in favour of a particular application, website or service.[92] Discrimination in this regard may relate to affecting information in a way that halts,

---

[86] 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).

[87] ARTICLE 19, 'Freedom of expression unfiltered: How blocking and filtering affect free speech, October 2016 at p 7 (accessible at: https://www.article19.org/data/files/medialibrary/38588/Blocking_and_filtering_final.pdf).

[88] Access Now, 'A broken promise to #KeepItOn: Guinea cuts internet access and blocks social media on referendum day' (2020) (accessible at: https://www.accessnow.org/a-broken-promise-to-keepiton-guinea-cuts-internet-access-and-blocks-social-media-on-referendum-day/).

[89] Access Now, 'How internet shutdowns are threatening 2020 elections, and what you can do about it' (2020) (accessible at: https://www.accessnow.org/internet-shutdowns-2020-elections/).

[90] BBC, 'Africa internet: Where and how are governments blocking it?' (2020) (accessible at: https://www.bbc.com/news/world-africa-47734843).

[91] 2017 Report of the UNSR on freedom of expression above at n 18 at para 23.

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

slows or otherwise tampers with the transfer of any data, except for a legitimate network management purpose, such as easing congestion or blocking spam.[93]

The 2017 Report of the UNSR on freedom of expression describes two key ways in which net neutrality may be affected:[94]

- **Paid prioritisation schemes** — where providers give preferential treatment to certain types of internet traffic over others for payment or other commercial benefit.
- **Zero-rating** — which is the practice of not charging for the use of internet data associated with a particular application or service; other services or applications, meanwhile, are subject to metered cost.

In various countries around Africa, there has been significant debate about access to zero-rated content, as particularly social networking sites offer some measure of free access to users. On the one hand, zero-rating provides access to persons who might not otherwise have been able to access the internet, and can serve as a gateway to users to understand the opportunities that the internet can offer. On the other hand is that zero-rating can lead to unfair competition, and can distort users' perceptions by only allowing access to particular sites.[95]

LIMITATION OF THE RIGHT TO FREEDOM OF EXPRESSION

In 2016, the UNSR on freedom of expression noted that "[t]he blocking of Internet platforms and the shutting down of telecommunications infrastructure are persistent threats, for even if they are premised on national security or public order, they tend to block the communications of often millions of individuals".[96] This poses an obvious limitation on the right to freedom of expression, and may further limit a range of other rights.

The 2011 Joint Declaration on Freedom of Expression and the Internet highlights the egregious nature that these limitations can cause:[97]

> "(a) Mandatory blocking of entire websites, [internet protocol (IP)] addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.

---

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

[94] 2017 Report of the UNSR on freedom of expression above n 18 at paras 24-28.

[95] For a discussion on zero-rating in Africa, see Research ICT Africa, 'Much ado about nothing? Zero-rating in the African context', 12 September 2016 (accessible at: https://www.researchictafrica.net/publications/Other_publications/2016_RIA_Zero-Rating_Policy_Paper_-_Much_ado_about_nothing.pdf).

[96] Report of the UNSR on Freedom of Expression to the UNGA, A/71/373, 6 September 2016 (2016 Report of the UNSR on Freedom of Expression) at para 22 (accessible at: https://www.un.org/ga/search/view_doc.asp?symbol=A/71/373).

[97] International Mechanisms for Promoting Freedom of Expression, 'Joint declaration on freedom of expression and the internet', 1 June 2011 (2011 Joint Declaration).

(b) 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 censorship and are not justifiable as a restriction on freedom of expression.

(c) Products designed to facilitate end-user filtering should be required to be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering."

Internet and telecommunications shutdowns that involve measures to intentionally prevent or disrupt access to or dissemination of information online are a violation of human rights law.[98] In the 2016 UN Resolution on the Internet, the UN Human Rights Council stated that it "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and calls upon all States to refrain from and cease such measures".[99]

As set out in General Comment No. 34:[100]

> "Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with [article 19(3) of the ICCPR]. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with [article 19(3) of the ICCPR]. It is also inconsistent with [article 19(3) of the ICCPR] to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."

The UNSR on freedom of expression has noted that internet shutdowns are often ordered covertly and without a legal basis, and violate the requirement that the restrictions must be provided for in law.[101] Similarly, shutdowns ordered pursuant to vaguely formulated laws and regulations, or laws and regulations that are adopted and implemented in secret, also fail to satisfy the legality requirement.[102] In some countries, this has led to the government enacting new laws to expressly allow for shutdowns to take place.[103]

---

[98] 2017 Report of the UNSR on freedom of expression above n 18 at para 8.

[99] 2016 UN Resolution on the Internet above n 8 at para 10.

[100] General Comment No. 34 at para 43.

[101] 2017 Report of the UNSR on Freedom of Expression at para 9.

[102] *Id.* at para 10.

[103] In India, for example, following the internet reportedly having been shut down more than 40 times during the course of 2017, the Department of Telecommunications issued new rules - the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules - in August 2017 allowing the government to shut down telephone and internet services during a public emergency or for public safety. The government had previously relied on section 144 of the Criminal Code that was aimed at preventing "obstruction, annoyance or injury" to impose internet restrictions. This legal development has been met with mixed responses. On the one hand, the new rules would potentially mean that, if the government were to persist with internet shutdowns, this could arguably be done in a more organised manner. On the other hand, however, concerns have been raised about the lack of definitions for the terms "public emergency" or "public safety", and the potential that these new rules may have for censorship online. See: for instance, http://www.hindustantimes.com/india-news/govt-issues-first-ever-rules-to-carry-out-internet-shutdowns-in-india/story-Drn0MnxJAp58RoZoFI7u4L.html.)

The UNSR on Freedom of Expression has further noted that network shutdowns invariably fail to meet the standard of necessity,[104] and are generally disproportionate.[105] States frequently seek to justify this on the ground of national security, which is discussed further below. For example, Chad blocked social media for a period of 472 days in 2018,[106] ostensibly for security reasons. A case was filed against two internet providers,[107] but access was restored shortly after.

Litigating the internet shutdown in Cameroon

Media Defence is currently assisting in litigating a case at the Constitutional Council of Cameroon. In January 2020, the Internet was shut down following protests against the arrest of civil society leaders resisting government efforts to impose the Francophone legal and education systems in these predominantly Anglophone regions. The Internet remained shut down for 93 days and was switched back on hours after Veritas Law filed the constitutional challenge. The constitutional challenge was brought to compel the government to restore the Internet, and so that the Constitutional Council could prevent the government from shutting the Internet down in the future. You can read more here.

In relation to the blocking and filtering of content, there may indeed be circumstances where such measures are justifiable. For example, in relation to websites distributing child pornography. Such measures are still required to meet the three-part test for a justifiable limitation. This will need to be assessed on a case-by-case basis.

Similarly, limitations to network neutrality may also be permissible in certain circumstances, for example for legitimate network management purposes. However, as a general principle, there should be no discrimination in the treatment of internet data and traffic, regardless of the device, content, author, origin and/or destination of the content, service or application.[108] Further, internet intermediaries should be transparent about any traffic or information management practices they employ, and relevant information on such practices should be made available in a form that is accessible to all stakeholders.[109]

NATIONAL SECURITY AS A GROUND OF JUSTIFICATION

[104] 2017 Report of the UNSR on freedom of expression above n 18 at para 14.

[105] *Id.* at para 15.

[106] Quartz Africa, 'Chad has now spent a full year without access to social media' (2019) (accessible at: https://qz.com/africa/1582696/chad-has-blocked-whatsapp-facebook-twitter-for-a-year/).

[107] Africa News, 'Chadian lawyers challenge ongoing social media shutdown' (2018) (accessible at: https://www.africanews.com/2018/08/21/chadian-lawyers-challenge-ongoing-social-media-shutdown//).

[108] 2011 Joint Declaration above n 32 at para 5(a).

[109] *Id.* at para 5(b).

National security is frequently relied upon as the justification for an interference with access to the internet, as well as other interferences with the right to freedom of expression.[110] While this may, in appropriate circumstances, be a legitimate aim, it also has the potential to be used to quell dissent and cover up state abuses.

The covert nature of many national security laws, policies and practices, as well as the refusal by states to disclose information about the national security threat, tends to exacerbate this concern. Furthermore, courts and other institutions have often been deferent to the state in determining what constitutes national security. As has been previously noted:[111]

> "The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability."

Principle XIII(2) of the Declaration of Principles on Freedom of Expression in Africa provides that freedom of expression should not be restricted on public order or national security grounds "unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression".

As set out in the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (the Johannesburg Principles):[112]

> "(a) A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.
>
> (b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest."

---

[110] For a fuller discussion on national security more broadly see Richard Carver, 'Training Manual on International and Comparative Media and Freedom of Expression Law at p 77-88 (accessible here: https://www.mediadefence.org/resources/mldi-manual-on-freedom-of-expression-law/).

[111] Report of the UNSR on freedom of expression to the UNGA, A/HRC/23/40, 17 April 2013 at para 60 (accessible at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf).

[112] Principle 2 of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, November 1996 (accessible at https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf). The Johannesburg Principles were developed by a group of experts in international law, national security and human rights, convened by ARTICLE 19. It was endorsed by the then UNSR on freedom of expression.

Principle 7 goes further to state that the peaceful exercise of the right to freedom of expression shall not be considered a threat to national security or subjected to any restrictions or penalties.

Another important principle contained in the Johannesburg Principles is principle 23, which provides that: "[e]xpression shall not be subject to prior censorship in the interest of protecting national security, except in time of public emergency which threatens the life of the country". As a general proposition, prior restraint of expression is impermissible. The measures described above can often give rise to a prior restraint on content, and consequently have a chilling effect on the enjoyment of the right to freedom of expression.

Similarly, counter-terrorism as a purported justification for network shutdowns or other interferences with access to the internet should also be treated with caution. As noted in General Comment No. 34, the media plays an important role in informing the public about acts of terrorism, and it should be able to perform its legitimate functions and duties without hindrance.[113] While governments may argue that internet shutdowns are necessary to ban the spread of news about terrorist attacks to prevent panic or copycat attacks, it has instead been found that maintaining connectivity may mitigate public safety concerns and help report public order.[114]

At a minimum, if there is to be a limitation of access to the internet, there should be transparency regarding the laws, policies and practices relied upon, clear definitions of terms such as 'national security' and 'terrorism', and independent and impartial oversight being exercised.

INTERMEDIARY LIABILITY

Intermediary liability occurs where governments or private litigants can hold technological intermediaries, such as ISPs and websites, liable for unlawful or harmful content created by users of those services.[115] This can occur in various circumstances, including copyright infringements, digital piracy, trademark disputes, network management, spamming and phishing, "cybercrime", defamation, hate speech, child pornography, "illegal content", offensive but legal content, censorship, broadcasting and telecommunications laws and regulations, and privacy protection.[116]

A report published by UNESCO identifies the following challenges facing intermediaries:[117]

- Limiting the liability of intermediaries for content published or transmitted by third parties is essential to the flourishing of internet services that facilitate expression.

---

[113] General Comment No. 34 at para 46.

[114] 2017 Report of the UNSR on freedom of expression above n 18 at para 14.

[115] Alex Comninos, 'The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain' (2012) at p 6 (accessible at: https://www.apc.org/sites/default/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL_0.pdf).

[116] *Id*.

[117] Rebecca MacKinnon et al, 'Fostering freedom online: The orle of internet intermediaries' (203) at pp 179-180 (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000231162_eng).

- Laws, policies, and regulations requiring intermediaries to carry out content restriction, blocking, and filtering in many jurisdictions are not sufficiently compatible with international human rights standards for freedom of expression.
- Laws, policies, and practices related to government surveillance and data collection from intermediaries, when insufficiently compatible with human rights norms, impede intermediaries' ability to adequately protect users' privacy.
- Whereas due process generally requires that legal enforcement and decision-making are transparent and publicly accessible, governments are frequently opaque about requests to companies for content restriction, the handover of user data, and other surveillance requirements.

There is general agreement that insulating intermediaries from liability for content generated by others protects the right to freedom of expression online. Such insulation can be achieved either through a system of absolute immunity from liability, or a regime that only fixes intermediaries with liability following their refusal to obey an order from a court or other competent body to remove the impugned content.

As to the latter, the 2011 Joint Declaration provides that intermediaries should only be liable for third party content when they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it.[118]

The ECtHR has considered intermediary liability in several cases:

- In 2013, in the case of *Delfi AS v Estonia*, the ECtHR considered the liability of an internet news portal for offensive comments that were posted by readers below one of its online news articles.[119] The portal complained that being held liable for the comments of its readers breached its right to freedom of expression. The ECtHR dismissed the case, holding that the finding of liability by the domestic courts was a justified and proportionate restriction of freedom of expression because the comments were highly offensive; the portal failed to prevent them from becoming public, profited from their existence, and allowed their authors to remain anonymous. It further noted that the fine imposed by the Estonian courts was not excessive.
- In 2016, in the case of *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*, the ECtHR considered the liability of a self-regulatory body of internet content providers and an internet news portal for vulgar and offensive online comments posted on their websites.[120] The ECtHR reiterated that, although not publishers of comments in the traditional sense, internet news portals still had to assume duties and responsibilities. The ECtHR found that, although offensive and vulgar, the comment had not constituted unlawful speech, and upheld the claim of a violation of the right to freedom of expression.

[118] 2011 Joint Declaration above n 32 at paras 2(a)-(b).

[119] Application No. 64569/09, 10 October 2013 (accessible at: httsp://hudoc.echr.coe.int/eng?i=001-155105).

[120] Application No 22947/13, 2 February 2016 (accessible at: https://hudoc.echr.coe.int/eng?i=001-160314).

- In 2017, in the case of *Tamiz v United Kingdom*, the ECtHR had cause to consider the ambit of intermediary liability.[121] The applicant, a former politician in the United Kingdom, had claimed before the domestic courts that a number of third-party comments posted by anonymous users on Google's Blogger.com were defamatory. Before the ECtHR, the applicant argued that his right to respect for his private life had been violated because the domestic courts had refused to grant him a remedy against the intermediary. His claim was ultimately dismissed by the ECtHR on the basis that the resulting damage to his reputation would have been trivial. The ECtHR highlighted the important role that ISPs perform in facilitating access to information and debate on a wide range of political, social and cultural rights, and seemed to endorse the line of argument that ISPs should not be obliged to monitor content or proactively investigate potential defamatory activity on their sites.

Other courts have taken more definitive positions in respect of intermediary liability. For example, the Supreme Court of India has interpreted the domestic law to only provide for intermediary liability where an intermediary has received actual knowledge from a court order, or where an intermediary has been notified by the government that one of the unlawful acts prescribed under the law are going to be committed and the intermediary has subsequently failed to remove or disable access to such information.[122] Furthermore, the Supreme Court of Argentina has held that search engines are under no duty to monitor the legality of third-party content to which they link, noting that only in exceptional cases involving "gross and manifest harm" could intermediaries be required to disable access.[123]

---

[121] *Tamiz v United Kingdom*, Application No. 3877/14, 19 September 2017 (accessible at: https://hudoc.echr.coe.int/eng?i=001-178106). Media Defence, together with a coalition of organisations, made submissions to the ECtHR on proposed principles for intermediary based on best practices in national legislation, the views of the Committee of Ministers of the Council of Europe (CoE) and special mandate holders.

In the above case before the ECtHR, Media Defence together with a coalition of other organisations. The proposed principles are as follows:

- Intermediaries should not be the arbiters of the lawfulness of content posted, stored or transferred by the users of their services.
- Assuming that they have not contributed to or manipulated content, intermediaries should not be liable for content posted, stored or transferred using their services unless and until they have failed to comply with an order of a court or other competent body to remove or block specific content.
- Notwithstanding the above, intermediaries should in no circumstances be liable for content unless it has been brought to their attention in such a way that the intermediary can be deemed to have actual knowledge of the illegality of that content.
- A requirement to monitor content on an ongoing basis is incompatible with the right to freedom of expression contained in article 10 of the European Convention on Human Rights.

The submissions are accessible here: https://www.mediadefence.org/sites/default/files/blog/files/20160407%20Tamiz%20v%20UK%20Intervention%20Filing.pdf.

[122] *Shreya Singhal v Union of India*, Application No. 167/2012 at paras 112-118 (accessible at: https://www.livelaw.in/summary-of-the-judgment-in-shreya-singhal-vs-union-of-india-read-the-judgment/).

[123] *María Belén Rodriguez v Google*, Fallo R.522.XLIX (accessible at: http://www.stf.jus.br/repositorio/cms/portalStfInternacional/newsletterPortalInternacionalJurisprudencia/anexo/Fallo_R.522.XLIX__Corte_Suprema_da_Argentina__28_oct._2014.pdf). The decision has been described in the 2016 Report of the UNSR on Freedom of Expression at para 52.

In light of the vital role played by intermediaries in promoting and protecting the right to freedom of expression online, it is imperative that they are safeguarded against unwarranted interference — by state and private actors — that could have a deleterious effect on the right. For example, as an individual's ability and freedom to exercise their right to freedom of expression online is dependent on the passive nature of online intermediaries, any legal regime that causes an intermediary to apply undue restraint or self-censorship toward content communicated through their services will ultimately have an adverse effect on the right to freedom of expression online. The UNSR has noted that intermediaries can serve as an important bulwark against government and private overreach, as they are usually, for instance, best-placed to push back on a shutdown.[124] However, this can only truly be realised in circumstances where intermediaries are able to do so without fear of sanction or penalties.

CONCLUSION

While the right of access to the internet does not yet find express recognition in international law, it is widely considered as an enabler of the right to freedom of expression and, as with all human rights, can only be justifiably limited if a three-part test is met. Additionally, restrictions to the internet may unduly infringe on freedom of expression and associated rights. In a rapidly developing digital world, the internet is increasingly becoming a contested space and it is used equally by those seeking to defend fundamental rights and those seeking to limit them. The proper understating of concepts such as internet shutdowns, the blocking and filtering of content, net neutrality and intermediary liability are increasingly necessary to fully protect and promote the right to freedom of expression online.

[124] 2017 Report of the UNSR on Freedom of Expression at para 50.

Module 4

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

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 4

DATA PRIVACY AND DATA PROTECTION

- **The right to privacy is gaining prominence with increasing data flows and the concomitant need for the protection of personal information.**
- **In the African context, there are multiple instruments, including the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention), which govern data protection.**
- **Importantly, states should ensure that their domestic legislation details principles for the lawful processing of personal information and that they keep step with data protection developments.**
- **Allied to data protection are the concepts of the 'right to be forgotten', encryption and government-led surveillance.**
- **Notably, the disclosure of journalistic sources as a result of state surveillance has a negative impact on freedom of expression and journalistic freedom.**

INTRODUCTION

The right to privacy and the concomitant requirement to protect personal information has garnered significant attention with the dawn of the information age. While the internet and online information-sharing and data collection increase at an exponential rate, legislative developments have failed to keep pace and adequately protect personal information. However, with time, African states and regional and continental bodies have begun to adopt data protection-related instruments and regulations in an attempt to remedy and vindicate the privacy rights of their citizens.

This module focuses on data protection in Africa and the related concepts of the 'right to be forgotten', encryption and surveillance.

THE RIGHT TO PRIVACY

There is an increasing recognition that the right to privacy plays a vital role in and of itself and in facilitating the right to freedom of expression. For instance, reliance on the right to privacy allows individuals to share views anonymously in circumstances where they may fear being censured for those views, it allows whistle-blowers to make protected disclosures, and it enables members of the media and activists to communicate securely beyond the reach of unlawful government interception.

The right to privacy is contained in article 17 of the International Covenant on Civil and Political Rights (ICCPR), which provides:

> "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> (2) Everyone has the right to the protection of the law against such interference or attacks."

Although not contained in the African Charter on Human and Peoples' Rights (ACHPR), the right to privacy of children is contained in article 10 of the African Charter on the Rights and Welfare of the Child (ACRWC), which provides that:

> "No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks."

The right to privacy has also been recognised in other regional and sub-regional instruments in the context of data protection, which is discussed further below. Moreover, almost all African states guarantee this right under their domestic constitutions.[125]

Interestingly, in 2017, the Supreme Court of India declared that the right to privacy is protected as an intrinsic part of the right to life and personal liberty, and as part of the fundamental freedoms guaranteed by Part III of the Constitution of India.[126] As such, although the Constitution of India does not expressly contain a right to privacy, the right can nevertheless be read when considered in the context of the other rights and freedoms that are constitutionally guaranteed. Although this has not been tested in the context of the ACHPR, there is arguably scope to read the right to privacy into other provisions of the African Charter.

As with the right to freedom of expression, a limitation of the right to privacy must comply with the three-part test for a justifiable limitation. According to the South African Constitutional Court:[127]

---

[125] At the domestic level, more than 50 African constitutions, inclusive of amendments and recent reviews, include reference to the right to privacy. Singh and Power, 'The privacy awakening: The urgent need to harmonise the right to privacy in Africa' African Human Rights Yearbook 3 (2019) 202 at p 202, http://www.pulp.up.ac.za/images/pulp/books/journals/AHRY_2019/Power%202019.pdf.

[126] *Justice K.S. Puttaswamy and Another v Union of India and Others*, Petition No. 494/2012, 24 August 2017 (accessible at: http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf).

[127] *NM and Others v Smith and Others*, [2007] ZACC 6, 4 April 2007 at para 33 (accessible at: https://www.saflii.org/za/cases/ZACC/2007/6.html), citing with approval *Bernstein and Others v Bester NNO and Others*, [1996] ZACC 2, 27 March 1996 at para 77.

> "A very high level of protection is given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual's activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation."

Set out below, we consider specific aspects of the right to privacy and the impact that the internet has had on the enjoyment of this right.

DATA PROTECTION

Data protection laws are aimed at protecting and safeguarding the processing of personal information (or personal data). This refers to any information relating to an identified or identifiable natural person — i.e. the data subject — by which the data subject can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. A data controller, which can typically be either a public or private body, refers to the person or entity responsible for processing the personal information about the data subject.

Data protection is one of the primary measures through which the right to privacy is given effect. There have already been a number of African states that have enacted data protection laws, and more that are in the process of doing so.[128] In addition to giving effect to the right to privacy, data protection legislation also has a key role to play in facilitating trade amongst states, as many data protection laws restrict cross-border data transfers in circumstances where the state receiving the information does not provide an adequate level of data protection.

In relation to data protection of personal information, General Comment No. 16 on article 17 of the ICCPR (General Comment No. 16) provides as follows:[129]

> "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not

[128] At present, there are 21 states in the African Union (AU) that have enacted comprehensive privacy laws: Angola, Benin, Burkina Faso, Cape Verde, Chad, Côte d'Ivoire, Equatorial Guinea, Egypt, Gabon, Ghana, Kenya, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Togolese Republic and Tunisia. There are a further four states that have shown indications of being close to adopting legislation: Niger, Tanzania, Uganda and Zimbabwe. See https://dataprotection.africa/ for more information.

[129] General Comment No. 16 at para 10.

> authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."

Most comprehensive data protection laws typically make provision for the following principles:[130]

- Personal information must be processed fairly and lawfully, and must not be processed unless the stipulated conditions are met.
- Personal information must be obtained for a specified purpose (or purposes), and must not be further processed in any manner incompatible with that purpose.
- Personal data must be adequate, relevant and not excessive in relation to the purpose (or purposes) for which it is processed.
- Personal information must be accurate and, where necessary, kept up to date.
- Personal information must not be kept for longer than is necessary for the purpose of collection.
- Personal information must be processed in accordance with the rights of data subjects provided for under the data protection law.
- Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to another country that does not ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

There are a number of African regional instruments that deal with data protection:

- **AU Convention on Cyber Security and Personal Data Protection 2014**[131] (AU Convention or "Malabo Convention"): This instrument, aimed at a continental level, includes provisions relating to data protection, e-transactions, cybercrimes and cybersecurity. The provisions relating to data protection are contained in Chapter II, and contain the conditions for the lawful processing of personal information, as well as the rights afforded to data subjects. Although it has not entered into force as yet, it may potentially in future be a binding legal instrument on data protection in Africa.

---

[130] Information Commissioner's Office, 'Data protection principles' (accessible at: https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/).

[131] Accessible at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. At present, it has been ratified by one state, and signed by a further ten states.

- **Draft EAC Legal Framework for Cyberlaws 2008**[132] (EAC Legal Framework): This instrument covers topics relating to data protection, electronic commerce, data security and consumer protection. It is not intended to be a model law but instead provides guidance and recommendations to states to assist with informing the development of their laws. Data protection is dealt with briefly at paragraph 2.5 of the EAC Legal Framework.
- **Supplementary Act on Personal Data Protection within ECOWAS 2010**[133] (ECOWAS Supplementary Act): This instrument is designed to be directly transposed into a domestic context, and, in a similar vein to the AU Convention, provides in detail for the conditions for lawful processing of personal information and the rights of data subjects.
- **SADC Data Protection Model Law 2013**[134] (SADC Model Law): This instrument is a model law that can be utilised in a national context by member states. It seeks to ensure the harmonisations of information and communications technologies (ICT) policies, and recognises that ICT developments impact the rights and protection of personal data, including in government and commercial activities. In addition to setting out the conditions for lawful processing of personal information and the rights of data subjects, it also deals with whistle-blowing, providing that the data protection authority must establish rules giving authorisation for and governing the whistleblowing system which preserve the data protection principles, including the principles of fairness, lawfulness, purpose-specification, proportionality and openness.

In addition to giving effect to the right to privacy, data protection laws also typically facilitate a right of access to information. In this regard, most data protection laws provide for data subjects to request, and be given access to, the information being held about them by a controller. This mechanism can enable data subjects to ascertain whether their personal information is being processed in accordance with the applicable data protection laws, and whether their rights are indeed being upheld.

'THE RIGHT TO BE FORGOTTEN'[135]

The so-called 'right to be forgotten' — which is perhaps better described as 'the right to erasure' or 'the right to be de-listed' — entails a right to request that commercial search engines or other websites that gather personal information for profit, such as Google, should remove links to private information when asked. The right to be forgotten progresses from the right of data subjects contained in many data protection laws that personal information held about a person should be erased in circumstances

---

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

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

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

[135] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

where it is inadequate, irrelevant or no longer relevant, or excessive in relation to purposes for which it was collected.

In 2014, the Court of Justice of the European Union (CJEU) handed down an important ruling in the case of *Google Spain v Gonzalez*.[136] Mr Gonzalez, a Spanish national, lodged a complaint in 2010 with the Spanish information regulator. The cause of Mr Gonzalez's complaint was that, when an internet user entered his name into Google's search engine, the user would obtain links to pages of the Spanish newspaper from 1998 referring to attachment proceedings against him for the recovery of certain debts. Mr Gonzalez requested that the personal data relating to him be removed or concealed because the proceedings against him had been fully resolved and the reference to him was therefore now entirely irrelevant.

Before the CJEU, relying to the EU data protection law in effect at the time, the claim was upheld. The CJEU noted that the very display of personal information on a search results page constitutes processing of such information,[137] and there was no reason why a search engine should not be subject to the obligations and guarantees laid out under the law.[138] Further, it was noted that the processing of personal information carried out by a search engine can significantly affect the fundamental rights to privacy and to the protection of personal data when a search is carried out of a person's name, as it enables any internet user to obtain a structured overview of information relating to that individual and establish a profile of the person.[139] According to the CJEU, the effect of the interference "is heightened taking into account the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous."[140]

With regard to de-listing, the CJEU held that the removal of links from the list of results could, depending on the information at issue, have effects on legitimate internet users potentially interested in having access to that information.[141] This would require a fair balance to be struck between that interest and the data subject's fundamental rights, taking into account the nature of the information, its sensitivity for the data subject's private life, and the interest of the public in having that information, which may vary according to the role played by the data subject in public life.[142]

The CJEU went on to hold that a data subject is permitted to request that information about him or her no longer be made available to the general public by its inclusion in

---

[136] *Google Spain SL and Another v Agencia Española de Protección de Datos (AEPD) and Another*, Case No. C-131/12, 13 May 2014 (accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131).

[137] *Id* at para 57.

[138] *Id* at para 58.

[139] *Id* at para 80.

[140] *Id.*

[141] *Id* at para 81.

[142] *Id*.

a list of search results where, having regard to all the circumstances, the information appears to be inadequate, irrelevant or no longer relevant, or excessive in relation to purposes of the processing carried out by the operator of the search engine.[143] In such circumstances, the information and links concerned in the list of results must be erased.[144]

The right to be forgotten has also been recognised in domestic contexts. For instance, Italy's Supreme Court of Cassation has held that the public interest in an article diminished after two and a half years, and that sensitive and private information should not be available to the public indefinitely.[145] The case is currently being litigated before the European Court of Human Rights.[146] The Belgian Court of Cassation has also recognised the right to be forgotten.[147]

There are, however, limits to the ambit of the right to be forgotten. In 2017, the CJEU was seized with a request for a preliminary ruling in the case of *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*.[148] Mr Manni, relying on the *Gonzalez* decision, sought an order requiring the Chamber of Commerce to erase, anonymise or block any data linking him to the liquidation of his company contained in the companies register. The CJEU declined to uphold Mr Manni's request, and held that in light of the range of possible legitimate uses for data in companies registers and the different limitation periods applicable to such records, it was impossible to identify a suitable maximum retention period. Accordingly, the CJEU declined to find that there is a general right to be forgotten from public company registers.

Furthermore, other jurisdictions have refused to uphold a right to be forgotten against search engines. In Brazil, for example, it was held that search engines cannot be compelled to remove search results relating to a specific term or expression;[149]

---

[143] *Id*. at para 94.

[144] *Id*. at para 94.

[145] *Plaintiff X v PrimaDaNoi*, Case No. 13161, 22 November 2015 (accessible at: https://globalfreedomofexpression.columbia.edu/cases/plaintiff-x-v-primadanoi/).

[146] European Court of Human Rights, Application no. 77419/16 (2020) (accessible at: https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-201483%22%5D%7D).

[147] *P.H. v O.G.*, Case No. 15/0052/F, 29 April 2016 (accessible at: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/06/download_blob.pdf). For a discussion of the case, see Hunton & Williams, 'Belgian Court of Cassation rules on right to be forgotten', 1 June 2016 (accessible at: https://www.huntonprivacyblog.com/2016/06/01/belgian-court-of-cassation-rules-on-right-to-be-forgotten/).

For more on the right to be forgotten, see *NT1 & NT2 v Google LLC* in the UK (2018) (accessible at: https://www.judiciary.uk/wp-content/uploads/2018/04/nt1-nt2-v-google-press-summary-180413.pdf).

[148] Case No. C-385-15, 9 March 2017 (accessible at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=446798).

[149] *Ministra Nancy Andrighi v Google Brasil Internet Ltd and Others*, 2011/0307909-6, 26 June 2012 (accessible at: https://www.internetlab.org.br/wp-content/uploads/2017/02/STJ-REsp-1316921.pdf).

similarly, the Supreme Court of Japan declined to enforce the right to be forgotten against Google, finding that deletion "can be allowed only when the value of privacy protection significantly outweighs that of information disclosure".[150]

According to the Global Principles of Freedom of Expression and Privacy (Global Principles),[151] the right — to the extent that it is recognised in a particular jurisdiction — should be limited to the right of individuals under data protection law to request search engines to delist inaccurate or out-of-date search results produced on the basis of a search for their name,[152] and should be limited in scope to the domain name corresponding to the country where the right is recognised and the individual has established substantial damage.[153] It states further that de-listing requests should be subject to ultimate adjudication by a court or independent adjudicatory body with relevant expertise in freedom of expression and data protection law.[154]

[150] The Japan Times, 'Top court rejects 'right to be forgotten' demand', 1 February 2017 (accessible at: https://www.japantimes.co.jp/news/2017/02/01/national/crime-legal/top-court-rejects-right-forgotten-demand/#.WqZQXehubIV).

[151] The Global Principles (accessible at: https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf) were developed by civil society, led by ARTICLE19, in cooperation with high-level experts from around the world.

[152] Principle 18(1) of the Global Principles.

[153] *Id* at principle 18(4).

[154] *Id* at principle 18(2).

ENCRYPTION AND ANONYMITY ON THE INTERNET[155]

Encryption refers to a mathematical process of converting messages, information or data into a form unreadable by anyone except the intended recipient, and in doing so protecting the confidentiality and integrity of content against third party access or manipulation.[156] With a "public key encryption" — the dominant form of end-to-end security for data in transit — the sender uses the recipient's public key to encrypt the message and its attachments, and the recipient uses her or his own private key to decrypt them.[157] It is also possible to encrypt data at rest that is stored on one's device, such as a laptop or hard drive.[158]

Anonymity can be defined either as acting or communicating without using or presenting one's name or identity, or as acting or communicating in a way that protects the determination of one's name or identity, or using an invented or assumed name that may not necessarily be associated with one's legal or customary identity.[159] Anonymity may be distinguished from pseudo-anonymity: the former refers to taking no name at all, whilst the latter refers to taking an assumed name.[160]

Encryption and anonymity are necessary tools for the full enjoyment of digital rights, and enjoy protection by virtue of the critical role that they play in securing the rights to freedom of expression and privacy. As described by the United Nations Special Rapporteur (UNSR) on freedom of expression:[161]

> "Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities.

---

[155] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

[156] Report of the UNSR on Freedom of Expression, 'Report on anonymity, encryption and the human rights framework', A/HRC/29/32, 22 May 2015 (UNSR Report on Anonymity and Encryption) at para 7 (accessible at: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx). For further discussion and resources, see UCI Law International Justice Clinic, 'Selected references: Unofficial companion report to Report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and freedom of expression' (accessible at: http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/Selected_References_SR_Report.pdf).

[157] *Id*.

[158] *Id*.

[159] Electronic Frontier Foundation, *Anonymity and encryption*, 10 February 2015 at p 3 (accessible at: https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf).

[160] *Id*.

[161] UNSR Report on Anonymity and Encryption above n 30 at para 12.

> Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression."

Encryption and anonymity are especially useful for the development and sharing of opinions online, particularly in circumstances where persons may be concerned that their communications may be subject to interference or attack by state or non-state actors. These are therefore specific technologies through which individuals may exercise their rights. Accordingly, restrictions on encryption and anonymity must meet the three-part test to justify the restriction.

According to the UNSR on freedom of expression, while encryption and anonymity may frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public justification to support the restriction or to identify situations where the restriction has been necessary to achieve a legitimate goal.[162] Outright prohibitions on the individual use of encryption technology disproportionately restricts the right to freedom of expression as it deprives all online users in a particular jurisdiction of the right to carve out a space for opinion and expression, without any particular claim of the use of encryption being for unlawful ends.[163] Likewise, state regulation of encryption may be tantamount to a ban, for example through requiring licences for encryption use, setting weak technical standards for encryption or controlling the import and export of encryption tools.[164]

The UNSR on freedom of expression has called on states to promote strong encryption and anonymity, and noted that decryption orders should only be permissible when it results from transparent and publicly-accessible laws applied solely on a targeted, case-by-case basis to individuals (not to a mass of people), and subject to a judicial warrant and the protection of due process rights of individuals.[165]

GOVERNMENT-LED DIGITAL SURVEILLANCE[166]

[162] *Id*. at para 36.

[163] *Id.* at para 40.

[164] *Id.* at para 41.

[165] *Id*. at paras 59-60.

[166] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

Communications surveillance encompasses the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future.[167] This relates to both the content of communications and metadata. In respect of the latter, it has been noted that the aggregation of information — commonly referred to as 'metadata' — may give an insight into an individual's behaviour, social relationships, private preferences and identity. Taken as a whole, it may allow very precise conclusions to be drawn concerning the private life of the person.

General Comment No. 16 provides that "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited".[168] Surveillance — both bulk (or mass) collection of data[169] or targeted collection of data — interferes directly with the privacy and security necessary for freedom of opinion and expression, and must be considered against the three-part test to assess the permissibility of the restriction.[170] In the digital age, ICTs have enhanced the capacity of governments, corporations and individuals to conduct surveillance, interception and data collection, and have meant that the effectiveness in conducting such surveillance is no longer limited by scale or duration.[171]

In a resolution adopted by the UN General Assembly (UNGA) on the right to privacy in the digital age, the UNGA emphasised that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data are highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and may contradict the tenets of a democratic society, including when undertaken on a mass scale.[172] It noted further that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory.[173]

---

[167] Necessary and proportionate: International principles on the application of human rights to communications surveillance, 2014 (Necessary and Proportionate Principles) at p 4 (accessible at: https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf).

[168] General Comment No. 16 at para 8.

[169] Revelations be whistle-blowers, such as Edward Snowden, have revealed that the National Security Agency in the USA and the General Communications Headquarters in the United Kingdom had developed technologies allowing access to much global internet traffic, calling records in the United States, individuals' electronic address books and huge volumes of other digital communications content. These technologies are deployed through a transnational network comprising strategic intelligence relationships between governments and other role-players. This is referred to as bulk or mass surveillance. See 2016 Report of the OHCHR at para 4.

[170] 2016 Report of the UNSR on Freedom of Expression at para 20.

[171] Report of the OHCHR at para 2.

[172] UNGA, 'Resolution on the right to privacy in the digital age', A/C.3/71/L.39/Rev.1, 16 November 2016 (2016 UN Resolution on Privacy) (accessible at: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1).

[173] *Id*.

In order to meet the condition of legality, many states have taken steps to reform their surveillance laws to allow for the powers required to conduct the surveillance activities. According to the Necessity and Proportionate Principles, communications surveillance should be regarded as a highly intrusive act, and in order to meet the threshold of proportionality, the state should be required at a minimum to establish the following information to a competent judicial authority prior to conducting any communications surveillance:[174]

- There is a high degree of probability that a serious crime or specific threat to a legitimate aim has been or will be carried out.
- There is a high degree of probability that evidence relevant and material to such a serious crime or specific threat to a legitimate aim would be obtained by accessing the protected information sought.
- Other less invasive techniques have been exhausted or would be futile, such that the technique used is the least invasive option.
- Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a legitimate aim alleged.
- Any excess information collected will not be retained, but instead will be promptly destroyed or returned.
- Information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.
- The surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

Surveillance constitutes an obvious interference with the right to privacy. Further, it also constitutes an interference on the right to hold opinions without interference and the right to freedom of expression. With particular reference to the right to hold opinions without interference, surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes.[175]

The interference with the right to freedom of expression is particularly apparent in the context of journalists and members of the media who may be placed under surveillance as a result of their journalistic activities. As noted by the Secretary-General of the UN, this can have a chilling effect on the enjoyment of media freedom, and renders it more difficult to communicate with sources and share and develop ideas, which may lead to self-censorship.[176] The use of encryption and other similar

[174] Above at n 43, Principle 5.

[175] UNSR Report on Anonymity and Encryption at para 21.

[176] Report of the Secretary-General on the UN to the UNGA, 'Report on the safety of journalists and the issue of impunity', A/70/290, 6 August 2015 (2015 Report of the UN Secretary-General) at paras 14-16 (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/247/06/PDF/N1524706.pdf?OpenElement).

tools have become essential to the work of journalists to ensure that they are able to conduct their work without interference.

The disclosure of journalistic sources and surveillance can have negative consequences for the right to freedom of expression due to a breach of an individual's confidentiality in their communications.[177] This is the same for cases concerning the disclosure of anonymous user data. Once confidentiality is undermined, it cannot be restored. It is, therefore, of utmost importance that measures that undermine confidentiality are not taken arbitrarily.

The importance of source protection has been well-established. For example, in *Bosasa Operation (Pty) Ltd v Basson and Another*, the South Africa High Court held that journalists are not required to reveal their sources, subject to certain exceptions.[178] The court stated in this regard that:

> "If indeed freedom of the press is fundamental and *sine qua non* for democracy, it is essential that in carrying out this public duty for the public good, the identity of their sources should not be revealed, particularly, when the information so revealed, would not have been publicly known. This essential and critical role of the media, which is more pronounced in our nascent democracy, founded on openness, where corruption has become cancerous, needs to be fostered rather than denuded."[179]

Surveillance activities carried out against journalists have the risk of fundamentally undermining the source protection to which journalists are otherwise entitled.[180]

CONCLUSION

[177] For more, see *Big Brother Watch v United Kingdom* in the ECtHR (2018) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/) and *amaBhungane Centre for Investigative Journalism v Minister of Justice* in South Africa (2019) (accessible at: http://www.saflii.org/za/cases/ZAGPPHC/2019/384.html).

[178] [2012] ZAGPJHC 71, 26 April 2012 (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2012/71.html).

[179] *Id*. at para 38.

[180] According to principle 9 of the Global Principles, states should provide for the protection of the confidentiality of sources in their legislation and ensure that:

- Any restriction on the right to protection of sources complies with the three-part test under international human rights law.
- The confidentiality of sources should only be lifted in exceptional circumstances and only by a court order, which complies with the requirements of a legitimate aim, necessity, and proportionality. The same protections should apply to access to journalistic material.
- The right not to disclose the identity of sources and the protection of journalistic material requires that the privacy and security of the communications of anyone engaged in journalistic activity, including access to their communications data and metadata, must be protected. Circumventions, such as secret surveillance or analysis of communications data not authorised by judicial authorities according to clear and narrow legal rules, must not be used to undermine source confidentiality.
- Any court order must only be granted after a fair hearing where sufficient notice has been given to the journalist in question, except in genuine emergencies.

As more of the world moves online, data protection is becoming increasingly necessary. In an African context, some headway has been made with 21 African states having privacy laws in place. However, with the rapid growth in data harvesting, legislators are some way behind in fully protecting and promoting data privacy and data protection. As we move forward, digital rights activists have a significant role to play in ensuring that states keep step with data protection developments and enact legislative frameworks that fully protect and promote peoples' rights to privacy.

Module 4

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

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 4

DATA PRIVACY AND DATA PROTECTION

- **The right to privacy is gaining prominence with increasing data flows and the concomitant need for the protection of personal information.**
- **In the African context, there are multiple instruments, including the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention), which govern data protection.**
- **Importantly, states should ensure that their domestic legislation details principles for the lawful processing of personal information and that they keep step with data protection developments.**
- **Allied to data protection are the concepts of the 'right to be forgotten', encryption and government-led surveillance.**
- **Notably, the disclosure of journalistic sources as a result of state surveillance has a negative impact on freedom of expression and journalistic freedom.**

INTRODUCTION

The right to privacy and the concomitant requirement to protect personal information has garnered significant attention with the dawn of the information age. While the internet and online information-sharing and data collection increase at an exponential rate, legislative developments have failed to keep pace and adequately protect personal information. However, with time, African states and regional and continental bodies have begun to adopt data protection-related instruments and regulations in an attempt to remedy and vindicate the privacy rights of their citizens.

This module focuses on data protection in Africa and the related concepts of the 'right to be forgotten', encryption and surveillance.

THE RIGHT TO PRIVACY

There is an increasing recognition that the right to privacy plays a vital role in and of itself and in facilitating the right to freedom of expression. For instance, reliance on the right to privacy allows individuals to share views anonymously in circumstances where they may fear being censured for those views, it allows whistle-blowers to make protected disclosures, and it enables members of the media and activists to communicate securely beyond the reach of unlawful government interception.

The right to privacy is contained in article 17 of the International Covenant on Civil and Political Rights (ICCPR), which provides:

> "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> (2) Everyone has the right to the protection of the law against such interference or attacks."

Although not contained in the African Charter on Human and Peoples' Rights (ACHPR), the right to privacy of children is contained in article 10 of the African Charter on the Rights and Welfare of the Child (ACRWC), which provides that:

> "No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks."

The right to privacy has also been recognised in other regional and sub-regional instruments in the context of data protection, which is discussed further below. Moreover, almost all African states guarantee this right under their domestic constitutions.[181]

Interestingly, in 2017, the Supreme Court of India declared that the right to privacy is protected as an intrinsic part of the right to life and personal liberty, and as part of the fundamental freedoms guaranteed by Part III of the Constitution of India.[182] As such, although the Constitution of India does not expressly contain a right to privacy, the right can nevertheless be read when considered in the context of the other rights and freedoms that are constitutionally guaranteed. Although this has not been tested in the context of the ACHPR, there is arguably scope to read the right to privacy into other provisions of the African Charter.

As with the right to freedom of expression, a limitation of the right to privacy must comply with the three-part test for a justifiable limitation. According to the South African Constitutional Court:[183]

---

[181] At the domestic level, more than 50 African constitutions, inclusive of amendments and recent reviews, include reference to the right to privacy. Singh and Power, 'The privacy awakening: The urgent need to harmonise the right to privacy in Africa' African Human Rights Yearbook 3 (2019) 202 at p 202, http://www.pulp.up.ac.za/images/pulp/books/journals/AHRY_2019/Power%202019.pdf.

[182] *Justice K.S. Puttaswamy and Another v Union of India and Others*, Petition No. 494/2012, 24 August 2017 (accessible at: http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf).

[183] *NM and Others v Smith and Others*, [2007] ZACC 6, 4 April 2007 at para 33 (accessible at: https://www.saflii.org/za/cases/ZACC/2007/6.html), citing with approval *Bernstein and Others v Bester NNO and Others*, [1996] ZACC 2, 27 March 1996 at para 77.

> "A very high level of protection is given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual's activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation."

Set out below, we consider specific aspects of the right to privacy and the impact that the internet has had on the enjoyment of this right.

DATA PROTECTION

Data protection laws are aimed at protecting and safeguarding the processing of personal information (or personal data). This refers to any information relating to an identified or identifiable natural person — i.e. the data subject — by which the data subject can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. A data controller, which can typically be either a public or private body, refers to the person or entity responsible for processing the personal information about the data subject.

Data protection is one of the primary measures through which the right to privacy is given effect. There have already been a number of African states that have enacted data protection laws, and more that are in the process of doing so.[184] In addition to giving effect to the right to privacy, data protection legislation also has a key role to play in facilitating trade amongst states, as many data protection laws restrict cross-border data transfers in circumstances where the state receiving the information does not provide an adequate level of data protection.

In relation to data protection of personal information, General Comment No. 16 on article 17 of the ICCPR (General Comment No. 16) provides as follows:[185]

> "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not

[184] At present, there are 21 states in the African Union (AU) that have enacted comprehensive privacy laws: Angola, Benin, Burkina Faso, Cape Verde, Chad, Côte d'Ivoire, Equatorial Guinea, Egypt, Gabon, Ghana, Kenya, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Togolese Republic and Tunisia. There are a further four states that have shown indications of being close to adopting legislation: Niger, Tanzania, Uganda and Zimbabwe. See https://dataprotection.africa/ for more information.

[185] General Comment No. 16 at para 10.

> authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."

Most comprehensive data protection laws typically make provision for the following principles:[186]

- Personal information must be processed fairly and lawfully, and must not be processed unless the stipulated conditions are met.
- Personal information must be obtained for a specified purpose (or purposes), and must not be further processed in any manner incompatible with that purpose.
- Personal data must be adequate, relevant and not excessive in relation to the purpose (or purposes) for which it is processed.
- Personal information must be accurate and, where necessary, kept up to date.
- Personal information must not be kept for longer than is necessary for the purpose of collection.
- Personal information must be processed in accordance with the rights of data subjects provided for under the data protection law.
- Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to another country that does not ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

There are a number of African regional instruments that deal with data protection:

- **AU Convention on Cyber Security and Personal Data Protection 2014**[187] (AU Convention or "Malabo Convention"): This instrument, aimed at a continental level, includes provisions relating to data protection, e-transactions, cybercrimes and cybersecurity. The provisions relating to data protection are contained in Chapter II, and contain the conditions for the lawful processing of personal information, as well as the rights afforded to data subjects. Although it has not entered into force as yet, it may potentially in future be a binding legal instrument on data protection in Africa.

---

[186] Information Commissioner's Office, 'Data protection principles' (accessible at: https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/).

[187] Accessible at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. At present, it has been ratified by one state, and signed by a further ten states.

- **Draft EAC Legal Framework for Cyberlaws 2008**[188] (EAC Legal Framework): This instrument covers topics relating to data protection, electronic commerce, data security and consumer protection. It is not intended to be a model law but instead provides guidance and recommendations to states to assist with informing the development of their laws. Data protection is dealt with briefly at paragraph 2.5 of the EAC Legal Framework.
- **Supplementary Act on Personal Data Protection within ECOWAS 2010**[189] (ECOWAS Supplementary Act): This instrument is designed to be directly transposed into a domestic context, and, in a similar vein to the AU Convention, provides in detail for the conditions for lawful processing of personal information and the rights of data subjects.
- **SADC Data Protection Model Law 2013**[190] (SADC Model Law): This instrument is a model law that can be utilised in a national context by member states. It seeks to ensure the harmonisations of information and communications technologies (ICT) policies, and recognises that ICT developments impact the rights and protection of personal data, including in government and commercial activities. In addition to setting out the conditions for lawful processing of personal information and the rights of data subjects, it also deals with whistle-blowing, providing that the data protection authority must establish rules giving authorisation for and governing the whistleblowing system which preserve the data protection principles, including the principles of fairness, lawfulness, purpose-specification, proportionality and openness.

In addition to giving effect to the right to privacy, data protection laws also typically facilitate a right of access to information. In this regard, most data protection laws provide for data subjects to request, and be given access to, the information being held about them by a controller. This mechanism can enable data subjects to ascertain whether their personal information is being processed in accordance with the applicable data protection laws, and whether their rights are indeed being upheld.

'THE RIGHT TO BE FORGOTTEN'[191]

The so-called 'right to be forgotten' — which is perhaps better described as 'the right to erasure' or 'the right to be de-listed' — entails a right to request that commercial search engines or other websites that gather personal information for profit, such as Google, should remove links to private information when asked. The right to be forgotten progresses from the right of data subjects contained in many data protection laws that personal information held about a person should be erased in circumstances

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

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

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

[191] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

where it is inadequate, irrelevant or no longer relevant, or excessive in relation to purposes for which it was collected.

In 2014, the Court of Justice of the European Union (CJEU) handed down an important ruling in the case of *Google Spain v Gonzalez*.[192] Mr Gonzalez, a Spanish national, lodged a complaint in 2010 with the Spanish information regulator. The cause of Mr Gonzalez's complaint was that, when an internet user entered his name into Google's search engine, the user would obtain links to pages of the Spanish newspaper from 1998 referring to attachment proceedings against him for the recovery of certain debts. Mr Gonzalez requested that the personal data relating to him be removed or concealed because the proceedings against him had been fully resolved and the reference to him was therefore now entirely irrelevant.

Before the CJEU, relying to the EU data protection law in effect at the time, the claim was upheld. The CJEU noted that the very display of personal information on a search results page constitutes processing of such information,[193] and there was no reason why a search engine should not be subject to the obligations and guarantees laid out under the law.[194] Further, it was noted that the processing of personal information carried out by a search engine can significantly affect the fundamental rights to privacy and to the protection of personal data when a search is carried out of a person's name, as it enables any internet user to obtain a structured overview of information relating to that individual and establish a profile of the person.[195] According to the CJEU, the effect of the interference "is heightened taking into account the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous."[196]

With regard to de-listing, the CJEU held that the removal of links from the list of results could, depending on the information at issue, have effects on legitimate internet users potentially interested in having access to that information.[197] This would require a fair balance to be struck between that interest and the data subject's fundamental rights, taking into account the nature of the information, its sensitivity for the data subject's private life, and the interest of the public in having that information, which may vary according to the role played by the data subject in public life.[198]

The CJEU went on to hold that a data subject is permitted to request that information about him or her no longer be made available to the general public by its inclusion in

---

[192] *Google Spain SL and Another v Agencia Española de Protección de Datos (AEPD) and Another*, Case No. C-131/12, 13 May 2014 (accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131).

[193] *Id* at para 57.

[194] *Id* at para 58.

[195] *Id* at para 80.

[196] *Id.*

[197] *Id* at para 81.

[198] *Id*.

a list of search results where, having regard to all the circumstances, the information appears to be inadequate, irrelevant or no longer relevant, or excessive in relation to purposes of the processing carried out by the operator of the search engine.[199] In such circumstances, the information and links concerned in the list of results must be erased.[200]

The right to be forgotten has also been recognised in domestic contexts. For instance, Italy's Supreme Court of Cassation has held that the public interest in an article diminished after two and a half years, and that sensitive and private information should not be available to the public indefinitely.[201] The case is currently being litigated before the European Court of Human Rights.[202] The Belgian Court of Cassation has also recognised the right to be forgotten.[203]

There are, however, limits to the ambit of the right to be forgotten. In 2017, the CJEU was seized with a request for a preliminary ruling in the case of *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*.[204] Mr Manni, relying on the *Gonzalez* decision, sought an order requiring the Chamber of Commerce to erase, anonymise or block any data linking him to the liquidation of his company contained in the companies register. The CJEU declined to uphold Mr Manni's request, and held that in light of the range of possible legitimate uses for data in companies registers and the different limitation periods applicable to such records, it was impossible to identify a suitable maximum retention period. Accordingly, the CJEU declined to find that there is a general right to be forgotten from public company registers.

Furthermore, other jurisdictions have refused to uphold a right to be forgotten against search engines. In Brazil, for example, it was held that search engines cannot be compelled to remove search results relating to a specific term or expression;[205]

---

[199] *Id*. at para 94.

[200] *Id*. at para 94.

[201] *Plaintiff X v PrimaDaNoi*, Case No. 13161, 22 November 2015 (accessible at: https://globalfreedomofexpression.columbia.edu/cases/plaintiff-x-v-primadanoi/).

[202] European Court of Human Rights, Application no. 77419/16 (2020) (accessible at: https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-201483%22%5D%7D).

[203] *P.H. v O.G.*, Case No. 15/0052/F, 29 April 2016 (accessible at: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/06/download_blob.pdf). For a discussion of the case, see Hunton & Williams, 'Belgian Court of Cassation rules on right to be forgotten', 1 June 2016 (accessible at: https://www.huntonprivacyblog.com/2016/06/01/belgian-court-of-cassation-rules-on-right-to-be-forgotten/).

For more on the right to be forgotten, see *NT1 & NT2 v Google LLC* in the UK (2018) (accessible at: https://www.judiciary.uk/wp-content/uploads/2018/04/nt1-nt2-v-google-press-summary-180413.pdf).

[204] Case No. C-385-15, 9 March 2017 (accessible at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=446798).

[205] *Ministra Nancy Andrighi v Google Brasil Internet Ltd and Others*, 2011/0307909-6, 26 June 2012 (accessible at: https://www.internetlab.org.br/wp-content/uploads/2017/02/STJ-REsp-1316921.pdf).

similarly, the Supreme Court of Japan declined to enforce the right to be forgotten against Google, finding that deletion "can be allowed only when the value of privacy protection significantly outweighs that of information disclosure".[206]

According to the Global Principles of Freedom of Expression and Privacy (Global Principles),[207] the right — to the extent that it is recognised in a particular jurisdiction — should be limited to the right of individuals under data protection law to request search engines to delist inaccurate or out-of-date search results produced on the basis of a search for their name,[208] and should be limited in scope to the domain name corresponding to the country where the right is recognised and the individual has established substantial damage.[209] It states further that de-listing requests should be subject to ultimate adjudication by a court or independent adjudicatory body with relevant expertise in freedom of expression and data protection law.[210]

ENCRYPTION AND ANONYMITY ON THE INTERNET[211]

Encryption refers to a mathematical process of converting messages, information or data into a form unreadable by anyone except the intended recipient, and in doing so protecting the confidentiality and integrity of content against third party access or manipulation.[212] With a "public key encryption" — the dominant form of end-to-end security for data in transit — the sender uses the recipient's public key to encrypt the message and its attachments, and the recipient uses her or his own private key to

[206] The Japan Times, 'Top court rejects 'right to be forgotten' demand', 1 February 2017 (accessible at: https://www.japantimes.co.jp/news/2017/02/01/national/crime-legal/top-court-rejects-right-forgotten-demand/#.WqZQXehubIV).

[207] The Global Principles (accessible at: https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf) were developed by civil society, led by ARTICLE19, in cooperation with high-level experts from around the world.

[208] Principle 18(1) of the Global Principles.

[209] *Id* at principle 18(4).

[210] *Id* at principle 18(2).

[211] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

[212] Report of the UNSR on Freedom of Expression, 'Report on anonymity, encryption and the human rights framework', A/HRC/29/32, 22 May 2015 (UNSR Report on Anonymity and Encryption) at para 7 (accessible at: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx). For further discussion and resources, see UCI Law International Justice Clinic, 'Selected references: Unofficial companion report to Report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and freedom of expression' (accessible at: http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/Selected_References_SR_Report.pdf).

decrypt them.[213] It is also possible to encrypt data at rest that is stored on one's device, such as a laptop or hard drive.[214]

Anonymity can be defined either as acting or communicating without using or presenting one's name or identity, or as acting or communicating in a way that protects the determination of one's name or identity, or using an invented or assumed name that may not necessarily be associated with one's legal or customary identity.[215] Anonymity may be distinguished from pseudo-anonymity: the former refers to taking no name at all, whilst the latter refers to taking an assumed name.[216]

Encryption and anonymity are necessary tools for the full enjoyment of digital rights, and enjoy protection by virtue of the critical role that they play in securing the rights to freedom of expression and privacy. As described by the United Nations Special Rapporteur (UNSR) on freedom of expression:[217]

> "Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression."

Encryption and anonymity are especially useful for the development and sharing of opinions online, particularly in circumstances where persons may be concerned that their communications may be subject to interference or attack by state or non-state actors. These are therefore specific technologies through which individuals may exercise their rights. Accordingly, restrictions on encryption and anonymity must meet the three-part test to justify the restriction.

According to the UNSR on freedom of expression, while encryption and anonymity may frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public

---

[213] *Id*.

[214] *Id*.

[215] Electronic Frontier Foundation, *Anonymity and encryption*, 10 February 2015 at p 3 (accessible at: https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf).

[216] *Id*.

[217] UNSR Report on Anonymity and Encryption above n 30 at para 12.

justification to support the restriction or to identify situations where the restriction has been necessary to achieve a legitimate goal.[218] Outright prohibitions on the individual use of encryption technology disproportionately restricts the right to freedom of expression as it deprives all online users in a particular jurisdiction of the right to carve out a space for opinion and expression, without any particular claim of the use of encryption being for unlawful ends.[219] Likewise, state regulation of encryption may be tantamount to a ban, for example through requiring licences for encryption use, setting weak technical standards for encryption or controlling the import and export of encryption tools.[220]

The UNSR on freedom of expression has called on states to promote strong encryption and anonymity, and noted that decryption orders should only be permissible when it results from transparent and publicly-accessible laws applied solely on a targeted, case-by-case basis to individuals (not to a mass of people), and subject to a judicial warrant and the protection of due process rights of individuals.[221]

GOVERNMENT-LED DIGITAL SURVEILLANCE[222]

Communications surveillance encompasses the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future.[223] This relates to both the content of communications and metadata. In respect of the latter, it has been noted that the aggregation of information — commonly referred to as 'metadata' — may give an insight into an individual's behaviour, social relationships, private preferences and identity. Taken as a whole, it may allow very precise conclusions to be drawn concerning the private life of the person.

General Comment No. 16 provides that "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited".[224] Surveillance — both bulk (or mass) collection of data[225] or targeted collection of data — interferes

---

[218] *Id*. at para 36.

[219] *Id.* at para 40.

[220] *Id.* at para 41.

[221] *Id*. at paras 59-60.

[222] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

[223] Necessary and proportionate: International principles on the application of human rights to communications surveillance, 2014 (Necessary and Proportionate Principles) at p 4 (accessible at: https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf).

[224] General Comment No. 16 at para 8.

[225] Revelations be whistle-blowers, such as Edward Snowden, have revealed that the National Security Agency in the USA and the General Communications Headquarters in the United Kingdom had developed technologies allowing access to much global internet traffic, calling records in the

directly with the privacy and security necessary for freedom of opinion and expression, and must be considered against the three-part test to assess the permissibility of the restriction.[226] In the digital age, ICTs have enhanced the capacity of governments, corporations and individuals to conduct surveillance, interception and data collection, and have meant that the effectiveness in conducting such surveillance is no longer limited by scale or duration.[227]

In a resolution adopted by the UN General Assembly (UNGA) on the right to privacy in the digital age, the UNGA emphasised that unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data are highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and may contradict the tenets of a democratic society, including when undertaken on a mass scale.[228] It noted further that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory.[229]

In order to meet the condition of legality, many states have taken steps to reform their surveillance laws to allow for the powers required to conduct the surveillance activities. According to the Necessity and Proportionate Principles, communications surveillance should be regarded as a highly intrusive act, and in order to meet the threshold of proportionality, the state should be required at a minimum to establish the following information to a competent judicial authority prior to conducting any communications surveillance:[230]

- There is a high degree of probability that a serious crime or specific threat to a legitimate aim has been or will be carried out.
- There is a high degree of probability that evidence relevant and material to such a serious crime or specific threat to a legitimate aim would be obtained by accessing the protected information sought.
- Other less invasive techniques have been exhausted or would be futile, such that the technique used is the least invasive option.
- Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a legitimate aim alleged.

United States, individuals' electronic address books and huge volumes of other digital communications content. These technologies are deployed through a transnational network comprising strategic intelligence relationships between governments and other role-players. This is referred to as bulk or mass surveillance. See 2016 Report of the OHCHR at para 4.

[226] 2016 Report of the UNSR on Freedom of Expression at para 20.

[227] Report of the OHCHR at para 2.

[228] UNGA, 'Resolution on the right to privacy in the digital age', A/C.3/71/L.39/Rev.1, 16 November 2016 (2016 UN Resolution on Privacy) (accessible at: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1).

[229] *Id*.

[230] Above at n 43, Principle 5.

- Any excess information collected will not be retained, but instead will be promptly destroyed or returned.
- Information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.
- The surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

Surveillance constitutes an obvious interference with the right to privacy. Further, it also constitutes an interference on the right to hold opinions without interference and the right to freedom of expression. With particular reference to the right to hold opinions without interference, surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes.[231]

The interference with the right to freedom of expression is particularly apparent in the context of journalists and members of the media who may be placed under surveillance as a result of their journalistic activities. As noted by the Secretary-General of the UN, this can have a chilling effect on the enjoyment of media freedom, and renders it more difficult to communicate with sources and share and develop ideas, which may lead to self-censorship.[232] The use of encryption and other similar tools have become essential to the work of journalists to ensure that they are able to conduct their work without interference.

The disclosure of journalistic sources and surveillance can have negative consequences for the right to freedom of expression due to a breach of an individual's confidentiality in their communications.[233] This is the same for cases concerning the disclosure of anonymous user data. Once confidentiality is undermined, it cannot be restored. It is, therefore, of utmost importance that measures that undermine confidentiality are not taken arbitrarily.

The importance of source protection has been well-established. For example, in *Bosasa Operation (Pty) Ltd v Basson and Another*, the South Africa High Court held that journalists are not required to reveal their sources, subject to certain exceptions.[234] The court stated in this regard that:

---

[231] UNSR Report on Anonymity and Encryption at para 21.

[232] Report of the Secretary-General on the UN to the UNGA, 'Report on the safety of journalists and the issue of impunity', A/70/290, 6 August 2015 (2015 Report of the UN Secretary-General) at paras 14-16 (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/247/06/PDF/N1524706.pdf?OpenElement).

[233] For more, see *Big Brother Watch v United Kingdom* in the ECtHR (2018) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/) and *amaBhungane Centre for Investigative Journalism v Minister of Justice* in South Africa (2019) (accessible at: http://www.saflii.org/za/cases/ZAGPPHC/2019/384.html).

[234] [2012] ZAGPJHC 71, 26 April 2012 (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2012/71.html).

> "If indeed freedom of the press is fundamental and *sine qua non* for democracy, it is essential that in carrying out this public duty for the public good, the identity of their sources should not be revealed, particularly, when the information so revealed, would not have been publicly known. This essential and critical role of the media, which is more pronounced in our nascent democracy, founded on openness, where corruption has become cancerous, needs to be fostered rather than denuded."[235]

Surveillance activities carried out against journalists have the risk of fundamentally undermining the source protection to which journalists are otherwise entitled.[236]

CONCLUSION

As more of the world moves online, data protection is becoming increasingly necessary. In an African context, some headway has been made with 21 African states having privacy laws in place. However, with the rapid growth in data harvesting, legislators are some way behind in fully protecting and promoting data privacy and data protection. As we move forward, digital rights activists have a significant role to play in ensuring that states keep step with data protection developments and enact legislative frameworks that fully protect and promote peoples' rights to privacy.

---

[235] *Id*. at para 38.

[236] According to principle 9 of the Global Principles, states should provide for the protection of the confidentiality of sources in their legislation and ensure that:

- Any restriction on the right to protection of sources complies with the three-part test under international human rights law.
- The confidentiality of sources should only be lifted in exceptional circumstances and only by a court order, which complies with the requirements of a legitimate aim, necessity, and proportionality. The same protections should apply to access to journalistic material.
- The right not to disclose the identity of sources and the protection of journalistic material requires that the privacy and security of the communications of anyone engaged in journalistic activity, including access to their communications data and metadata, must be protected. Circumventions, such as secret surveillance or analysis of communications data not authorised by judicial authorities according to clear and narrow legal rules, must not be used to undermine source confidentiality.
- Any court order must only be granted after a fair hearing where sufficient notice has been given to the journalist in question, except in genuine emergencies.

Module 5

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

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 5

DEFAMATION

- **Defamation is frequently used to unjustly stifle dissent. However, it can provide a genuine remedy for those harmed by the statements or actions of others.**
- **Criminal defamation is generally considered to be disproportionate in terms of international law. Even civil defamation is often punished too harshly rather than righting the wrong that was committed.**
- **Truth is a core defence against defamation claims.**
- **Some types of speech are excluded from defamation laws, such as opinion and satire.**
- **The growth of SLAPP[237] suits by corporate actors using defamation laws to silence or intimidate is a concerning contemporary development that needs to be challenged.**

INTRODUCTION

Defamation is a notorious method of stifling freedom of expression and dissent, particularly of journalists. While defamation laws aim to provide individuals with a remedy for public statements that may harm their reputation or honour, they frequently come into conflict with the right to freedom of expression, which is enshrined in a number of international law instruments and national laws. Balancing the protection of fundamental rights with protecting individuals from harmful statements is central to the appropriateness or otherwise of defamation claims.

The impact of the internet, and particularly social media networks, has meant that it is easier than ever to publish content to a wide audience. As a result, defamation has become a commonly used defence against statements published online, whether justifiably so or not.

The ability to freely post information on social media and the internet without the same degree of thought and review as traditional media, combined with a lack of awareness about defamation laws and the fact that many countries lack clear legislative frameworks dealing with defamation in the online space has led to an increase in online defamation cases and some ambiguity in how defamation applies in the online sphere.[238]

---

[237] Strategic Lawsuits Against Public Participation, see page 10.
[238] SAFLII Speculum Juris, 'An Analytical Look Into the Concept of Online Defamation in South Africa.' Desan Iyer, (2018) (accessible at: http://www.saflii.org/za/journals/SPECJU/2018/10.pdf).

Dealing with online defamation cases is particularly challenging for many reasons.[239] "The internet is not an easily identifiable body that is administered or regulated within the confines of strict internationally recognised parameters or boundaries."[240] The online environment can make it more difficult to identify or trace perpetrators, and victims may want to consider whether to pursue the perpetrator or the system operator, since some legal systems consider anyone who participates in distributing defamatory material equally liable.[241] In addition, deciding the jurisdiction of the court to hear the matter can be difficult as messages can be posted from all over the world, and the parties to a dispute may come from and be located in different jurisdictions, or the message may have been posted somewhere else entirely.

This module provides an overview of defamation laws in Africa, and how the courts have attempted to find the balance between various rights in recent jurisprudence, particularly in dealing with online defamation cases.

WHAT IS DEFAMATION?

Defamation is a false statement of fact that is harmful to someone's reputation, and published "with fault," meaning as a result of negligence or malice.[242]

The law of defamation dates back to the Roman Empire, but while the penalties and costs attached to defamation today are not as serious as they once were, they can still have a notorious "chilling effect," with prison sentences or massive compensation awards posing a serious risk to freedom of expression, journalistic freedom, and dissent in many countries.

The foundation for defamation in international law is article 17 of the International Covenant on Civil and Political Rights (ICCPR), which provides for protection against unlawful attacks on a person's honour and reputation. Article 19(3) of the ICCPR also makes reference to the rights and reputation of others as a legitimate ground for limitation of the right to freedom of expression.[243] Reputation is therefore the underlying basis in any claim of defamation, whether slander or libel.[244]

Defamation can be an important legal remedy to those who genuinely need it, but it can also be a weapon to quash dissent. There are many real examples where defamation may provide an important defence, for example in the non-consensual distribution of intimate images, a

---

[239] *Ibid* at section 3.
[240] *Ibid* at p 127.
[241] For example, South African law, as seen in *National Media Ltd and Others v Bogoshi,* per note 22.
[242] Electronic Frontier Foundation, 'Online Defamation Law' (accessible at https://www.eff.org/issues/bloggers/legal/liability/defamation#:~:text=Generally%2C%20defamation%20is%20a%20false,slander%20is%20a%20spoken%20defamation). Under some legal systems, most commonly English law jurisdictions such as Tanzania or Zambia, libel is the term used for a written defamation, while slander refers to spoken defamation.
[243] ICCPR: International Covenant on Civil and Political Rights (1976) (accessible at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx).
[244] For a fuller discussion on the law on defamation, see the training manual published by Media Defence on the principles of freedom of expression under international law: Richard Carver, 'Training manual on international and comparative media and freedom of expression law', Media Defence at pp 48-64 (2018) (accessible at: https://www.mediadefence.org/sites/default/files/resources/files/MLDI.FoEManual.Version1.1.pdf). See also above no. 6 for a definition of libel and slander.

growing trend in the online era that disproportionately affects women. In these cases, defamation may provide recourse to women to seek justice for the non-consensual sharing of images.

However, defamation is also frequently misused, particularly by states and powerful individuals to stifle free speech, as well as by non-state actors in the context of SLAPP suits.

CRIMINAL DEFAMATION

Historically, defamation was usually a criminal offence. While some countries still have the offence of criminal defamation on their statute books, it is widely opposed, most notably by the United Nations (UN) and the Africa Commission on Human and People's Rights (ACHPR) who have both urged states to reconsider such laws. For instance, the UN Human Rights Council (UNHRC) General Comment No. 34 provides that: "States Parties should consider the decriminalisation of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty".[245] Moreover, Principle XIII(1) of the Principles on Freedom of Expression in Africa calls on states to review all criminal restrictions on content to ensure that they serve a legitimate interest in a democratic society.

In a landmark decision handed down by the African Court on Human and Peoples' Rights (African Court) in 2013 in the matter *of Konaté v Burkina Faso*,[246] it was held that imprisonment for defamation violates the right to freedom of expression, and that criminal defamation laws should only be used in restricted circumstances. Since the African Court's decision, there have been important developments in domestic courts on the continent. For instance, in the 2016 case of *Misa-Zimbabwe et al v Minister of Justice et al*,[247] the Constitutional Court of Zimbabwe declared the offence of criminal defamation unconstitutional and inconsistent with the right to freedom of expression as protected under the Zimbabwean Constitution. Most recently, in 2018 the Constitutional Court of Lesotho struck down the provisions of the Penal Code relating to criminal defamation in *Peta v Minister of Law, Constitutional Affairs and Human Rights*,[248] stating that they violated the right to freedom of expression as protected in the Lesotho Constitution. Sierra Leone also repealed its criminal defamation laws in 2020.[249]

Additionally, the ECOWAS Court has upheld that criminal defamation and libel laws should be repealed, as evidenced in the 2018 judgment in *Federation of African Journalists and Others v The Gambia* which "recognised that the criminal laws on libel, sedition and false news

---

[245] UN Human Rights Council, 'General Comment No. 34 at article 47 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).
[246] African Court, Application No. 004/2013 (2013) (accessible at: https://en.african-court.org/images/Cases/Judgment/Judgment%20Appl.004-2013%20Lohe%20Issa%20Konate%20v%20Burkina%20Faso%20-English.pdf).
[247] Constitutional Court of Zimbabwe, Case no. CCZ/07/15 (2015) (accessible at: https://www.southernafricalitigationcentre.org/wp-content/uploads/2017/08/Order-3-Feb-2016.pdf).
[248] Constitutional Court of Lesotho, Case no. CC 11/2016 (2018) (accessible at: https://www.southernafricalitigationcentre.org/wp-content/uploads/2018/05/2018-05-21-Judgement.pdf).
[249] Media Foundation for West Africa, 'Major Boost for Press Freedom as Sierra Leone Scraps Criminal Libel Law after 55 years' (24 July 2020) (accessible at: https://www.mfwa.org/major-boost-for-press-freedom-as-sierra-leone-scraps-criminal-libel-law-after-55-years/).

disproportionately interfere with the rights of Gambian journalists and directed that The Gambia "immediately repeal or amend" these laws in line with its obligations under international law."[250]

Despite this, many countries retain criminal defamation laws, even where they have been declared unconstitutional and are clearly contrary to international law instruments. Some countries, such as Rwanda and Zambia,[251] continue to apply criminal defamation laws with vigour, while others such as South Africa have pledged to get rid of them but thus far have failed to do so.[252]

Protections against criminal defamation laws

When a criminal defamation law remains on the statue book, there are a number of strict protections that should apply to prevent defamation from being used to stifle freedom of expression:[253]

- The criminal standard of proof — beyond a reasonable doubt — should be fully satisfied.[254]
- Convictions for criminal defamation should only be secured when the allegedly defamatory statements are false, and when the mental element of the crime is satisfied, i.e. when they are made with the knowledge that the statements were false or with reckless disregard as to whether they were true or false.
- Penalties should not include imprisonment, nor should they entail other suspensions of the right to freedom of expression or the right to practice journalism.[255]
- As a less restrictive means, states should not resort to criminal law when a civil law alternative is readily available.[256]

---

[250] Media Defence, 'Update: ECOWAS Court delivers landmark decision in one of our strategic cases challenging the laws used to silence and intimidate journalists in the Gambia' (2018) (accessible at: https://www.mediadefence.org/news/update-ecowas-court-delivers-landmark-decision-in-one-of-our-strategic-cases-challenging-the-laws-used-to-silence-and-intimidate-journalists-in-the-gambia/).

[251] In 2012 Rwanda convicted a journalist of defaming the President, but in 2020 the African Commission of Human and People's Rights found that it violated her right to freedom of expression and that Rwanda's criminal defamation law violates article 9 of the African Charter. For more see here: https://www.mediadefence.org/news/african-commission-finds-rwandan-authorities-violated-journalists-right-to-freedom-of-expression/. In Zambia, the law on criminal defamation is contained in Sections 191-198 of the Penal Code (accessible here: https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/66208/62114/F-489934566/ZMB66208.pdf), while there is a separate Defamation Act of 1953, Chapter 68, that covers civil defamation (accessible here: http://www.parliament.gov.zm/node/792).

[252] Bregman Moodley Attorneys, 'Criminal Defamation', (2019) (accessible at: https://www.bregmans.co.za/criminal-defamation/).

[253] Carver, above at n 8 at p 49.

[254] Inter-American Court of Human Rights, *Kimel v. Argentina*, (2008) (accessible at: https://www.corteidh.or.cr/docs/casos/articulos/seriec_177_ing.pdf).

[255] African Court, above at n 10.

[256] See for example: European Court of Human Rights, *Amorim Giestas and Jesus Costa Bordalo v. Portugal*, Application No. 37840/10 (2014), par. 36 (accessible at: https://hudoc.echr.coe.int/eng?i=001-142084 in French).

CIVIL DEFAMATION

Despite widespread agreement that criminal punishment for defamation is no longer acceptable in a democratic society, there is nevertheless a need for some sort of remedy for those who believe that their reputation or honour has been unfairly harmed.

Therefore, many countries have domestic laws regarding civil claims for defamation, but these laws vary by jurisdiction. In some countries such as Zambia, defamation laws date back to the colonial era and are considered overly restrictive on freedom of speech by limiting criticism of leaders or by instituting disproportionately harsh sanctions.[257]

If a person is able to prove a civil claim for defamation, and the person responsible for the statement or publication is not able to successfully raise a defence, the person who has suffered reputational harm is typically entitled to monetary compensation in the form of civil damages. While civil defamation claims may serve the intended purposes of restoring reputation or honour, they can be misused and cause a "chilling effect" on the full enjoyment and exercise of freedom of expression.

Defamation used against survivors of gender-based violence

The case of Shailja Patel in Kenya is instructive of how defamation has been used specifically as a tool to silence victims of gender-based violence. Patel, a renowned Kenyan poet, playwright and activist, publicly accused a fellow writer, Tony Mochama, of sexual harassment at a writers' workshop the two attended. Mochama sued for defamation, claiming the allegations were false and Patel had a pre-existing grudge against him. In 2019, a judge found against Patel, ordered her to pay damages of more than $87,000, to apologise, and to never publish defamatory statements against Mochama again. The magistrate also castigated Patel for initially turning to social media for justice as she did not believe the justice system would treat her case fairly.[258]

Online 'naming and shaming' has become a popular recourse for victims of gender-based violence in recent years, particularly in countries where there is little trust in the criminal justice system to fairly investigate their crimes, and in which women are frequently blamed, including by police and the courts, for their own role in supposedly enabling the crime. In some cases, public 'registers' have even been compiled of accused perpetrators with the aim of warning future potential victims and raising awareness about the pervasiveness of these crimes. Allegations such as these are generally considered defamatory, and the people who originate or distribute such statements may be held liable.

---

[257] Quartz Africa, Jonathen Rozen 'Colonial and Apartheid-era laws still govern press freedom in southern Africa' (2018) (accessible at: https://qz.com/africa/1487311/colonial-apartheid-era-laws-hur-southern-africas-press-freedom/).

[258] BuzzFeed News, Tamerra Griffin, 'She Was Ordered to Pay Damages and Apologize to the Man who Allegedly Assaulted Her – So She Left the Country.' (2019) (accessible at: https://www.buzzfeednews.com/article/tamerragriffin/shailja-patel-defamation-sexual-assault-kenya-exile).

The best defence against such suits is if the accusations can be proven true and in the public interest to share. In civil cases, the standard of proof is generally lower than in criminal cases, only needing to prove truth 'on the balance of probabilities' rather than 'beyond reasonable doubt.' An additional defence is that of privilege: "statements made by someone who is under a moral or legal duty to make them or has an interest in making them to someone else who has an interest in hearing them or a duty to do so." This would require making the argument that the criminal justice system cannot provide adequate redress for the victim, and there is therefore a need for the public to hear the allegations, though success in this argument is likely to be difficult.[259]

CAN A TRUE STATEMENT BE DEFAMATORY?

In most jurisdictions, truth is a defence to defamation claims, provided it can be proven. However, in some jurisdictions, truth alone is not sufficient: it is further required that the public interest in the publication be established as well.

From a continental perspective, the ACHPR states in the Declaration of Principles on Freedom of Expression and Access to Information in Africa that "[n]o one shall be found liable for true statements, expressions of opinions or statements which are reasonable to make in the circumstances."[260]

Courts in some jurisdictions, notably South Africa, have even found that false statements may still not constitute defamation. In *National Media Ltd and Others v Bogoshi*, the court developed the defence of reasonable publication, finding that:

> "[T]he publication in the press of false defamatory allegations of fact will not be regarded as unlawful if, upon a consideration of all the circumstances of the case, it is found to have been reasonable to publish the particular facts in the particular way and at the particular time."[261]

The term "reasonable publication" encompasses the idea that the author took reasonable steps to ensure the accuracy of the content of the publication, and also that the publication was on a matter of public interest.[262] In *Trustco Group International Ltd and Others v Shikongo*, the Namibian Supreme Court found that "[t]he defence of reasonable publication holds those publishing defamatory statements accountable while not preventing them from publishing statements that are in the public interest."[263]

---

[259] The Conversation, Helen Scott, Where South Africa defamation law stands on 'naming and shaming,' (2016) (accessible at: https://theconversation.com/where-south-african-defamation-law-stands-on-naming-and-shaming-58246#:~:text=In%20South%20African%20law%20the,%E2%80%9Cright%2Dthinking%20people%E2%80%9D).

[260] African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression in Africa', (2019) (accessible at: https://www.achpr.org/legalinstruments/detail?id=69).

[261] Supreme Court of Appeal of South Africa, Case No. 579/96 (1998) (accessible at: http://www.saflii.org/za/cases/ZASCA/1998/94.pdf).

[262] Carver above at n 8 at p 52.

[263] Supreme Court of Namibia, Case No. SA 8/2009 (2010) (accessible at: https://namiblii.org/system/files/judgment/supreme-court/2010/6/2010_6.pdf).

Similarly, General Comment No. 34 states that "a public interest in the subject matter of the criticism should be recognised as a defence"[264] against defamation.

THE RIGHT TO PROTECTION AGAINST ATTACKS ON REPUTATION

The right to protection against attacks on reputation is firmly established in international law. Article 12 of the Universal Declaration of Human Rights provides that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[265] This is echoed in identical words in article 17 of the ICCPR.

However, as indicated, a balance often needs to be found against offending statements which constitute an attack on a person's reputation and the justifiable limitations on the right to freedom of expression and any associated rights.

WHAT IS THE RIGHT WAY TO DEAL WITH DEFAMATION?

When a person is found to have been defamed, they are entitled to a remedy. However, the remedies imposed are often punitive and disproportionate. We have already seen that sentences of imprisonment for criminal defamation are widely regarded as disproportionate due to their impact on freedom of expression.[266] Likewise, heavy fines, whether in criminal or civil cases, are aimed at punishing the defamer rather than redressing the wrong to the defamed.[267]

Whenever possible, redress in defamation cases should be non-pecuniary (non-financial) and aimed directly at remedying the wrong caused by the defamatory statement, such as through publishing an apology or correction.

Monetary awards — the payment of damages — should only be considered when other less intrusive means are insufficient to redress the harm caused. Compensation for harm caused (pecuniary damages) should be based on evidence quantifying the harm and demonstrating a causal relationship with the alleged defamatory statement.

Defamation on new media platforms

The growth of new media, including social media, in recent years has raised questions about whether existing civil defamation laws are adequate for the times and these new technologies. The 2019 judgment of the High Court of South Africa in *Manuel v Economic Freedom Fighters and Others*[268] provides insight into how courts may use existing

[264] UNHRC above at n 9 at p 12.
[265] UN General Assembly, 'Universal Declaration of Human Rights, Resolution 217 A (III)' (1948) (accessible at: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf).
[266] UNHRC above at n 9.
[267] African Court, above at n 10.
[268] High Court of South Africa, Gauteng Division, Case no. 13349/2019, (2019) (Accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2019/157.pdf).

defamation laws to deal with cases involving statements in online publications. The Court's judgment contained a number of novel findings:[269]

- Because it centred on a statement posted on Twitter, the Court explained that "[t]he hypothetical ordinary reader must be taken to be a reasonable representative of Twitter users who follow the EFF and Mr Malema and share his interest in politics and current affairs". The EFF is a controversial South African far-left political party, of which Mr Malema is the President and "Commander-in-Chief". Both parties have been repeatedly accused of using language that incites violence, particularly of a racial form, in their efforts to achieve 'radical transformation' of society and the economy.
- The Court referred to the 'repetition rule,' whereby persons who repeat a defamatory allegation made by another "are treated as if they made the allegation themselves, even if they attempt to distance themselves from the allegation." This has implications for others who play a role in disseminating defamatory statements further, such as by 'retweeting.' The Court did not explicitly address this point further.
- The Court also stated that the reasonable publication defence is applicable beyond just the media to ordinary members of the public too, provided they take all reasonable steps to verify the information as normally required under that defence.
- Although the judgment ordered the defendants to remove the impugned statement from their media platforms within 24 hours, 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 not addressed by the deletion (such as retweets in which persons added a comment of their own). This is a particular challenge that social media platforms pose when seeking to find an effective remedy to a claim of defamation.

The matter will soon be heard on appeal at the Supreme Court of Appeal in November 2020.[270]

TYPES OF DEFAMATORY MATERIAL

Opinion versus fact

We have dealt with above factual statements that may be defamatory. However, expressions of opinion are differentiated from factual statements. General Comment No. 34 states that defamation laws, particularly penal defamation laws, "should not be applied with regard to those forms of expression that are not, of their nature, subject to verification,"[271] such as opinions and value judgments. It also notes that "[a]ll forms of opinion are protected, including opinions of a political, scientific, historic, moral or religious nature."

[269] ALT Advisory Africa, 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/).

[270] Likewise, the case of *Stocker v Stocker* from the United Kingdom Supreme Court is instructive. The ruling was notable for its creation of a new sub-category of the 'reasonable reader' of a social media post in analysing the intended meaning of a statement, rather than relying on a more traditional and formal understanding of language. For more see: https://inforrm.org/2019/04/05/case-law-stocker-v-stocker-supreme-court-overturns-judge-on-meaning-of-tried-to-strangle-oliver-cox/).

[271] UNHRC above at n 9 at p 12.

To determine what counts as opinion, courts tend to look at whether a reasonable reader or listener would understand the statement as asserting a statement of verifiable fact, which is capable of being proven true or false. In the context of social media, a reasonable reader tends to be defined as someone who would ordinarily be following and reading the content of the person who has made the allegedly defamatory statement (per the example of *Manuel v Economic Freedom Fighters* above). The context in which the statement was made is critical to determine whether a reasonable reader or listener would understand it as opinion or as a statement of fact. There are, for example, ways in which a statement of fact may be made to appear as opinion.[272] In 2020, a US District Court dismissed a slander lawsuit filed against controversial Fox News talk show host Tucker Carlson, citing the fact that the "'general tenor' of the show should then inform a viewer that [Carlson] is not 'stating actual facts' about the topics he discusses and is instead engaging in 'exaggeration' and 'non-literal commentary.'"[273]

Humour

Similarly, content that a reasonable reader or listener would identify as humour or satire, and not reasonably interpret as stating fact, is also not liable for defamation.

A prime example is that of the South African cartoonist Jonathan "Zapiro" Shapiro, who was sued for defamation by former South African President Jacob Zuma for a cartoon in which he depicted the former President, who was previously charged with rape and accused of undermining the justice system to avoid charges of corruption, preparing to sexually assault a symbolic Lady Justice. Right before the case was to be heard, Zuma withdrew his suit, which Shapiro hailed as "an important signal that the president respects the right of the media to criticise his conduct."[274]

Statements of others

A point of consideration, particularly for journalists, is the extent to which they are liable for the potentially defamatory statements of others since a central part of their work is reporting on the words of others. The European Court of Human Rights (ECtHR) has found that a journalist is not automatically liable for the opinions stated by others, and is not required to "systematically and formally" distance themselves from "the content of a statement that might defame or harm a third party,"[275] provided they have not repeated potentially defamatory statements as their own, endorsed, or clearly agreed with them. The ruling of the High Court of South Africa in *Manuel v Economic Freedom Fighters and Others*[276] raises some questions about the extent to which this principle holds up in African courts, particularly in the online domain.

---

[272] Electronic Frontier Foundation above at n 6.
[273] US District Court, Southern District of New York, Case No. 1:2019cv11161 - Document 39' (2020) (accessible at: https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2019cv11161/527808/39/).
[274] Mail & Guardian, Verashni Pillay, 'Zapiro cartoon: Zuma surrenders, drops lawsuit,' (2012) (accessible at: https://mg.co.za/article/2012-10-28-zuma-avoids-zapiro-court-showdown-over-cartoon/).
[275] European Court of Human Rights, Application No. 1131/05 (2007).
[276] High Court of South Africa above at n 32.

Privileged statements

Privileged statements refer to those made in the public interest. Statements that are reported from the legislature or judicial proceedings are usually considered absolutely privileged, meaning that neither the author of the statement nor the media reporting it are liable for defamation. Some other types of statements reported from public meetings, documents and other material in the public domain may also enjoy qualified privilege.

Whose burden of proof?

A general principle of law is that the burden of proof lies with the claimant — the person who brings the suit or makes the "claim". However, with defamation, this principle is generally reversed, and the responsibility lies with the defendant — the person who made the allegedly defamatory statement — to prove that the statement did not damage the claimant's reputation, either because it is true or for one of the other reasons listed above. The United States is a prominent exception to this rule, wherein the burden of proof in cases brought by any public figure falls on the claimant.

Remedies and penalties

As discussed above, criminal penalties have been the focus of much attention by international bodies, to the fear of many journalists. However, it is notable that no international human rights court has ever upheld a custodial sentence on a journalist for a 'regular' defamation case. In *Konaté v Burkina Faso*, the African Court held that:

> "Apart from serious and very exceptional circumstances for example, incitement to international crimes, public incitement to hatred, discrimination or violence or threats against a person or a group of people, because of specific criteria such as race, colour, religion or nationality, the Court is of the view that violations of laws on freedom of speech and the press cannot be sanctioned by custodial sentences."[277]

It is important that civil defamation laws contain sufficient checks and balances to prevent them being used to unduly stifle freedom of expression, such as limits on financial penalties. Even in Ghana, the first African country to decriminalise defamation, "there has been an increase in civil suits for libel brought by powerful individuals, leading, in some cases, to damages payouts of such large proportions to powerful individuals as to threaten the existence of some media outlets."[278]

ALTERNATIVE CLAIMS

SLAPP suits

Alternative methods are also used to silence critics and journalists. One such example is strategic lawsuits against public participation (SLAPP), which aim to intentionally bury critics

[277] African Court above at n 10.
[278] PEN South Africa, 'Stifling Dissent, Impeding Accountability: Criminal Defamation Laws in Africa,' p 4 (2017) (accessible at: http://pensouthafrica.co.za/wp-content/uploads/2017/11/Stifling-Dissent-Impeding-Accountability-Criminal-Defamation-Laws-in-Africa.pdf).

under expensive and often baseless legal claims in order to intimidate and silence them. Usually, the objective in these cases is not a positive judgment, but rather to leverage the threat of financial damage. Libel and slander are often used as the underlying complaints in SLAPP suits.

Once case which may have a profound impact on the freedom of expression landscape in the future is that between Mineral Commodities Resources (Pty) Ltd, an Australian Mining Company, and a group of six activists who have been sued by the company for defamation, and who claim the litigation is an attempt to intimidate them and silence their criticism of the company's mining activity in the environmentally sensitive area of Xolobeni in South Africa.[279]

Concerningly, contemporary SLAPP suits now often target the lawyers representing defendants. In South Africa, a mining company Atha-Africa Ventures (Pty) Ltd), recently filed heads of argument suggesting that the public interest lawyers representing the claimants in the matter, the Centre for Environmental Rights, were inherently conflicted because their organisation aligns with the cause of the claimants, in this instance a clean and safe environment.[280] This new tactic, which finds no reference in previous precedent or case law, appears to be an attempt to intimidate not only the claimants but their lawyers as well.

A limited number of states, such as Canada,[281] have adopted anti-SLAPP legislation to ensure the protection of freedom of expression, which enables cases to be heard quickly and may allow defendants to reclaim costs from the claimant. However, there is a need for much more widespread adoption of such anti-SLAPP laws to protect critical speech and access to the courts.

Online harassment as an alternative method of suppressing dissent

Online harassment of journalists using non-legal means is another too-often used method of stifling freedom of expression and dissent in Africa, and one that has a particularly gendered nature. The case of Karima Brown in South Africa is instructive in this regard. Brown, a journalist and talk-show host, received countless death and rape threats on social media after Economic Freedom Fighters leader Julius Malema posted her phone number online (known as doxing) in retaliation for what he believed was an attempt by Brown to surveil the EFF.[282]

In its ruling, the High Court of South Africa ruled that Malema had breached the Electoral Commission Act that protects journalists from facing any harassment, intimidation, threats

[279] Centre for Environmental Rights, 'Mining company's SLAPP suit against CER lawyers, activist in court today' (2019) (accessible at: https://cer.org.za/news/mining-companys-slapp-suit-against-cer-lawyers-activist-in-court-today).
[280] See *Endangered Wildlife Trust & Another v Director General, Department of Water and Sanitation*, High Court of South Africa, Pretoria, Case No. A155/19.
[281] Osler, O'Brien and Tsilivis, 'Ontario Court of Appeal clarifies test under "anti-SLAPP" legislation' (2018) (accessible at: https://www.osler.com/en/resources/regulations/2018/ontario-court-of-appeal-clarifies-test-under-anti-slapp-legislation).
[282] Daily Maverick, Rebecca Davis. 'EFF court losses mount as Karima Brown wins battle, but faces criticism of her own' (2019) (accessible at: https://www.dailymaverick.co.za/article/2019-06-06-eff-court-losses-mount-as-karima-brown-wins-battle-but-faces-criticism-of-her-own/).

by political parties. In particular, the judge ruled that the EFF had failed to "instruct and take reasonable steps to ensure that their supporters do not harass, intimidate, threaten or abuse journalists and especially women".[283]

Insult laws

A number of other insult laws are still at play across the continent and continue to pose risks for journalists and others critical of government. For example, under the Lesotho Penal Code, the crime of *scandalum magnatum* (offences against the royal family) is created as a separate crime to defamation, and thus remains on the statute books despite criminal defamation recently being declared unconstitutional. *Scandalum magnatum* is increasingly being used by the government of Lesotho against its detractors.[284]

Likewise, the crime of sedition remains on the statute books in many countries, and continues to be used to stifle freedom of expression. Sedition is commonly defined as the crime of "incitement of resistance to or insurrection against lawful authority."[285] The Nigerian Federal Court of Appeal has distinguished between an outmoded notion of the "sovereign," who is protected by sedition laws, and the contemporary politician who is regularly subjected to a process of democratic accountability.[286]

A more recent development has been the passing of 'fake news' laws in various countries. These laws are justified by states as being necessary to protect national security or public order and to deal with the misinformation pandemic that has been unleashed by the growth of the internet and social media, but are frequently in tension with the right to freedom of expression.

Regional courts, including the African Court on Human and People's Rights, have increasingly argued that public officials should enjoy *less* protection from criticism than others.[287] Because of their status, access to the media, and power, public officials can often use their office to try to curtail freedom of expression and prosecute critics. Additional protections for those who criticise them may therefore be warranted, to counter this imbalance of power. In addition, there is a real need for those serving in public office to be open to criticism and public input. As the European Court of found:

> "The [politician] inevitably and knowingly lays himself open to close scrutiny of his every word and deed by both journalists and the public at large, and he must display a greater degree of

[283] High Court of South Africa, Gauteng Division, Case No. 14686/2019 (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2019/166.html).
[284] Hoolo 'Nyane, 'Abolition of criminal defamation and retention of *scandalum magnatum* in Lesotho', African Human Rights Law Journal (2019) (accessible at: http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1996-20962019000200010).
[285] Merriam Webster Dictionary, 'Sedition', (accessible at: https://www.merriam-webster.com/dictionary/sedition).
[286] Federal Court of Appeal of Nigeria, Chief Arthur Nwankwo v. The State, 6 NCLR 228 (1983), par. 237.
[287] African Court on Human and Peoples' Rights, Application No. 004/2013, at par. 155 (2014) (accessible at: https://en.african-court.org/index.php/55-finalised-cases-details/857-app-no-004-2013-lohe-issa-konate-v-burkina-faso-details).

> tolerance, especially when he himself makes public statements that are susceptible of criticism."[288]

The Office of the High Commissioner for Human Rights (OHCHR) has also called for the abolition of the offence of 'defamation of the State,'[289] and some jurisdictions have refused to allow elected and other public authorities to sue for defamation.[290] The ECtHR has limited such suits to situations which threaten public order, implying that governments cannot sue in defamation simply to protect their honour.[291]

Abuse of process

Lastly, those seeking to silence critics and journalists may abuse court processes to meet their objectives. Recently in South Africa, a mining company, Tharisa Minerals (Pty) Ltd, filed for a protection order against two community activists. The mine ultimately withdrew the application which is largely reserved for victims and survivors of domestic abuse.[292]

Practical steps on defamation

- **If you have been a victim or survivor of the non-consensual distribution of intimate images**, you may be able to use defamation as a remedy.
  - If you are able to show that the distribution of the images harmed your reputation, you may have success in a defamation case.
  - The challenge with using civil defamation as a remedy is that the images may technically be 'true', or even taken with the victim's consent. However, if it can be shown that there existed an associated implication about the subject of the images (e.g. that reflect on their character) which can be proven false, a defamation claim is more likely to have success.

- **If someone has posted slanderous comments about you online**, and you are also a user of the same social media platform, you may have recourse with that social media company.

---

[288] European Court of Human Rights, Application No. 11662/85 (1991), par. 59 (accessible at: https://hudoc.echr.coe.int/eng?i=001-58044). For more on this topic, see the seminal case establishing the need for public officials to face a higher threshold of criticism, *New York Times v Sullivan* in the United States Supreme Court, 376 US 254 (1964) at paras 279-80 (accessible at: https://supreme.justia.com/cases/federal/us/376/254/).

[289] OHCHR, Concluding Observations of the Human Rights Committee: Serbia and Montenegro, CCPR/CO/81/SEMO (12/08/2004), par. 22 (accessible at: https://www.refworld.org/docid/42ce6cfe4.html).

[290] OHCHR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,' E/CN.4/2000/63 (2000) (accessible at: https://www.ohchr.org/en/issues/freedomopinion/pages/annual.aspx).

[291] *Ibid*.

[292] See Power Singh Inc, 'Protecting and promoting freedom of expression in Marikana,' (accessible at: https://powersingh.africa/2020/09/22/protecting-and-promoting-freedom-of-expression-in-marikana/).

- Most social media companies have defamation reporting processes,[293] which may enable you to have the comments taken down. However, they are unlikely to provide further recourse beyond removing the offending content.

- **If you have been targeted by a SLAPP suit** that uses defamation charges to silence or intimidate you:
  - Approach a reputable public interest law firm or human rights lawyers for assistance. Sometimes, lawyers may be able to act *pro bobo* (free of charge) or rely on legal defence funds for their fees.

- **If you live in a country that has defamation laws that infringe regional and international human rights**, you may be able to do something about it:
  - Consider whether you have access to other regional or international human rights courts, such as the African Court of Human Rights, or regional courts such as the ECOWAS Community Court of Justice.
  - There may be jurisprudence in your country opposing the use of disproportionate penalties for defamation, but which have not yet been implemented by the judiciary or criminal justice system.

CONCLUSION

The criminalisation of defamation poses a serious risk to freedom of expression, particularly with the rise of new media platforms online. Defamation serves a real purpose to protect individuals from affronts to their dignity, but is too often abused to instead silence and punish dissent. Despite the recent trend towards the decriminalisation of defamation, there remains a need to ensure the implementation of judgments, to remove criminal punishments for other insult laws, and to institute legal protections against alternative methods of silencing activists such as SLAPP suits.

[293] For Facebook, see here: https://www.facebook.com/help/contact/233704034440069.
For Twitter, see here: https://help.twitter.com/forms/abusiveuser.

Module 6

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

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 6

HATE SPEECH

- **Certain types of speech, known as hate speech, are prohibited by international law.**
- **It is important to find the right balance between speech that is offensive, yet important for freedom of expression and dissent, and speech which constitutes impermissible hate speech.**
- **Regulating hate speech can be particularly difficult in the online context.**
- **Most domestic laws mandate that hate speech requires an intention to incite violence with a reasonable chance, but not that actual harm results.**
- **The biggest danger with hate speech is that vagueness in defining its meaning may open up space for such laws to be used as tools to stifle criticism.**
- **Advocacy of genocide or denial of the holocaust, along with religious defamation, are often treated as special cases of hate speech.**

INTRODUCTION

Despite the importance of freedom of expression, not all speech is protected under international law, and some forms of speech are required to be prohibited by states. Article 20 of the International Covenant on Civil and Political Rights (ICCPR) provides that:

> "(1) Any propaganda for war shall be prohibited by law.
> (2) Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."

In addition, article 4(a) of the International Convention on the Elimination of All Forms of Racial Discrimination requires that the dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, must be declared an offence that is punishable by law.

Hate speech provisions under international law distinguish between three categories of speech: that which must be restricted, that which may be restricted; and that which is lawful and subject to protection, according to the severity of the speech in question. Hate speech regulations vary significantly by jurisdiction, particularly in how they define what constitutes hate speech and to what extent they differ by speech that is offline versus online.

There is a need for clear and narrowly circumscribed definitions of what is meant by the term "hate speech", or objective criteria that can be applied. Over-regulation of hate speech can violate the right to freedom of expression, while under-regulation may lead to intimidation, harassment or violence against minorities and protected groups.

Importantly, hate speech should not be conflated with offensive speech, as the right to freedom of expression includes speech that is robust, critical, or that causes shock or offence.[294] Hate speech is perhaps the topic that creates the most disagreement among defenders of freedom of expression, as defining the line between offensive but constructive critical speech and hate speech can be extremely difficult.

As a general principle, no one should be penalised for statements that are true. Furthermore, the right of journalists to communicate information and ideas to the public should be respected, particularly when they are reporting on racism and intolerance, and no one should be subject to prior censorship. Finally, any sanctions for hate speech should be in strict conformity with the principle of proportionality.

There are some distinctions between hate speech online and offline that may require consideration,[295] but the law usually does not distinguish between the two:

- Content is more easily posted online without due consideration or thought. Online hate speech cases need to distinguish between poorly considered statements posted hastily online, and an actual threat that is part of a systemic campaign of hatred.
- Once something is online, it can be difficult (or impossible) to get it off entirely. Hate speech posted online can persist in different formats across multiple different platforms, which can make it difficult to police.
- Online content is frequently posted under the cover of anonymity, which presents an additional challenge to dealing with hate speech online.
- The internet has transnational reach, which raises cross-jurisdictional complications in terms of legal mechanisms for combatting hate speech.

The re-emergence of the use of hate speech laws in Kenya is an example of how well-meaning laws that limit supposedly dangerous speech can quickly turn into tools for the suppression of dissent. The 2008 National Cohesion and Integration Act (NCIC) encourages national cohesion and integration by outlawing discrimination and hate speech on ethnic grounds to prevent the kind of deadly election-related violence that Kenya experienced in 2007-2008. However, in 2020 two Members of Parliament were arrested for speech that was critical of the President and his mother under provisions in the NCIC.[296]

---

[294] Media Defence, 'Training manual on digital rights and freedom of expression online, at p 57 (2020) (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

[295] Media Defence, 'Training Manual on Digital Rights and Freedom of Expression Online' (2010) at p 57 (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).

[296] Article 19 Eastern Africa, 'Kenya: Use of "hate speech" laws and monitoring of politicians on social media platforms' (2020) (accessible at: https://www.article19.org/resources/kenya-use-of-hate-speech-laws/).

WAS "HATE SPEECH" INTENDED TO INCITE?

Hate speech that is intended to incite hostility, discrimination or violence falls under the type of expression that international law mandates must be restricted. Therefore, a key factor when dealing with hate speech cases is the requirement for there to have been an *intention* to incite hatred.

The Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence,[297] compiled by a meeting of experts coordinated by the United Nations Office of the High Commissioner for Human Rights (OHCHR), proposes a six-part threshold test to establish whether expression rises to the threshold of being criminal. One of these is intent: "advocacy" and "incitement" are required, rather than mere distribution or circulation. Article 20 of the ICCPR also requires intent. Negligence and recklessness therefore do not rise to the standard of hate speech.

A prime example of this distinction is the case of *Jersild v Denmark* before the European Court of Human Rights (ECtHR). Jersild was a television journalist who made a documentary featuring interviews with members of a racist, neo-Nazi gang. He was prosecuted and convicted for propagating racist views. However, the ECtHR found that the journalist's intent was to make a serious social inquiry exposing the views of the racist gangs, not to promote their views. There was a clear public interest in the media playing such a role:

> "Taken as a whole, the feature could not objectively have appeared to have as its purpose the propagation of racist views and ideas. On the contrary, it clearly sought - by means of an interview - to expose, analyse and explain this particular group of youths, limited and frustrated by their social situation, with criminal records and violent attitudes, thus dealing with specific aspects of a matter that already then was of great public concern… The punishment of a journalist for assisting in the dissemination of statements made by another person in an interview would seriously hamper the contribution of the press to discussion of matters of public interest and should not be envisaged unless there are particularly strong reasons for doing so."[298]

Building counter-narratives as a response to hate speech

According to the United Nations Educational, Scientific and Cultural Organization (UNESCO), non-legal methods of countering hate speech are equally important. One such measure is building a counter-narrative by promoting greater media and information literacy as a more structural response to hate speech online:

> "Given young people's increasing exposure to social media, information about how to identify and react to hate speech may become increasingly important. It is particularly important that anti-hate speech modules are incorporated in those countries where the

[297] Office of the High Commissioner for Human Rights (OHCHR), 'Freedom of expression vs incitement to hatred: OHCHR and the Rabat Plan of Action', (2012) (accessible at: https://www.ohchr.org/en/issues/freedomopinion/articles19-20/pages/index.aspx).
[298] European Court of Human Rights, Application No. 15890/89, (1994) para. 33-35 (accessible at: http://hudoc.echr.coe.int/eng?i=001-57891).

actual risk of widespread violence is highest. There is also a need to include in such programmes, modules that reflect on identity, so that young people can recognise attempts to manipulate their emotions in favour of hatred, and be empowered to advance their individual right to be their own masters of who they are and wish to become."[299]

MUST VIOLENCE OR HATRED ACTUALLY RESULT?

Another tenet of the Rabat Plan of Action threshold test is the likelihood and imminence of violence.[300] Incitement, by definition, is an inchoate crime. The action advocated through incitement speech does not have to be committed for it to amount to a crime. Nevertheless, some degree of risk of resulting harm must be identified. This means that courts will have to determine that there was a reasonable probability that the speech would succeed in inciting actual action against the target group. Courts in different jurisdictions have differed on just how likely the harm needs to be to constitute a criminal act.

For example, in *South African Human Rights Commission v Khumalo*,[301] the High Court of South Africa found that the respondent's utterances against white people were hate speech, despite the fact that there was no evidence of an actual harm having being committed as a result of his statements, though they did clearly incite and advocate for violence.[302]

Online hate speech laws being used to stifle free speech

Many African states are increasingly resorting to new online hate speech laws to curb the flood of mis- and disinformation that arrived with the advent of the internet and social media. For example, in 2020 Ethiopia enacted the Hate Speech and Disinformation Prevention and Suppression Proclamation which, while having seemingly well-intentioned objectives, has been decried by civil society as a threat to freedom of expression and access to information online.[303]

Often this is because of:

- Overly broad definitions of hate speech and disinformation.
- Vague provisions that allow discretionary interpretation by law enforcers such as prosecutors and courts and enable the laws to abuse fundamental rights.
- Holding internet intermediaries liable for content policing.

---

[299] UNESCO, Iginio Gagliardone et al, 'Countering online hate speech' at p 58 (accessible at: http://unesdoc.unesco.org/images/0023/002332/233231e.pdf).
[300] OHCHR above n 4.
[301] High Court of South Africa, Gauteng Division, Case No. EQ6/2016 & EQ1/2018 (2018) (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2018/528.html).
[302] South African Human Rights Commission, 'Media Statement: SAHRC Welcomes the Equality Court's Finding Against Velaphi Khumalo' (2018) (accessible at: https://www.sahrc.org.za/index.php/sahrc-media/news-2/item/1591-media-statement-sahrc-welcomes-the-equality-court-s-finding-against-velaphi-khumalo).
[303] CIPESA, Edrine Wanyama, 'Ethiopia's New Hate Speech and Disinformation Law Weighs Heavily on Social Media Users and Internet Intermediaries' (2020) (accessible at: https://cipesa.org/2020/07/ethiopias-new-hate-speech-and-disinformation-law-weighs-heavily-on-social-media-users-and-internet-intermediaries/).

- Providing for overly harsh and punitive penalties for violations.

Kenya has passed a similar law,[304] and more are under consideration in Nigeria[305] and South Africa.[306] Critics argue that these laws constitute nothing less than online censorship.

THE DANGER OF VAGUENESS

The obvious danger in regulating hate speech is that vagueness in the definition of what constitutes a criminal act will be used to penalise expression that has neither the intent nor the realistic possibility of inciting hatred.

The Constitutional Court of South Africa recently reflected on this in the case of *Qwelane v South African Human Rights Commission and Another*. Qwelane, who at the time was serving as South Africa's ambassador to Uganda, had published a column in a local newspaper disparaging the "lifestyle and sexual preferences" of "homosexuals". The High Court found that the statement constituted hate speech as defined in the Equality Act, section 10 of which prohibits the publishing of hurtful statements that cause harm or spread hate. Qwelane sought to have section 10 of the Equality Act declared unconstitutional on the basis that it infringed on the right to freedom of expression. In 2019, the Supreme Court of Appeal (SCA) agreed the section was unconstitutional because it "extends far beyond the limitations on freedom of expression provided for in the Constitution and in many respects is unclear."[307]

The SCA deemed the section's use of the word "hurtful" particularly vague, adding that all definitions of the word "are concerned with a person's subjective emotions . . . in response to the actions of a third party. This does not equate with causing harm or incitement to harm."[308] Counsel for the South African Human Rights Commission contended, however, that:

> "Viewed from the equality and dignity lens, 'hurtful' is not merely concerned about the subjective emotions and feelings of a person in response to the actions of a third party — instead, it is concerned about injuries or impairments on a person's dignity."[309]

---

[304] Mail & Guardian, 'Kenya signs bill criminalizing fake news' (2019) (accessible at: https://mg.co.za/article/2018-05-16-kenya-signs-bill-criminalising-fake-news/).
[305] Amnesty International, 'Nigeria: bills on hate speech and social media are dangerous attacks on freedom of expression' (2019) (accessible at: https://www.amnesty.org/en/latest/news/2019/12/nigeria-bills-on-hate-speech-and-social-media-are-dangerous-attacks-on-freedom-of-expression/).
[306] Daily Maverick, Pierre de Vos, 'Hate speech bill could be used to silence free speech' (2019) (accessible at: https://www.dailymaverick.co.za/opinionista/2019-02-26-hate-speech-bill-could-be-used-to-silence-free-speech/).
[307] Supreme Court of Appeal of South Africa, Case no. 686/2018, (2018) (accessible at: http://www.saflii.org/za/cases/ZASCA/2019/167.pdf).
[308] Mail & Guardian, Sarah Smit, 'The Qwelane case: when human rights meet human rights' (2020) (accessible at: https://mg.co.za/news/2020-09-20-the-qwelane-case-when-human-rights-meet-human-rights/).
[309] *Ibid*.

The case hinges on whether homophobic slurs constitute incitement, and whether the definition of 'hurtful' in the Equality Act is sufficiently precise so as not to unduly restrict freedom of expression. The Constitutional Court reserved judgment in September 2020.[310]

ADVOCACY OF GENOCIDE AND HOLOCAUST DENIAL: A SPECIAL CASE?

Some commentators argue that the issues of advocacy for genocide and denial of the Holocaust constitute special cases within the debate on hate speech and incitement. According to the 1948 Genocide Convention, "direct and public incitement to commit genocide" is a punishable act,[311] following the role of the media in perpetuating hatred against Jewish people in Germany and advocating for their extermination.

Likewise, in Rwanda the media played a crucial role during the genocide in drumming up hatred and distributing propaganda, which led to the first prosecutions at the International Criminal Tribunal for Rwanda (ICTR) for "direct and public incitement to commit genocide." In the same way as hate speech, incitement to genocide was defined as an inchoate crime, meaning it is not necessary for genocide to actually have occurred for the crime to have been committed, but it did require intent.

One of the most notable cases brought against journalists at the ICTR was *Nahimana et al*, known as the Media Trial.[312] Two of the respondents were the founders of a radio station that broadcast anti-Tutsi propaganda before the genocide and the names and licence plate numbers of intended victims during the genocide.[313]

The Rome Statute establishing the International Criminal Court also establishes the crime of incitement to genocide.[314]

The genocide of the Jews in Nazi-occupied Europe was such a formative event in the creation of the European human rights system that Holocaust denial — claiming that the genocide did not occur — is an offence in several countries and is treated in a particular fashion within the European Court of Human Rights jurisprudence, even when compared to similar cases of historical revisionism.[315]

---

[310] Daily Maverick, Greg Nicholson, ''The best remedy for hateful speech is more speech' Jon Qwelane's advocate argues in ConCourt' (2020) (accessible at: https://www.dailymaverick.co.za/article/2020-09-23-the-best-remedy-for-hateful-speech-is-more-speech-jon-qwelanes-advocate-argues-in-concourt/).

[311] United Nations General Assembly, Convention on the Prevention and Punishment of the Crime of Genocide, Resolution 260 (III) (1948), Art. 3.(accessible at: https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.1_Convention%20on%20the%20Prevention%20and%20Punishment%20of%20the%20Crime%20of%20Genocide.pdf).

[312] International Criminal Tribunal for Rwanda, Case No. ICTR-99-52-T, (2003) (accessible at: https://unictr.irmct.org/en/cases/ictr-99-52).

[313] Media Defence above at no. 2.

[314] International Criminal Court, 'Rome Statue of the International Criminal Court' at articles 6, 25 and 33 (2002) (accessible at: https://www.icc-cpi.int/resource-library/documents/rs-eng.pdf).

[315] For example, see the cases of *Léhideux and Isorni v. France,* Application No. 55/1997/839/1045 (1998), and *Garaudy v. France*, Application No. 65831/01 (2003), both in the ECtHR.

RELIGIOUS DEFAMATION

Many African states have laws prohibiting defamation of religions, and many that inherited the common law system also have the crime of blasphemous libel. For example, despite ostensibly being a secular state with no state religion, article 816 of Ethiopia's Criminal Code states that anyone who, by:[316]

> "…gestures or words scoffs at religion or expresses himself in a manner which is blasphemous, scandalous or grossly offensive to the feelings or convictions of others or towards the Divine Being or the religious symbols, rites or religious personages, is punishable with fine or arrest not exceeding one month."

Some countries have implemented excessively harsh penalties for the crimes of blasphemy and defamation of religion, including death. For example, Mauritania's blasphemy law, updated in 2017 to include even harsher language, ranks as the worst blasphemy law in the world, containing the penalty of death even if the accused repents for the alleged insult.[317] Six other African countries, including Somalia and Egypt, have scored 'higher than average' on the harshness of their religious defamation laws.[318]

General Comment 34 states that:[319]

> "Prohibitions of displays of lack of respect for a religion or other belief system, including blasphemy laws, are incompatible with the Covenant, except in the specific circumstances envisaged in article 20, paragraph 2, of the Covenant. Such prohibitions must also comply with the strict requirements of article 19, paragraph 3, as well as such articles as 2, 5, 17, 18 and 26. Thus, for instance, it would be impermissible for any such laws to discriminate in favour of or against one or certain religions or belief systems, or their adherents over another, or religious believers over non-believers. Nor would it be permissible for such prohibitions to be used to prevent or punish criticism of religious leaders or commentary on religious doctrine and tenets of faith."

Many other countries have abolished the offence of blasphemy in recent years, for example the United Kingdom in 2008,[320] Canada in 2018,[321] and Denmark in 2017.[322]

---

[316] End Blasphemy Laws, 'Ethiopia,' (2020) (accessible at: https://end-blasphemy-laws.org/countries/africa-sub-saharan/ethiopia/).
[317] United States Commission on International Religious Freedom, 'Apostasy, blasphemy, and hate speech laws in Africa: Implications for freedom of religion or belief,' at page 16 (2019) (accessible at: https://www.justice.gov/eoir/page/file/1243281/download).
[318] *Ibid* at page 15.
[319] UN Human Rights Council, 'General Comment No. 34 at p 12 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).
[320] Media Defence, 'Training Manual on International and Comparative Media and Freedom of Expression Law', Richard Carver, (2020) (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI.FoEManual.Version1.1.pdf).
[321] Global News Wire, 'Repeal of Canada's Blasphemy Law Applauded by National Secularist Organization' (2018) (accessible at: https://www.globenewswire.com/news-release/2018/12/14/1667079/0/en/Repeal-of-Canada-s-Blasphemy-Law-Applauded-by-National-Secularist-Organization.html).
[322] The Guardian, 'Denmark scraps 334-year old blasphemy law' (2017) (accessible at: https://www.theguardian.com/world/2017/jun/02/denmark-scraps-334-year-old-blasphemy-law).

The Constitutional Court of South Africa grappled with religious hate speech in the case of *South African Human Rights Commission v Masuku*,[323] which concerns whether statements made by the respondent constitute hate speech against Jewish people in terms of the Equality Act. Judgment has, however, been reserved until the Constitutional Court determines the constitutionality of section 10 of the Equality Act (see *Qwelane* above).

CONCLUSION

Hate speech is a highly contentious issue in Africa, dividing the community of freedom of expression defenders on where the line should sit between protecting speech that is harmful to minority groups and enabling important dissent and criticism. The challenges of dealing with hate speech are particularly salient in online hate speech cases, where intent can be more complicated and remedies harder to implement. Defamation of religion and particularly tragic past events such as genocides are sometimes treated as special cases, but there are questions around whether this is justified. Related crimes such as blasphemy are beginning to be removed in progressive jurisdictions, and African states who have not yet removed these crimes, should be encouraged to follow suit.

[323] Constitutional Court of South Africa, Case CCT 14/19 (2019) (accessible here: https://collections.concourt.org.za/handle/20.500.12144/36612?show=ful).

Module 7

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

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 7

CYBERCRIMES

- **As access to the internet continues to grow rapidly in Africa, cybercrimes are becoming ever more prevalent and dangerous.**
- **However, laws which regulate criminal activity on the internet are increasingly providing tools for the state to suppress dissent and the media.**
- **The African Union (AU) has encouraged a harmonised, continent-wide approach to tackling cybercrimes in Africa, but the AU Convention on Cyber Security and Personal Data (Malabo Convention) has not yet achieved widespread adoption, limiting its efficacy.**
- **Despite the limited adoption of the Malabo Convention, data privacy is starting to attract more widespread attention across the continent, with many countries recently passing new data protection acts.**
- **Concerningly, many cybercrimes have a particularly gendered nature, such as cyberstalking and revenge porn.**
- **There are, however, various practical steps that can be taken to address online harms, and ensure that fundamental rights are equally protected both off- and online.**

INTRODUCTION

The increase in internet access in the recent past has created a number of new legal challenges. While the internet is transnational, amorphous, and difficult to define, the new landscape created by the digital world has often confounded the law when it comes to protecting fundamental rights in the digital age. Old definitions about what constitutes a publisher or a journalist are increasingly complicated; overcoming the anonymity afforded by many internet platforms can be a difficult, if not impossible, endeavour; and there are serious questions about who is liable for content shared online that may affect multiple parties in different jurisdictions in some way.

Regulating and legislating crimes that occur on, or relate to, the internet has been a difficult undertaking for states and international bodies. It is estimated that African economies lost $3.5 billion in 2017 due to cybercrimes,[324] and Africa accounts for 10% of the total global cyber

[324] Kshetri, 'Cybercrime and Cybersecurity in Africa' (2019) (accessible at: https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527).

incidents.[325] Without adequate regulatory frameworks and protections, the growth of internet access, e-commerce, and economic development may lead to increased instances of cybercrimes.

In Africa, where the number of new internet users continues to grow at a rapid rate, the increase in access to the internet and information and communications technologies (ICTs) has also led to increased violations of users' rights. Laws to regulate criminal activity on the internet are increasingly providing tools for the state to suppress dissent or to punish critics and independent media because of their often vague and overly broad nature.

As far back as 2011, the United Nations (UN) Special Rapporteur on freedom of expression warned that:

> "[L]egitimate online expression is being criminalized in contravention of States' international human rights obligations, whether it is through the application of existing criminal laws to online expression, or through the creation of new laws specifically designed to criminalize expression on the internet. Such laws are often justified on the basis of protecting an individual's reputation, national security or countering terrorism, but in practice are used to censor content that the Government and other powerful entities do not like or agree with."[326]

Unfortunately, little has changed in the intervening period.

WHAT IS A CYBERCRIME?

Definition

There is no precise, universal definition of the term 'cybercrime'. In general terms, it refers to a crime that is committed using a computer network or the internet.[327] This can cover a wide range of activities, including terrorist activities and espionage conducted with the help of the internet and illegal hacking into computer systems, content-related offences, theft and manipulation of data, and cyberstalking.[328]

Cybercrimes and cybersecurity are two issues that cannot be separated in an interconnected digital environment. Cybersecurity, or the management of cybercrimes, refers to the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber-environment and organisational and user's assets, such as computing devices, applications and telecommunication systems.[329]

---

[325] African Union, 'A global approach on Cybersecurity and Cybercrime in Africa' at p 9 (accessible at: https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf).
[326] United Nations General Assembly, Human Rights Council, 17th Session, 'Report of the Special Rapporteur on freedom of expression' at p10 (2011) (accessible at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf).
[327] Article 19, 'Freedom of Expression and ICTs: overview of international standards' at p 25 (2018) (accessible at: https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf).
[328] *Id.*
[329] ITU Definition of Cybersecurity, (accessible at: https://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx).

Cybercrimes in international law

The African Union (AU) has sought to encourage a continent-wide approach to tackling cybercrimes through the Convention on Cyber Security and Personal Data Protection (known as the Malabo Convention).[330] Because of the cross-border and international nature of cybercrimes, the AU argues that "national legislation cannot be drafted in isolation and national governments must seek to harmonize national legislation, regulations, standards and guidelines on Cybersecurity issues."[331] However, even the AU itself was the target of a major cyberattack between 2013 and 2017,[332] and the Malabo Convention has been criticised for using vague language which may be open to abuse by states. An example is the provision that criminalises the use of insulting language.[333]

Article 25 of the Malabo Convention calls on states to adopt legislation and/or regulatory measures to prosecute cybercrimes. Nevertheless, the text is clear that such legislation should not infringe on fundamental rights and freedoms:

> "In adopting legal measures in the area of cybersecurity and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others."[334]

The UN General Assembly Resolution on the Creation of a global culture of cyber security also states that:

> "Security should be implemented in a manner consistent with the values recognised by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency."[335]

The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention, is the only binding international instrument on cybercrime, and serves as a useful guideline for countries developing cybercrimes legislation.[336]

---

[330] Institute for Security Studies, Karen Allen 'Is Africa cybercrime savvy?' (2019) (accessible at: https://issafrica.org/iss-today/is-africa-cybercrime-savvy).
[331] African Union above n 2 at p 3.
[332] Le Monde, 'A Addis-Abeba, le siège de l'Union africaine espionné par Pékin' (2018) (accessible at: https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html).
[333] African Union 'Convention on Cyber Security and Personal Data Protection' Article 3(g) (2014) (accessible at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection).
[334] *Id*.
[335] UN General Assembly, Fifty-seventh session, 'Resolution on the Creation of a global culture of cyber security, at p 3 (accessible at: https://digitallibrary.un.org/record/482184?ln=en).
[336] Council of Europe, 'Budapest Convention and Related Standards', (accessible at: https://www.coe.int/en/web/cybercrime/the-budapest-convention).

Cybercrimes in domestic law

Cybercrime legislation has proliferated across Africa in recent years, but only eight states ratified the Malabo Convention which requires fifteen ratifications to enter into force.[337]

In order to ensure that cybercrimes laws do not unnecessarily infringe on the fundamental rights to freedom of expression, privacy and access to information, they should meet the following criteria:

- Provide narrow, clear and adequate definitions of cybercrimes.
- Require proof about the likelihood of harm arising from a given criminal activity.
- Require the nature of the threat to national security resulting from any criminal activity to be identified.
- Provide for a public interest defence in relation to the obtaining and dissemination of information classified as secret.
- As a general principle, not impose prison sentences for expression-related offences, except for those permitted by international legal standards and with adequate safeguards against abuse.[338]

TYPES OF CYBERCRIMES

Data privacy violations

The use of data, including the volume of cross-border data flows, is increasing every year, particularly in relation to personal data. However, there is a lack of adequate regulations for the collection and processing of personal information which can have significant ramifications, making data protection regulations critical. At least fourteen African countries currently have data protection laws in place,[339] but their comprehensiveness and effectiveness varies significantly. Some of the most recently passed laws were in Kenya and the Togolese Republic, which were signed into law in November and October 2019 respectively.[340] Countries such as South Africa and Morocco have successfully set up Data Protection Authorities (DPAs) to enforce data protection regulations and investigate violations, though many such DPAs still suffer from a lack of funding and political support, leading to a lack of proper enforcement.

The rise of sophisticated surveillance technologies and the use of biometric technologies without proper safeguards are just some of the many threats to the right to privacy across Africa. There have, however, been some encouraging judgments in recent years pointing to the willingness of judiciaries around Africa to protect the right to privacy.

---

[337] African Union, 'List of countries which have signed, ratified/acceded to the African Union Convention on cyber security and personal data protection' (2020) (accessible at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection).
[338] Media Defence, 'Training manual on digital rights and freedom of expression online, at pp 62 (2020) (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).
[339] ALT Advisory, 'Data Protection Africa' (accessible at: https://dataprotection.africa/).
[340] *Id* at https://dataprotection.africa/trends/.

In Kenya, the High Court in Nairobi ruled in 2020 in *Nubian Rights Forum and Others v The Hon. Attorney General and Others*[341] that the government could not implement a new comprehensive digital identity system without an adequate data protection law being in place. On surveillance, the High Court of South Africa found in the case of *amaBhungane and Another v Minister of Justice and Correctional Services and Others*[342] in 2019 that mass surveillance and the interception of communications by the National Communications Centre were unlawful, and declared certain sections of the Regulation of Interceptions of Communications and Provision of Communication Related Information Act (RICA) unconstitutional.

These developments follow the rapid development of data protection legislation around the world since the entry into force of the European Union's General Data Protection Regulations (GDPR) in 2018. The GDPR has set a new standard for the protection of personal data online, and has served as a template for numerous other countries' legislation. The California Consumer Privacy Act (CCPA) likewise has set sweeping regulations regarding consumers' rights to know what personal information is being collected from them, to request deletion of their data, and to opt out of data collection.[343] Because of its application to the technology sector of Silicon Valley, the CCPA has also been lauded for advancing the state of data protection globally.[344]

Criminalisation of online speech

Cybercrimes legislation usually seeks to deal with a wide range of illegal or harmful content that is posted online. This may include terrorist propaganda, racist content, hate speech, sexually explicit content such as child pornography, blasphemous content, content critical of states and their institutions and content unauthorised by intellectual property rights holders.[345]

This is often the area in which such legislation most conflicts with the right to freedom of expression and the right to information. The UN Special Rapporteur on Freedom of Expression stated in 2011 that the only types of expression that states may prohibit under international law are: (a) child pornography; (b) direct and public incitement to commit genocide; (c) hate speech; (d) defamation; and (e) incitement to discrimination, hostility or violence.[346] Even legislation that does criminalise these forms of expression needs to be precise, have adequate and effective safeguards against abuse or misuse, and include

[341] High Court of Kenya in Nairobi, Consolidated petitions no. 56, 58 & 59 of 2019, (2020) (accessible at: http://kenyalaw.org/caselaw/cases/view/189189/).
[342] High Court of South Africa in Pretoria, Case No. 25978/2017, (2019) (accessible at: http://www.saflii.org/za/cases/ZAGPPHC/2019/384.html).
[343] Forbes, 'California Begins Enforcing Broad Data Privacy Law – Here's What You Should Know' (2020) (accessible at: https://www.forbes.com/sites/siladityaray/2020/07/01/california-begins-enforcing-broad-data-privacy-law---heres-what-you-should-know/?sh=1279e683de5c).
[344] The Guardian, 'California's groundbreaking privacy law takes effect in January. What does it do?' (2019) (accessible at: https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do).
[345] Article 19, 'Freedom of Expression and ICTs' (2018) (accessible at: https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf).
[346] United Nationals Special Rapporteur on the Right to Freedom of Opinion and Expression, Frank La Rue, (2011) para 25 (accessible at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf).

oversight and review by an independent and impartial tribunal or regulatory body.[347] In 2018, the Special Rapporteur stated that "[b]roadly worded restrictive laws on "extremism", blasphemy, defamation, "offensive" speech, "false news" and "propaganda" often serve as pretexts for demanding that companies suppress legitimate discourse."[348]

In Zimbabwe, for example, the Cyber Security and Data Protection Bill was published in the Zimbabwean Government Gazette shortly after extensive public protests had taken place over rising fuel and commodity prices in the country. It is intended to consolidate cyber-related offences and provide for data protection and seeks to "create a technology-driven business environment and encourage technological development and the lawful use of technology."[349] However, the Bill has been widely criticised as being a tool for the Zimbabwean government to stifle freedom of expression, access to information, promote interference of private communications and data, and use search and seizure powers to access the information of activists in order to quell protests.[350] MISA-Zimbabwe has criticised the Bill for:

> "Criminali[sing] the sending of messages that incite violence or damage to property. In the past, this charge has been used to prosecute organizers of peaceful protests and other forms of public disobedience. The same goes for sections 164A and 164B that criminalize the sending of threatening messages and cyber-bullying and harassment respectively."[351]

For more on the criminalisation of online speech, see Module 3 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online.

Cyberstalking and online harassment

Online harassment is becoming increasingly prevalent with the spread of social media, which can provide especially fertile ground for online harassment. Cyberstalking is undue harassment and intimidation online through text messages, phone calls or social media, and it severely restricts the enjoyment that persons have of their rights online, particularly vulnerable and marginalised groups, including women and members of sexual minorities. Research has shown that online harassment is often focused on personal or physical characteristics, with political views, gender, physical appearance and race being among the most common.[352] Furthermore, women encounter sexualised forms of online harassment at much higher rates than men.[353]

---

[347] *Id* at para. 71.
[348] United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression, (2018) para 13 (accessible at: https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf.)
[349] ALT Advisory Africa, 'Zimbabwe gazettes Cyber Security and Data Protection Bill' (2020) (accessible at: https://altadvisory.africa/2020/05/20/zimbabwe-gazettes-cyber-security-and-data-protection-bill/).
[350] Paradigm Initiative, 'On Zimbabwe's Approval of a Cybercrime and Cybersecurity Bill' (2019) (accessible at: https://paradigmhq.org/zimbabwe-cybercrime-bill/).
[351] MISA-Zimbabwe, 'Commentary on Cybersecurity and Data Protection Bill HB 18 of 2019' (2019) (accessible at: https://zimbabwe.misa.org/wp-content/uploads/sites/13/2020/06/Commentary-on-Zimbabwe-Cybersecurity-and-Data-Protection-Bill-2019.pdf).
[352] Pew Research Center, 'Online harassment 2017, (2017), (accessible at: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/).
[353] *Id*.

A worrying new trend: non-consensual dissemination of intimate images

A particular form of online harassment that has emerged as a concerning new trend is that of private and sexually explicit images, mostly of women, being shared publicly online without their permission or consent, often by former partners in retaliation for a break-up or other falling out, or for the purposes of extortion, blackmail or humiliation. However, few countries' cybercrime legislation specifically caters for offences related to non-consensual dissemination of intimate images (NCII), often leaving victims with little recourse against perpetrators.[354]

South Africa is an exception, having passed the Film and Publications Board Amendment Act[355] in 2019 which, for the first time, explicitly criminalised the practice of non-consensual dissemination of intimate images, stating that:

> "[A]ny person who knowingly distributes private sexual photographs and films in any medium including through the internet, without prior consent of the individual or individuals and where the individual or individuals in the photographs or films is identified or identifiable in the said photographs and films, shall be guilty of an offence and liable upon conviction."[356]

Practical steps to take if you are a victim of non-consensual dissemination of intimate images:

- Make a record (and copies) of the content posted online, to ensure permanent documentation of the crime. This should include the date the content was posted, where it was posted, and who posted it. Screenshots are a useful way to do this.
- Seek psycho-social and legal assistance. (You may be able to interdict the further dissemination of images or video.)[357]
- File a report with the police. Even if your country does not have a specific provision for the non-consensual dissemination of intimate images, an offence may be located within the existing criminal law.
- File a report with the platform on which the content was posted. It might also help to include a copy of the police report in your report to the platform.[358]

The importance of a name:

---

[354] For example, although legislation in both Malawi and Uganda includes anti-pornography and anti-obscenity provisions, neither cater specifically to NCII situations, often leaving victims with little recourse. For more see Chisala-Tempelhoff and Kirya, 'Gender, law and revenge porn in Sub-Saharan Africa: a review of Malawi and Uganda' (2016) (accessible at: https://www.nature.com/articles/palcomms201669).

[355] South Africa Film and Publications Board Amendment Act, 2019 (accessible at: https://static.pmg.org.za/Films_and_Publications_Act.pdf).

[356] *Ibid* at section 24(E).

[357] See Case number A3032-2016 in the High Court of South Africa for reference (2017) (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2017/297.html).

[358] News24, Oberholzer, 'What to do if you're a victim of revenge porn & image-based abuse,' (2020) (accessible at: https://www.sowetanlive.co.za/s-mag/2020-06-29-what-to-do-if-youre-a-victim-of-revenge-porn-image-based-abuse/).

The non-consensual dissemination of intimate images is often referred to as 'revenge porn.' However, activists and researchers have universally rejected the term as being misleading.[359] Firstly, the word 'revenge' implies that the victim has committed a harm worth seeking revenge for, and 'porn' conflates the practice with the consensual production of content for mass consumption, which NCII decidedly is not. Secondly, the term "repackages an age-old harm as a new-fangled digital problem," belying the long history that exists of images of women being distributed non-consensually across a range of mediums.[360] Lastly, the term oversimplifies the offence by ignoring a range of aggressors and motivations, and invoking a moralist reaction against the victim.[361]

Many stalking crimes begin online before moving offline,[362] and cyberstalking can be complicated for many reasons:

> "[Cyberstalking is] online harassment, threats, intimidating messages and subscribing the victim to unwanted online services. From the outset this interaction may be considered an irritation or an annoyance or may give rise to a belief that harm may be caused. The cyber-stalker may however initiate contact in a non-confrontational manner and proceed to woo or groom the victim into a cyber-friendship in order to gain the victim's confidence and to determine personal details such as the person's address. Without the victim's knowledge the same "cyber-friend" could be stalking the victim in person, perhaps even giving the victim advice on how he or she should respond to the stalker. Although cyberstalking which has escalated into stalking the victim in person i.e. "real-time stalking" may result in the commission of a sexual offence, it is not the only outcome."[363]

Because of this complexity, as well as the rapid evolution of technology that makes it difficult for regulation to keep up, the South African Law Reform Commission recommended that specific reference to cyberstalking not be included explicitly in law:

> "In reality, however surreal "cyberstalking" or the use of technical or computerised equipment to stalk a person is it fundamentally amounts to an extension of physical stalking. One is merely dealing with a different medium."[364]

Ongoing harassment and attacks on members of the media have also become a particularly worrying trend.

---

[359] GenderIT, '"Revenge Porn": 5 important reasons why we should not call it by that name' (2019) (accessible at: https://www.genderit.org/articles/5-important-reasons-why-we-should-not-call-it-revenge-porn).
[360] *Id*.
[361] Association for Progressive Communications, 'Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences' (2017) at p.21 (accessible at: https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf)).
[362] South Africa Law Reform Commission, 'Report on Stalking,' (2006) (accessible at: https://www.justice.gov.za/salrc/reports/r_pr130_stalking.pdf).
[363] *Id* at p 182.
[364] *Id* at p 183.

Online harassment of the media

Where journalists allege imminent threats to their safety, courts are empowered to grant interdictory relief in appropriate circumstances and subject to the relevant legal requirements.

For instance, in the matter of *South African National Editors Forum and Others v Black Land First and Others*,[365] the High Court of South Africa granted an interdict in favour of the media broadly, in terms of which the respondents were interdicted from "engaging in any of the following acts directed towards the applicants: intimidation; harassment; assaults; threats; coming to their homes; or acting in any manner that would constitute an infringement of their personal liberty", and from "making any threatening or intimidating gestures on social media… that references any violence, harm and threat."[366]

Cyberbullying

It is also worth noting the crime of cyberbullying, which is the sending of intimidating or threatening messages, often via social media, and which is pervasive among children and young adult.[367] According to the United Nations Children's Fund (UNICEF):

> "[Cyberbullying] can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include:
>
> - spreading lies about or posting embarrassing photos of someone on social media;
> - sending hurtful messages or threats via messaging platforms;
> - impersonating someone and sending mean messages to others on their behalf.
>
> Face-to-face bullying and cyberbullying can often happen alongside each other. But cyberbullying leaves a digital footprint — a record that can prove useful and provide evidence to help stop the abuse."[368]

The scale of the problem is significant and growing. A study by UNICEF and the UN Special Representative of the Secretary-General (SRSG) on Violence against Children found that one in three young people in 30 countries reported being a victim of online bullying.[369]

---

[365] High Court of South Africa in Johannesburg, Case No 23897/17, (2017) (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2017/179.html).
[366] *Ibid* at para. 29.
[367] News24, above at no. 35. For more on online harassment see pp. 38-44 of Module 4 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-4-privacy-and-security-online/).
[368] UNICEF, 'Cyberbullying: What is it and how to stop it' (accessible at: https://www.unicef.org/end-violence/how-to-stop-cyberbullying).
[369] UNICEF, 'UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying' (2019) (accessible at: https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying).

David v Goliath: tackling cyberbullying on tech platforms

In South Africa, the family of a teenager who was sent graphic threats through Instagram from an anonymous account, has pitted them against one of the largest technology companies in the world, Facebook, the owner of Instagram.[370] The girl, who has reason to believe the threats are from someone attending her school, fears for her physical safety and has therefore been attempting to force Facebook to release the identity of the person behind the anonymous account sending the threats. Multiple attempts to do so were futile, forcing the family to turn to the courts for relief. The case is an interesting example of challenges in holding multi-national companies to account in the digital age, and raises questions about how far their responsibility to protect children who use their platforms should go.

Other violations

Given that the Malabo Convention has yet to be tested in practice, a reading of the Budapest Convention on Cybercrime, the first international treaty that seeks to address internet and computer crimes, is instructive.[371] It is increasingly being used in Africa, and has served as a guideline or source for more than 80% of states around the world to develop domestic cybercrimes laws.[372] It is also open for any state willing to implement its provisions to join, and can be ratified by African countries.[373]

The Budapest Convention defines the following types of cybercrimes:

- Illegal access to a computer system;
- Illegal interception;
- Data interference;
- System interference;
- Misuse of devices;
- Computer-related forgery;
- Computer-related fraud;
- Child pornography;
- Offences related to infringements of copyright and related rights.[374]

Although these definitions date to 2001, much of what constitute cybercrimes today is still covered by these categories and provisions.

---

[370] Daily Maverick, 'Anonymously threatened with gang rape and murder, SA teenager takes Facebook Inc to court to disclose perpetrator' (2020) (accessible at: https://www.dailymaverick.co.za/article/2020-07-24-anonymously-threatened-with-gang-rape-and-murder-sa-teenager-takes-facebook-inc-to-court-to-disclose-perpetrator/).
[371] Council of Europe, 'The State of Cybercrime Legislation in Africa – an Overview' at p. 2 (2015) (accessible at: https://rm.coe.int/16806b8a79).
[372] Council of Europe, 'The global state of cybercrime legislation 2013 – 2020: A cursory overview,' at page 5 (2020) (accessible at: https://rm.coe.int/3148-1-3-4-cyberleg-global-state-feb2020-v1-public/16809cf9a9).
[373] Council of Europe, 'Chart of signatures and ratifications of Treaty 185' (2020) (accessible at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures).
[374] Council of Europe above n 48 at p 8.

TRENDS IN AFRICA

As the AU notes in the 'Common Approach on Cybersecurity and Cybercrimes':

> "[T]he rapid pace of innovation in the ICT sector can result in gaps in the legislative and regulatory cybersecurity framework since the challenge for the legislator is the delay in the recognition of the new types of offences and the adoption of amendments to the applicable legislation."[375]

As a result, many African governments have been keenly adopting new cybercrimes legislation in an attempt to keep pace and to continue to protect against crimes committed online. There are currently at least 41 African states that have basic cybercrimes legislation either fully or partially in place, though many are missing implementing regulations.[376]

However, cybercrimes legislation is increasingly being used to unjustly regulate internet content as well, including undesirable criticism or dissent. Access Now notes that one of the main concerns about the plethora of laws that are currently being enacted to regulate cybercrimes — whilst there may be a legitimate aim in doing so — is that many of them lack clear definitions and are susceptible to being used to regulate online content and restrict freedom of expression.[377] This is a growing concern among human rights defenders as many have been subjected to a wave of arrests and convictions in what is an escalating assault on freedom of expression by cybercrime laws. Many of the laws are vague and overbroad, lacking clear definitions, leaving them open to arbitrary and subjective interpretation.

For example, Nigeria's Cybercrime Act of 2015 has been widely criticised for being used to suppress dissent and silence the media.[378] The Committee to Protect Journalists states that in just the first year of the law being in force, five bloggers who criticised politicians and businesspeople online and through social media were accused of the crime of cyberstalking under the new law, which carries a fine of up to 7 million naira (USD$22 000) and a maximum jail term of three years. According to Paradigm Initiative Nigeria, it gives law enforcement "extensive powers to hold personal data without corresponding liability" and has "no provision… to seek redress."[379] It also makes the all-too-common error of using vaguely defined "national security" as a justification for outlawing a wide range of online activities.[380]

Other common problematic clauses in cybercrimes legislation include those that criminalise the "creation of sites with a view to disseminating ideas and programmes contrary to public

---

[375] African Union above n 2 at p 3.
[376] Council of Europe above n 49 at p 4.
[377] Access Now, 'When "cybercrime" laws gag free expression: stopping the dangerous trend across MENA' (2018) (accessible at: https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/).
[378] Committee to Protect Journalists, Peter Nkanga 'How Nigeria's cybercrime law is being used to try to muzzle the press' (2016) (accessible at: https://cpj.org/2016/09/how-nigerias-cybercrime-law-is-being-used-to-try-t/).
[379] *Id.*
[380] OrderPaper, 'Tomiwa Ilori, The Nigerian Cybercrimes Act 2015: Is It Uhuru Yet?' (accessible at: http://www.orderpaper.ng/nigerian-cybercrimes-act-2015-uhuru-yet/).

order or morality", "broadcasting information to mislead security forces", "publication of false information," and more.[381]

In the case of *Andare v Attorney General of Kenya*,[382] the High Court of Kenya emphasised that the state has a duty to demonstrate that cybercrimes laws are permissible in a free and democratic society, to establish the relationship between the limitation and its purpose, and to show that there were no less restrictive means to achieve the purpose intended.[383] Unfortunately, too few states in Africa have so far taken this approach.

STEPS TO TAKE IN RESPONSE TO ONLINE HARMS

This section lays out practical approaches to dealing with various online harms.

Actions taken by state actors

- **Tell the story and engage in advocacy**. While ensuring that the identity of the victim or survivor is fully protected, identify the online harms committed and brief the press and start an advocacy campaign. Too often, reportage is limited in terms of the perpetration of online harms which enables these practices to grow.
- **Consider domestic legal challenges.** Many cybercrimes laws in Africa arguably breach fundamental rights and freedoms, especially in their vagueness and generality. In such cases, recourse to the courts may provide relief, especially in constitutional democracies. In cases where existing legislation does not cater specifically for crimes committed online, there may be an opportunity to apply or develop existing laws, such as those found with existing criminal laws.
- **Approach regional courts**. In cases where cybercrimes legislation is being used to unjustly violate rights and freedoms and domestic courts are not amenable, there may be recourse in regional human rights courts such as the ECOWAS Community Court of Justice, the East African Court of Justice, or the African Court on Human and Peoples' Rights, if jurisdiction can be established. These courts have jurisdiction to determine State compliance with regional human rights agreements and related legal instruments.[384]

Actions taken by non-state actors

- **Consider obtaining an interdict or harassment order.** A harassment order can be an inexpensive civil remedy useful in cases where the behaviour may not constitute a crime but may impact negatively on the rights of a person. The order prohibits a person from harassing another person, and breaching it constitutes an offence, which is usually

---

[381] *Id* at p 8.
[382] High Court of Kenya at Nairobi, Petition No. 149 of 2015 (2015) (accessible at: http://kenyalaw.org/caselaw/cases/view/121033/).
[383] See also, *Shreyal Singh v India*, Writ 167 of 2012 (accessible at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2015/06/Shreya_Singhal_vs_U.O.I_on_24_March_2015.pdf).
[384] International Justice Resource Center, 'Courts and Tribunals of Regional Economic Communities,' (accessible at: https://ijrcenter.org/regional-communities/).

punishable by a fine or a period of imprisonment. Many anti-harassment acts include bullying and cyberstalking. Legal representation is usually not necessary, and orders can be applied for at the lower courts.[385]

- **Report behaviour to the relevant platform that was used.** Most social media platforms have mechanisms for reporting illegal or unethical behaviour, which may result in content being taken down or the offending user being blocked either temporarily or permanently. It may help to revise the relevant platforms' terms of use prior to reporting to identify the most salient term that has been violated.[386]

CONCLUSION

Although the rise of cybercrimes must be addressed, a growing trend of using cybercrimes legislation to clamp down on dissent and free speech is deeply concerning. While the internet is a rapidly evolving space, legislation can and should be designed to include specific protections for online harms both at an individual level, such as cyberstalking, and at a societal level, such as regulating the flow and use of personal data. Social media companies also have a role to play in ensuring that their platforms are not used for the distribution of illegal and harmful content. More generally, there is a need for countries in Africa to collaborate on an approach to tackling cybercrimes which are frequently transnational in nature.

---

[385] Department of Justice and Constitutional Development, Protection from Harassment Act, 2011 (Act 17 of 2011 (accessible at: https://www.justice.gov.za/forms/form_pha.html).

[386] Complaints platforms are available:
Facebook: https://www.facebook.com/help/263149623790594;
Instagram: https://help.instagram.com/192435014247952;
Twitter: https://help.twitter.com/en/rules-and-policies/twitter-report-violation#:~:text=Open%20the%20profile%20you'd,the%20issue%20you're%20reporting;
YouTube: https://support.google.com/youtube/answer/2802027?co=GENIE.Platform%3DAndroid&hl=en-GB; and
TikTok: https://support.tiktok.com/en/privacy-safety/report-inappropriate-content-default.

Module 8

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

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 8

'FALSE NEWS', MISINFORMATION AND PROPAGANDA

- **'False news' refers to news items that are intentionally and verifiably false, and seek to mislead readers.**
- **While acknowledging the social ills occasioned by false news and misinformation, courts and international actors maintain that general and over-broad provisions which criminalise false news and misinformation violate the right to freedom of expression.**
- **As a result, strategies to combat misinformation, at this stage, are more social and educational in their character. These include Media and Information Literacy (MIL) strategies and campaigns which focus on human rights, media, computer, intercultural, and privacy literacy as a holistic method of mitigating misinformation. These strategies may be complemented by social media verification, fact-checking, and the publication of counter-narratives.**
- **In limited instances, misinformation may constitute hate speech and litigation may be necessary. However, any litigation relating to expression should be fully considered for unintended consequences and the possibility of jurisprudence which may negatively impact freedom of expression.**
- **Propaganda is dissimilar to misinformation in that it is expressly prohibited in international law, where it propagates for war or advocacy of hatred that constitutes incitement.**

INTRODUCTION[387]

The phenomenon of false news and misinformation has increased exponentially in recent times with the advent of the internet and social media platforms. While manipulating and distorting information is squarely part of the historical record, the weaponisation of information in the 21st century is occurring on an unprecedented scale, which requires urgent and effective responses.[388] This module focuses on 'false news', misinformation and propaganda and provides guidance on media and information literacy (MIL) strategies and campaigns[389] which may assist with mitigating misinformation while ensuring that the right to freedom of expression is not violated.

---

[387] For more on this topic see Media Defence "Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf). For further information see First Draft, 'Understanding and addressing the disinformation ecosystem' (2017) (accessible at: https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v3.pdf?x17007).

[388]

[389] *Id* at page 70 (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000265552).

For the purposes of this module, the terms "misinformation" is used broadly and, unless otherwise specified, includes reference to disinformation and mal-information.

WHAT IS 'FALSE NEWS'

'False news' refers to news items that are intentionally and verifiably false, and seek to mislead readers. In March 2017, the Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda (2017 Joint Declaration) was issued by the relevant freedom of expression mandate-holders of the United Nations (UN), the African Commission on Human and Peoples' Rights (ACHPR), the Organisation for Security and Co-operation in Europe (OSCE), and the Organisation of American States (OAS).[390] The 2017 Joint Declaration noted the growing prevalence of disinformation and propaganda, both online and offline, and the various harms to which they may contribute or be a primary cause. The quandary remains that the internet both facilitates the circulation of disinformation and propaganda and also provides a useful tool to enable responses to this.

Importantly, the 2017 Joint Declaration stressed that general prohibitions on the dissemination of information based on vague and ambiguous ideas, such as "false news", are incompatible with international standards for restrictions on freedom of expression. However, it went further to state that this did not justify the dissemination of knowingly or recklessly false statements by official or state actors. In this regard, the Joint Declaration called on state actors to take care to ensure that they disseminate reliable and trustworthy information, and not to make, sponsor, encourage or further disseminate statements that they know (or reasonably should know) to be false or which demonstrate a reckless disregard for verifiable information.

The 2017 Joint Declaration identified the following standards on disinformation and propaganda:

> "**Standards on disinformation and propaganda**
>
> (a) General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a), and should be abolished.
>
> (b) Criminal defamation laws are unduly restrictive and should be abolished. Civil law rules on liability for false and defamatory statements are legitimate only if defendants are given a full opportunity and fail to prove the truth of those statements and also benefit from other defences, such as fair comment.
>
> (c) State actors should not make, sponsor, encourage or further disseminate statements which they know or reasonably should know to be false (disinformation) or which demonstrate a reckless disregard for verifiable information (propaganda).
>
> (d) State actors should, in accordance with their domestic and international legal obligations and their public duties, take care to ensure that they disseminate reliable and trustworthy information, including about matters of public interest, such as the economy, public health, security and the environment."

[390] Accessible at: https://www.osce.org/fom/302796?download=true.

False news provisions are laws which prohibit and punish the dissemination of false or inaccurate statements. This has been decriminalised in various countries. For example, in the matter of *Chavunduka and Another v Minister of Home Affairs and Another*,[391] the Zimbabwe Supreme Court dealt with the constitutionality of the criminal offence of publishing false news under Zimbabwean law. In 1999, following the publication of an article in *The Standard* titled "Senior army officers arrested", the editor and a senior journalist were charged with contravening section 50(2)(a) of the Law and Order Maintenance Act, on the basis that they had published a false statement that was likely to cause fear, alarm or despondency among the public or a section of the public. The editor and journalist challenged the constitutionality of this provision as being an unjustifiable limitation of the right to freedom of expression and the right to a fair trial.

Of particular relevance, in finding that the section was indeed unconstitutional, the Supreme Court stated that:

> "Because s 50(2)(a) is concerned with likelihood rather than reality and since the passage of time between the dates of publication and trial is irrelevant, it is, to my mind, vague, being susceptible of too wide an interpretation. It places persons in doubt as to what can lawfully be done and what cannot. As a result, it exerts an unacceptable "chilling effect" on freedom of expression, since people will tend to steer clear of the potential zone of application to avoid censure, and liability to serve a maximum period of seven years" imprisonment.
>
> The expression "fear, alarm or despondency" is over-broad. Almost anything that is newsworthy is likely to cause, to some degree at least, in a section of the public or in a single person, one or other of these subjective emotions. A report of a bus accident which mistakenly informs that fifty instead of forty-nine passengers were killed, might be considered to fall foul of s 50(2)(a).
>
> The use of the word "false" is wide enough to embrace a statement, rumour or report which is merely incorrect or inaccurate, as well as a blatant lie; and actual knowledge of such condition is not an element of liability; negligence is criminalised. Failure by the person accused to show, on a balance of probabilities, that any or reasonable measures to verify the accuracy of the publication were taken, suffices to incur liability even if the statement, rumour or report that was published was simply inaccurate."

Accordingly, the Supreme Court held that the criminalisation of false news, as contained in section 50(2)(a), was unconstitutional and a violation of the right to freedom of expression.

[391] Supreme Court of Zimbabwe, 2000 (1) ZLR 552 (S) (2000) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/chavunduka-v-minister-home-affairs/).

More recently, the ECOWAS Court of Justice delivered a landmark judgment in the case of *Federation of African Journalists and Others v The Gambia*,[392] where it found that the rights of four Gambian journalists had been violated by the state authorities. It was submitted that security agents of The Gambia arbitrarily arrested, harassed and detained the journalists under inhumane conditions, and forced them into exile for fear of persecution as a consequence of their work as journalists.

The Court upheld the claim, finding that The Gambia had violated the journalists' rights to freedom of expression, liberty, and freedom of movement, as well as violated the prohibition against torture. As such, it awarded six million Dalasi in compensation to the journalists. Importantly, the Gambia was ordered to immediately repeal or amend its laws on, amongst others, false news in line with its obligations under international law.

MISINFORMATION, DISINFORMATION AND MAL-INFORMATION

The problem statement

Misinformation is distinct to the quality of journalism and the circulation of trustworthy information which complies with professional standards and ethics.[393] However, misinformation and its ilk are not new but rather have become increasingly more powerful as they are fueled by new technologies and rapid online dissemination. The consequence is that digitally-fueled misinformation, in contexts of polarisation, risks eclipsing quality journalism, and the truth.[394]

Increasingly, the strategies to combat misinformation are more social and educational in their character in order to ensure that the right to freedom of expression is not violated by over-broad legislative provisions which criminalise or, in any way, chill expression. The current misinformation ecosystem, therefore, requires a critical assessment of the reasons for the dissemination of misinformation and the establishment of MIL campaigns.[395] In effect, combatting misinformation, at this stage, falls more within the realm of advocacy and education than it does litigation. The limited litigation in this space bears testament to this. However, this is likely to change as digital rights litigators engage in more strategic and test case litigation seeking to mitigate misinformation while protecting and promoting freedom of expression.

Defining false information[396]

[392] ECOWAS Community Court of Justice, Application No. ECW/CCJ/APP/36/15, (2018) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/federation-african-journalists-faj-others-v-gambia/).

[393] UNESCO Handbook above n 2 at p.18.

[394] *Id*.

[395] *Id* at p. 70.

[396] *Id* at pp. 45-6.

Disinformation	Disinformation is information that is false, and the person who is disseminating it knows it is false. "It is a deliberate, intentional lie, and points to people being actively disinformed by malicious actors".[397]
Misinformation	Misinformation is information that is false, but the person who is disseminating it believes that it is true.[398]
Mal-information	Mal-information is information that is based on reality but it is used to inflict harm on a person, organisation or country.[399]

Causes of misinformation

To understand how to combat misinformation, it is useful to first understand how it spreads. With the advent of the information age and the internet, information is spread more rapidly and often with the click of a mouse.[400] Equally, the speed at which information is transmitted and the instant access to information which the internet provides has caused a rush to publish and be the first to transit information. This, alongside more insidious practices such as the intentional distribution for disinformation for economic or political gain, has created what the UN Educational, Scientific and Cultural Organisation (UNESCO) refers to as a "perfect storm".[401]

UNESCO identifies three causes enabling the spread of misinformation:

1. **Collapsing traditional business models**. As a result of the rapid decline in advertising revenue and the failure of digital advertising to generate profit, traditional newsrooms are bleeding audiences, with media consumers moving to "peer-to-peer" news products offering "on demand-access". These decreasing budgets lead to reduced quality control and less time for "checks and balances". They also promote "click-bait" journalism.[402] Importantly, peer-to-peer news has no agreed-upon ethics and standards.
2. **Digital transformation of newsrooms and storytelling**. As the information age develops, there is a discernible digital transformation in the news industry. This transformation causes journalists to prepare content for multiple platforms, limiting their ability to properly interrogate facts. Often, journalists apply a principle of "social-first publishing" whereby their stories are posted directly to social media to meet audience demand in real-time. This, in turn, promotes click-bait practices and the pursuit of "virality" as opposed to quality and accuracy.[403]
3. **The creation of new news ecosystems**. With increasing access to online audiences as a result of the advent of social media platforms, users of these platforms can curate their own content streams and create their own "trust network" or "echo chambers" within

[397] *Id* at pp 44-5.
[398] *Id*.
[399] *Id*.
[400] *Id* at p.55.
[401] *Id*.
[402] *Id* at p. 57.
[403] *Id* at pp. 57-8.

> which inaccurate, false, malicious and propagandistic content can spread. These new ecosystems allow misinformation to flourish as users are more likely to share sensationalists stories and are far less likely to properly assess sources or facts. Importantly, once published, a user who becomes aware that a publication may constitute misinformation is largely unable to "pull back" or correct the publication.[404]

These causes continue to pose difficulties for newsrooms, journalists, and social media users as the new news ecosystems, in particular, enable malicious practices and actors to flourish. However, as discussed, there is a fine line between seeking to combat the spread of misinformation online and violating the right to freedom of expression.

WASHLITE v Fox News[405]

On 2 April 2020, the Washington League for Increased Transparency and Ethics (WASHLITE) instituted proceedings against Fox News, a conservative American news network, claiming that "Fox's repeated claims that the COVID-19 pandemic was/is a hoax is not only an unfair act, it is deceptive and therefore actionable under Washington's Consumer Protection Act."[406] WASHLITE sought a declaration to this effect and an injunction (interdict) prohibiting repeated statements on Fox News stating that COVID-19 is a hoax. In its findings, the Washington Superior Court found that WASHLITE's goal was "laudable" but that its arguments ran "afoul of the protections of the First Amendment", the right to freedom of expression. Its case was subsequently dismissed.

How to combat misinformation

Effectively combatting misinformation remains a pressing contemporary issue, with various remedies posited by jurists, academics, and activists. Notably, Associate Justice of the Supreme Court of the United States, Anthony Kennedy, in his majority decision in *United States v Alvarez*[407] held that "[t]he remedy for speech that is false is speech that is true. This is the ordinary course in a free society. The response to the unreasoned is the rational; to the uninformed, the enlightened; to the straight-out lie, the simple truth."[408] MIL strategies and campaigns proposed by UNESCO seek to operationalise the position proposed by Justice Kennedy and provide a holistic approach to combating misinformation, without limiting the right to freedom of expression.

---

[404] *Id* at pp. 59-61.
[405] *Washington League for Increased Transparency and Ethics v Fox News*, Plaintiffs Complaint for Declaratory and Injunctive Relief, 2 April 2020 (accessible here: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3190&context=historical).
[406] *Id.*
[407] *United States v Alvarez*, 567 U.S. 709 (2012) (accessible at: https://www.supremecourt.gov/opinions/11pdf/11-210d4e9.pdf).
[408] *Id* at pp. 15-6.

Media and Information Literacy (MIL) strategies and campaigns

As a point of departure, UNESCO proposes MIL strategies and campaigns as a process which enables the detection of misinformation and a means to combat its spread, particularly online.[409] MIL is an umbrella and inter-related concept which is divided into:

- **Human rights literacy** which relates to the fundamental rights afforded to all persons, particularly the right to freedom of expression, and the promotion and protection of these fundamental rights.[410]
- **News literacy** which refers to literacy about the news media, including journalistic standards and ethics.[411] This includes, for example, the specific ability to understand the "language and conventions of news as a genre and to recognise how these features can be exploited with malicious intent."[412]
- **Advertising literacy** which relates to understanding how advertising online works and how profits are driven in the online economy.[413]
- **Computer literacy** which refers to basic IT usage and understating the easy manner in which headlines, images, and, increasingly, videos can be manipulated to promote a particular narrative.[414]
- **Understanding the "attention economy"** which relates to one of the causes of misinformation and need for journalists and editors to focus on click-bait headlines and misleading imagery to grab the attention of users and, in turn, drive online advertising revenue.[415]
- **Privacy and intercultural literacy** which relates to developing standards on the right to privacy and a broader understanding of how communications interact with induvial identity and social developments.[416]

MIL strategies and campaigns, such as the COVID-19 campaign by the UN detailed below, should underscore the importance of media and information literacy in general but should also include a degree of philosophical understating. According to UNESCO, "[MIL strategies and campaigns should assist users] grasp that authentic news does not constitute the full 'truth' (which is something only approximated in human interactions with each other and with reality over time)."[417]

Five ways in which the UN is fighting the COVID-10 'infodemic'[418]

The coronavirus (COVID-19) pandemic has generated significant amounts of misinformation, ranging from the use of disinfectants to combat the virus to false

---

[409] UNESCO Handbook above n 2 at p.70.
[410] *Id* at p.70.
[411] *Id*.
[412] *Id.*
[413] *Id*.
[414] *Id*.
[415] *Id* at p.47.
[416] *Id* at p.70.
[417] *Id* at p.72.
[418] Accessible at: https://www.un.org/en/un-coronavirus-communications-team/five-ways-united-nations-fighting-%E2%80%98infodemic%E2%80%99-misinformation.

claims that the virus can spread through radio waves and mobile networks. In order to counter this "infodemic", the UN has taken five steps to combat misinformation:

1. **Produce and disseminate facts and accurate information**. As a point of departure, the UN identified that the World Health Organisation (WHO) is at the foreground of the battle against the pandemic and that it is transmitting authoritative information based on science while also seeking to counter myths. Identifying sources such as the WHO that produce and disseminate facts is a central tenet to countering misinformation.
2. **Partner with platforms and suitable partners**. Allied to the distribution of accurate information is finding the right partners. The UN and the WHO have partnered with the International Telecommunications Union (ITU) and the UN Children's Fund (UNICEF) to help persuade all telecommunications companies worldwide to circulate factual text messages about the virus.
3. **Work with the media and journalists**. UNESCO has published two policy briefs that assess the COVID-19 which assist journalists working on the frontlines of the "infodemic" around the world to ensure accurate, trustworthy and verifiable public health information.
4. **Mobilise civil society**. Through the UN Department of Global Communications, key sources of information on opportunities to access, participate and contribute to UN processes during COVID-19 have been communicated to civil society organisations (CSOs) to ensure that all relevant stakeholders ae communicated.
5. **Speak out for rights**. Michelle Bachelet, recently joined a chorus of other activists, to speak out against restrictive measures imposed by states against independent media, as well as the arrest and intimidation of journalists, arguing that the free flow of information is vital in fighting COVID-19.

Litigation where justifiable limitations exist[419]

The International Covenant on Civil and Political Rights (ICCPR) provides in article 20 that "[a]ny propaganda for war shall be prohibited by law" and that "[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."

In addition, article 4(a) of the International Convention on the Elimination of All Forms of Racial Discrimination (CERD) requires that the dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, must be declared an offence that is punishable by law.

Despite the importance of freedom of expression, not all speech is protected under international law, and some forms of speech are required to be prohibited by states. However, there is a need for clear and narrowly circumscribed definitions of what is meant by the term "hate speech", or objective criteria that can be applied. Over-regulation of hate speech can violate the right to freedom of expression, while under-

[419] See Module 6 of this series for more information on hate speech and justifiable limitations to freedom of expression.

regulation may lead to intimidation, harassment or violence against minorities and protected groups.

In instances where misinformation is so egregious that it meets the definitional elements of hate speech, litigation may be a useful and important tool in the protection and promotion of fundamental rights, includes the right to equality and dignity.[420] However, such litigation should be fully considered for unintended consequences and the possibility of jurisprudence which may negatively impact freedom of expression. Dependent on the content of the speech and the harm that it causes, the publication of counter-narratives may constitute a useful complementary strategy to litigation.

For more information on this topic, see module 6 of this series.

Fact-checking and social media verification

Alongside MIL strategies and campaigns and litigating misinformation that constitutes hate speech, another effective tool to combat misinformation is fact-checking and social media verification. According to the Duke Reporters' Lab, in 2020 there are over 290 fact-checking projects debunking false news and misinformation in 83 countries, an increase of over 100 organisations from 2019.[421]

In general, fact-checking and verification processes, which were first introduced by US weekly magazines such as *Time* in the 1920s,[422] consist of:

- **Ex-ante fact-checking and verification**. Increasingly and due to shrinking newsroom budgets, ex-ante (or before the event) fact-checking is reserved for more prominent and established newsroom and publications who employ dedicated fact-checkers.[423]
- **Ex-post fact-checking, verification and "debunking"**. This method of fact-checking is becoming increasingly popular and focuses on information published after the fact. It concentrates "primarily (but not exclusively) on political ads, campaign speeches and political party manifestos" and seeks to make politicians and other public figures accountable for the truthfulness of their statements.[424] Debunking is a subset of fact-checking and requires a specific set of verification skills, increasingly in relation to user-generated content on social media platforms.

Fact-checking is central to strategies to combat misinformation and has grown exponentially in recent years due to the increasing spread of false news and misinformation, and the need to debunk viral hoaxes.[425] Alongside MIL strategies and campaigns, fact-checking and social media verification is becoming increasingly important in the fight against false news and misinformation.

---

[420] For a useful discussion on the balancing of rights see J Geldenhuys and M Kelly-Louw, 'Hate Speech and Racist Slurs in the South African Context: Where to Start?' (Vol 23) [2020] PER 12 (accessible at: http://www.saflii.org/za/journals/PER/2020/12.html).
[421] Duke Reporters' Lab, Annual census finds nearly 300 fact-checking projects around the world' (22 June 2020) (accessible at: https://reporterslab.org/tag/international-fact-checking-network/).
[422] UNESCO above n 2 at p.81.
[423] *Id*.
[424] *Id* at p.82.
[425] For more resources on the legal defence of factcheckers, see the Fact-Checkers Legal Support Initiative (accessible at: https://factcheckerlegalsupport.org/).

The REAL411[426] and PADRE[427]

The Real 411 is a new initiative which was recently launched in South Africa and which constitutes a civil society-led strategy to combat disinformation. The online REAL411 platform, which was supported by South Africa's Independent Electoral Commission during South Africa's 2019 national elections, allows users to report disinformation to the Digital Complaints Committee (DCC) who assist a complainant with referrals to one of the multiple statutory bodies in South Africa which may assist with a remedy. The DCC may also assist with the publication of counter-narratives. Aggrieved parties may appeal to the Appeals Committee should they be dissatisfied with an outcome.

In addition to the REAL411, PADRE or the Political Party Advert Repository was an innovative civil-society initiative which collated political party advertisements and assisted users to distinguish between genuine and false political party advertising during South Africa's 2019 national elections.

PROPAGANDA

As detailed above and in module 6 of this series, unlike dis- and misinformation, the spread of propaganda is expressly prohibited in international law, provided that it propagates for war or advocacy of hatred that constitutes incitement.[428] In these instances, multiple direct legal remedies such as criminal prosecutions and interdictory or injunctive relief may result. However, often propaganda does not meet these thresholds. In these instances, MIL strategies and campaigns and fact-checking, coupled with the publication of counter-narratives or counter-disinformation, are effective remedies.[429]

CONCLUSION

The advent of the internet and the proliferation of false news and misinformation occasioned by the increased use of social media platforms is a primary contemporary concern. It fuels political polarisation and impacts a plethora of fundamental rights, including the right to freedom of expression, equality, and free and fair elections. However, absent unprotected speech, the remedies to combat misinformation are, at this stage, largely social and educational. MIL strategies and campaigns, coupled with

[426] Accessible at: https://www.real411.org/.
[427] Accessible at: https://padre.org.za/.
[428] Article 20 of the ICCPR, read with article 4(a) of CERD.
[429] See, for example, the UK Government Communications Services, 'RESIST: Counter-disinformation toolkit' (accessible at: https://www.fundacioncarolina.es/wp-content/uploads/2020/11/Toolkit-UK.pdf.

fact-checking and the publication of counter-narratives, remain the primary vanguard in the fight for the truth.

Module 9

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

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 9

NATIONAL SECURITY

- **"National security" is one of the most common justifications offered by states for limiting freedom of expression by journalists, bloggers, and media organs. However, it has the potential to be relied upon to quell dissent and cover up state abuses.**
- **National security legislation can have wide-reaching implications for media freedom and can be used to avoid constitutional checks and balances.**
- **The Johannesburg and the Tshwane Principles, alongside the Siracusa Principles, provide guidance on the extent of the national security limitation in relation to media freedom although they only constitute non-binding international law.**
- **Recent instances of terrorism have caused international decision-makers to seek to better define terrorist activities in order to ensure that justifiable limitations of fundamental rights relating to terrorism are properly prescribed by law.**
- **Prior restraint, even on the grounds of national security, is unlikely to succeed in a legal challenge as a result of the precedent set by the United States Supreme Court in the *Pentagon Papers* case.**

INTRODUCTION[430]

"National security" is one of the most common justifications offered by states for limiting freedom of expression by journalists, bloggers, and media organs. It is a legitimate restriction on fundamental rights and freedoms in the International Covenant on Civil and Political Rights (ICCPR)[431] and the African Charter on Human and Peoples' Rights (ACHPR),[432] provided it is not misused. While the ACHPR does not contain an explicit national security limitation on freedom of expression, article 9 does state that it is to be exercised "within the law" and article 29(3)states that an individual has a general duty "not to compromise the security of the State whose national or resident he is."[433]

[430] This module should be read in conjunction with Richard Carver 'Training Manual on International and Comparative Media and Freedom of Expression Law at pp 76-86 (accessible here: https://www.mediadefence.org/resources/mldi-manual-on-freedom-of-expression-law/)
[431] International Covenant on Civil and Political Rights (1966) at articles 19, 21 and 22 (accessible at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx).
[432] African Charter on Human and Peoples' Rights (ACHPR), at articles 3, 11, 12, 27 (1981) (accessible at: https://au.int/en/treaties/african-charter-human-and-peoples-rights).
[433] *Id.*

It is therefore a matter of debate how the legitimacy of a limitation on freedom of expression on grounds of national security should be assessed. Exceptionally, the right to freedom of expression can be partly or wholly suspended — a process known as *derogation* — because of a grave, imminent security threat. However, the national security limitation also has the potential to be relied upon to quell dissent and cover up state abuses.

This module examines how the derogation process is treated under international and regional human rights law.

THE DEROGATION PROCESS UNDER INTERNATIONAL AND REGIONAL HUMAN RIGHTS TREATIES

Most of the key human rights instruments allow a temporary derogation from certain human rights obligations in situations of national emergency. For example, article 4 of the ICCPR states:

> "In a time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin."[434]

Article 4 then proceeds to list a number of articles that may not be derogated from, even in times of public emergency. These include the rights not to be enslaved or tortured, and the right to freedom of opinion. It does not, however, include article 19, the right to freedom of expression.

The United Nations Human Rights Committee (UNHRCtte) has devoted two of its General Comments to explaining, in detail, the meaning of article 4 and the procedure and scope of derogation. The more recent of these, General Comment No. 29, can be taken as an authoritative interpretation of derogation during states of emergency. There are a number of key points to note, which can be applied equally to other human rights treaties that provide for derogation:

- The state of emergency must be publicly proclaimed according to domestic legal requirements, and should also accompanied by notification to other State Parties and (via the UN Secretary General or other body that serves as the technical secretariat of the treaty), explaining why it is necessary.[435]
- The situation leading to derogation must be "a public emergency which threatens the life of the nation."[436] In terms of General Comment No. 29, the threshold of threatening "the life of the nation" is a high one, and the UNHRCttee has been highly critical of

[434] ICCPR above n 2 at article 4.
[435] United Nations Human Rights Council, 'General Comment No. 29, states of emergency (article 4)' at para. 2 (2001) (accessible at: https://digitallibrary.un.org/record/451555?ln=en).
[436] *Id*.

derogations that have taken place in situations that appear to fall short of the article 4 requirements.[437]

- The UNHRCtte emphasises the importance of the principle that derogations should be limited "to the extent strictly required by the exigencies of the situation."[438] Even in instances when derogation may be warranted, there should only be derogation from those rights that are strictly required and only to the extent necessary.

The ACHPR, on the other hand, does not contain a clause explicitly permitting derogation during a public emergency. However, many states who are nevertheless party to the ACHPR have adopted constitutions or legislative measures that do contain derogation clauses, contrary to the position of the ACHPR and the African Commission.[439] For example, article 24 of the Bill of Rights in the Constitution of Kenya states that:

> "A right or fundamental freedom in the Bill of Rights shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom."

However, the High Court of Kenya decided that "protecting national security carries with it the obligation on the State not to derogate from the rights and fundamental freedoms guaranteed in the Constitution."[440]

The absence of a derogation clause in the ACHPR has caused controversy amongst legal scholars, some of whom argue that a derogation clause provides important protections against state abuse of freedoms during a public emergency,[441] while others claim its omission has enabled the positive development of human rights norms in Africa.[442]

LIMITING MEDIA FREEDOM ON GROUNDS OF NATIONAL SECURITY

Despite the above provisions in international law that allow the exercise of the right to freedom of expression to be limited on grounds of national security, provided that this is explicitly provided by law and that the restriction is necessary and proportional in an open and democratic society, in practice, national security is one of the most problematic areas of interference with media freedom.

One difficulty is the tendency on the part of many governments to assume that it is legitimate to curb all public discussion on national security issues. Yet, according to international standards, expressions may only be lawfully restricted if they threaten actual damage to national security.

---

[437] *Id* at para. 3.
[438] *Id* at para. 4.
[439] Abdi Jibril Ali, 'Derogation from Constitutional Rights and Its Implication Under the African Charter on Human and Peoples' Rights' *Law, Democracy & Development*, Vol. 17 (2013) (accessible at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2399789).
[440] Kenya Court of Appeal, Petition 628 of 2014 (2015) (accessible at: http://kenyalaw.org/caselaw/cases/view/106083/).
[441] Melkamu Aboma Tolera, 'Absence of a derogation clause under the African Charter and thsse position of the African Commission' (2013) (accessible at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/bahirdjl4&div=14&id=&page=).
[442] Jibril Ali above at n10.

In South Africa, the Protection of State Information Bill (known as the Secrecy Bill) was ardently opposed by media and civil society for many years for likely having "a chilling effect on the media and [probably stopping] many whistleblowers from leaking sensitive or embarrassing information to the media."[443] Constitutional scholar Pierre de Vos, argued that although this was a side effect of the Bill, its real intent was to:[444]

> "[Shield] the various intelligence agencies and structures from too much scrutiny and [ensure] that the ordinary constitutional checks and balances that apply to other organs of state that exercise public power would not apply to the intelligence services."

The Secrecy Bill is an example of how national security legislation can both unintentionally or intentionally stifle media freedom. Likewise, Kenya's anti-terrorism regime, including most notably the 2018 Prevention of Terrorism Amendment Bill, have been criticised for undermining human rights in an effort to protect national security.[445]

The Johannesburg Principles

In 1995, a group of international experts drew up the Johannesburg Principles on Freedom of Expression and National Security.[446] Although non-binding, these principles are frequently cited (notably by the UN Special Rapporteur on freedom of expression) as a progressive summary of standards in this area. The Johannesburg Principles address the circumstances in which the right to freedom of expression might legitimately be limited on national security grounds, at the same time as underlining the importance of the media, and freedom of expression and information, in ensuring accountability in the realm of national security.

In 2013, a group of civil society organisations from across the globe — including many who were involved in the drafting of the Johannesburg Principles — published an updated version known as the 'Tshwane Principles.'[447] The Tshwane Principles state that:[448]

---

[443] Pierre de Vos, 'Secrecy Bill less about media freedom, more about national security state,' on Constitutionally Speaking (2012) (accessible at: https://constitutionallyspeaking.co.za/secrecy-bill-less-about-media-freedom-more-about-national-security-state/).
[444] *Ibid*.
[445] Freedom House, 'Kenya's Antiterrorism Strategy Should Prioritize Human Rights, Rule of Law' (2018) (accessible at: https://freedomhouse.org/sites/default/files/2020-02/Final_PolicyBriefKenya_11_14_18.pdf).
[446] Article 19: Global Campaign for Free Expression, 'The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information,' (1996) (accessible at: https://www.article19.org/wp-content/uploads/2018/02/joburg-principles.pdf).
[447]Open Society Justice Initiative, 'Understanding the Global Principles on National Security and the Right to Information' (2013) (accessible at: https://fas.org/sgp/library/tshwane-und.pdf).
[448] Open Society Justice Initiative, 'The Tshwane Principles on National Security and the Right to Information: An Overview in 15 Points' (accessible at: https://www.justiceinitiative.org/publications/tshwane-principles-national-security-and-right-information-overview-15-points#:~:text=Related%20Work-,The%20Tshwane%20Principles%20on%20National%20Security%20and%20the%20Right%20to,and%20national%20law%20and%20practices).

- Governments may legitimately withhold information in some narrowly defined areas, such as defence plans, weapons development, and the operations and sources used by intelligence services.
- Information about serious human rights violations may not be classified or withheld.
- People who disclose wrongdoing or other information of public interest (whistleblowers and the media) should be protected from any type of retaliation, provided they acted in good faith and followed applicable procedures.
- Disclosure requirements apply to all public entities, including the security sector and intelligence authorities.

Although the principles do not constitute binding international law, they were developed with wide consultation and have broad consensus; for example, they have been welcomed by all three of the special experts on freedom of expression — for the UN, the Organisation of American States (OAS), and the African Union (AU), as well as the Organisation for Security and Cooperation in Europe's (OSCE) expert on freedom of the media.[449]

THE SCOPE OF NATIONAL SECURITY

"Freedom of expression" and "national security" are very often seen as principles or interests that are inevitably opposed to each other. Governments often invoke national security as a rationale for violating freedom of expression, particularly media freedom. Yet national security remains a genuine public good — and without it, media freedom would be scarcely possible. On the other hand, governments are seldom inclined to recognise that media freedom may actually be a means to ensure better national security by exposing abuses in the security sector. In South Africa, for example, media revelations about abuse in the police and military led to some reforms that arguably make for improved national security.[450]

The Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR (Siracusa Principles) define a legitimate national security interest as one that aims "to protect the existence of the nation or its territorial integrity or political independence against force or threat of force."[451] Subsequent articles indicate that a national security limitation "cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order."

The UN Special Rapporteur on Freedom of Expression has repeatedly limited the scope of a national security limitation in similar terms. For example:

---

[449] Open Society Justice Initiative above n 18.
[450] Katie Trippe, 'Pandemic policing: South Africa's most vulnerable face a sharp increase in police-related brutality' for Atlantic Council, (2020) (accessible at: https://www.atlanticcouncil.org/blogs/africasource/pandemic-policing-south-africas-most-vulnerable-face-a-sharp-increase-in-police-related-brutality/).
[451] United Nations Economic and Social Council, 'Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights,' Principle 29 (1985) (accessible at: https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf).

> "For the purpose of protecting national security, the right to freedom of expression and information can be restricted only in the most serious cases of a direct political or military threat to the entire nation."[452]

In a similar vein, the Johannesburg Principles define a national security interest as being:

> "To protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government."[453]

TERRORISM

Since the terror attacks in the United States on 11 September 2001, much of the focus of security legislation has been on countering terrorism. In part, this reflects a genuine change in understanding the nature of the threat to national security — seen also in the notion that terrorism or terrorist organisations are the objects of a "war." More generally, it serves as a rhetorical device whereby dissent — including critical media coverage — may be characterised as giving succour to terrorists.

The UN Security Council has required member states to take a number of steps to combat terrorism. One measure of particular relevance to the media is contained in Resolution 1624 of 2005, which was the first international instrument to address the issue of incitement to terrorism. The preamble to Resolution 1624 condemns "incitement to terrorist acts" and repudiates "attempts at the justification or glorification (*apologie*) of terrorist acts that may incite further terrorist acts."[454]

Defining terrorism

One serious problem with legal restrictions on glorification (or even incitement) of terrorism is the lack of any commonly accepted definition of terrorism in international law. Early counter-terrorism treaties focused on the criminalisation of particular acts, such as hijacking aircraft, without using the term terrorism. Later treaties, such as the International Convention for the Suppression of Financing of Terrorism,[455] do offer a definition, although this has no binding character beyond signatories to the treaty.

Many states, as well as entities such as the European Union, additionally define terrorism with reference to certain organisations "listed" as terrorist entities. This may hold particular dangers for the media in reporting the opinions and activities of such organisations. The United Nations Special Rapporteur (UNSR) on counter-terrorism and human rights has offered

---

[452] UN Special Rapporteur on Freedom of Expression, 'Report of the Special Rapporteur on the nature and scope of the right to freedom of opinion and expression, and restrictions and limitations to the right to freedom of expression,' (1995) (accessible at: https://www.ohchr.org/en/issues/freedomopinion/pages/annual.aspx).
[453] Johannesburg Principles above no. 17 at Principle 2(a).
[454] UN Security Council, Resolution 1624 of 2005, (2005) (accessible at: http://unscr.com/en/resolutions/1624).
[455] International Convention for the Suppression of Financing of Terrorism, article 2(1) (1999)

a definition of terrorism, based upon best practices worldwide, which focuses on the act of terror rather than the perpetrator:[456]

> "Terrorism means an action or attempted action where:
>
> 1. The action:
>   a. Constituted the intentional taking of hostages; or
>   b. Is intended to cause death or serious bodily injury to one or more members of the general population or segments of it; or
>   c. Involved lethal or serious physical violence against one or more members of the general population or segments of it; and
> 2. The action is done or attempted with the intention of:
>   a. Provoking a state of terror in the general public or a segment of it; or
>   b. Compelling a Government or international organization to do or abstain from doing something; and
> 3. The action corresponds to:
>   a. The definition of a serious offence in national law, enacted for the purpose of complying with international conventions and protocols relating to terrorism or with resolutions of the Security Council relating to terrorism; or
>   b. All elements of a serious crime defined by national law."

Sometimes expression on its own is deemed a threat to national security — and these situations are addressed under incitement. For more detail on incitement, see Module 6 of this series on Hate speech.

Terrorism and internet shutdowns

General Comment No. 34 on the ICCPR states that the media plays an important role in informing the public about acts of terrorism, and it should be able to perform its legitimate functions and duties without hindrance.[457] While governments may argue that internet shutdowns are necessary to ban the spread of news about terrorist attacks to prevent panic or copycat attacks, the UNSR on freedom of expression has instead found that maintaining connectivity may mitigate public safety concerns and help restore public order.[458]

At a minimum, if there is to be a limitation of access to the internet, there should be transparency regarding the laws, policies and practices relied upon, clear definitions of terms such as 'national security' and 'terrorism', and independent and impartial oversight being exercised.

---

[456] UN Special Rapporteur on the promotion and protection of human rights while countering terrorism, 'Statement by the Special Rapporteur on the promotion and protection of human rights while countering terrorism at the International Seminar Terrorism and human rights standards: Santiago de Chile, Chile' (2011) (accessible at: https://newsarchive.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=11737&LangID=E).
[457] UN Human Rights Council, 'General Comment no. 34 at para 46 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).
[458] UN Human Rights Council, '2017 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' at para. 14 (2017) (accessible at: https://www.undocs.org/A/HRC/35/22).

PRESCRIBED BY LAW

If national security is to be used to limit freedom of expression, the restriction must not only address a legitimate national security interest but must also be prescribed by law. The exact meaning of this has been an issue in several national security-related cases.

In *Chavunduka and Choto v. Minister of Home Affairs & Attorney General*, the Zimbabwe Supreme Court considered the case of two journalists who had been charged with publishing false news on the strength of an article reporting that an attempted military coup had taken place. The Court found that false news was protected by the constitutional guarantee of freedom of expression stating that "[p]lainly embraced and underscoring the essential nature of freedom of expression are statements, opinions and beliefs regarded by the majority as false."[459]

The offence of publishing false news in the Zimbabwean criminal code was vague and over-inclusive. It included statements that "might be likely" to cause "fear, alarm or despondency" — without any requirement to demonstrate that they actually did so. In any event, as the Court pointed out: "almost anything that is newsworthy is likely to cause, to some degree at least, in a section of the public or a single person, one or other of these subjective emotions."[460]

The word "false" was vague, since it included any statement that was inaccurate, as well as a deliberate lie. The law did not require it to be proved that the defendant knew the statement was false. The Court then went on to find the provision unconstitutional on necessity grounds as well.

NECESSARY IN A DEMOCRATIC SOCIETY

Most cases involving national security restrictions tend to be decided based on necessity. One area where restrictions may fall down is if they are overbroad. This was the issue in the before the UNHRCtte in the case of *Mukong v Cameroon*. Albert Mukong was a journalist and author who had spoken publicly, criticising the president and Government of Cameroon.[461] He was arrested twice under a law that criminalised statements “intoxicat[ing] national or international public opinion.”

The government justified the arrests to the UN Committee on national security grounds. The Committee disagreed, finding that laws of this breadth that "muzzled advocacy of multiparty democracy, democratic tenets and human rights" could not be necessary.[462]

The African Commission on Human and Peoples' Rights (ACHPR) has taken similar positions. In *Constitutional Rights Project and Civil Liberties Organisation v Nigeria*, opponents of the annulment of the 1993 presidential elections, including journalists, had been arrested and

---

[459] Supreme Court of Zimbabwe, Civil Application No. 156/99 (2000) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/chavunduka-v-minister-home-affairs/).
[460] *Id*.
[461] United Nations Human Rights Commission, Communication No. 458/1991 (1994) (accessible at: http://hrlibrary.umn.edu/undocs/html/vws458.htm).
[462] *Id* at para 9.7.

publications were seized and banned.[463] The African Commission said that no situation could justify such a wholesale interference with freedom of expression.

Various bodies have found that the burden is on the government to show that a restriction on freedom of expression is necessary. Courts have also insisted that there must be a close nexus between the restricted expression and actual damage to national security or public order.

In *CORD v Republic of Kenya*, the Kenya High Court eloquently explained the fundamental nature of human rights, and that they are not to be regarded as transitory:

> "It must always be borne in mind that the rights and fundamental freedoms in the Bill of Rights are not granted by the State and therefore the State and/or any of its organs cannot purport to make any law or policy that deliberately or otherwise takes away any of them or limits their enjoyment, except as permitted by the Constitution. They are not low-value optional extras to be easily trumped or shunted aside at the altar of interests perceived to be of greater moment in moments such as this."[464]

PRIOR RESTRAINT IN NATIONAL SECURITY CASES

There is a general presumption in international law against prior restraint of freedom of expression as unnecessary and disproportionate, on the grounds that it has a chilling effect on the enjoyment of the right to freedom of expression. Principle 23 of the Johannesburg Principles provides that: "[e]xpression shall not be subject to prior censorship in the interest of protecting national security, except in time of public emergency which threatens the life of the country."[465] It is notable that this principle explicitly acknowledges that in cases of national security interests, there may be a strong argument for the need to step in to stop the dissemination of information prior to publication.

In a landmark judgment in June 2020, the Economic Community of West African States (ECOWAS) Court of Justice ruled that the September 2017 internet shutdown ordered by the Togolese government during ongoing protests in that country was illegal and an affront to the applicants' right to freedom of expression.[466]

This was also the question that the United States Supreme Court confronted in *New York Times Co. v United States*[467] — better known as the "Pentagon Papers" case. The government sought prior restraint on publication of a large stash of documents — 47 volumes of them — labelled "top secret" and leaked from the Department of Defense.

---

[463] African Commission on Human and Peoples' Rights, Communication No. 102/93 (1998) (accessible at: https://africanlii.org/afu/judgment/african-commission-human-and-peoples-rights/1998/2).
[464] High Court of Kenya, Petition no.628 of 2014 (2015) (accessible at: http://kenyalaw.org/caselaw/cases/view/106083/).
[465] Johannesburg Principles, above at no.17.
[466] Economic Community of West African States Community Court of Justice, Suit no. ECW/CCJ/APP/61/18 (2020) (accessible at: https://www.accessnow.org/cms/assets/uploads/2020/07/ECOWAS_Togo_Judgement_2020.pdf).
[467] United States Supreme Court, Case 403 US 713 (1971) (accessible at: https://www.law.cornell.edu/supremecourt/text/403/713).

The documents detailed the decision-making leading to the United States' involvement in the Vietnam war and the government sought to prevent publication because of alleged damage to national security and relations with other countries.

In a brief judgment rejecting the request for prior restraint, the Court drew on earlier judgments to note that prior restraint can only be allowed in extreme circumstances:

> "Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity" … The Government "thus carries a heavy burden of showing justification for the imposition of such a restraint."[468]

Individual opinions by the judges elaborated on this reasoning. Justice Hugo Black argued:

> "The word "security" is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment. The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security ... ."[469]

National security is also frequently relied upon as a reason for justifying an interference with access to the internet, which is seen as a form of prior restraint. While this may, in appropriate circumstances, be a legitimate aim, it also has the potential to be relied upon to quell dissent and cover up state abuses. (For more on this, see Module 3 of this series on access to the internet.)

The covert nature of many national security laws, policies and practices, as well as the refusal by states to disclose complete information about the national security threat, tends to exacerbate this concern.

CONCLUSION

National security remains one of the most common justifications offered by states for limiting freedom of expression by journalists, bloggers, and media organs. However, it has the potential to be used to quell dissent and cover up state abuses. Increasingly, courts are limiting the scope of application of national security laws as they are often vague and drafted to circumvent constitutional checks and balances. Activists, lawyers, and members of the media should, however, remain vigilant and test all national security-related laws for compliance with international law, including the Tshwane and Siracusa Principles.

[468] *Id.*
[469] *Id*.

Module 10

KEY PRINCIPLES OF INTERNATIONAL LAW AND FREEDOM OF EXPRESSION

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

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 10

INTRODUCTION TO LITIGATING DIGITAL RIGHTS IN AFRICA

- **The evolution of the internet and the practicalities of the spread of information online are creating new challenges for protecting human rights.**
- **Strategic litigation is a powerful tool to advance digital rights and it is increasingly being used in a variety of different and innovative ways.**
- **Litigating digital rights requires an understanding of how to develop an optimal litigation strategy based on core principles.**
- **Litigating at the various regional courts and forums in Africa is a promising strategy but requires lawyers to appreciate the jurisdiction and procedures of the various forums.**

INTRODUCTION

The internet is one of the most powerful tools for facilitating the receiving and imparting of information and ideas. It allows for instant sharing of volumes of information, across borders and to wide audiences. It enables individuals to engage with diverse views and perspectives, and to access an array of resources to assist them to formulate their own views.

While the internet and other technologies offer enormous opportunities, they also present particular challenges. The digital rights landscape is constantly evolving as new technologies develop, and as we increasingly test the ambit of the right to freedom of expression and other rights online.

Even though litigation can be a protracted and costly process, it can contribute, in a meaningful way, to the evolution of legal frameworks that truly ensure that human rights are respected, protected and promoted. Strategic and test case litigation is increasingly being used as a tool to advance freedom of expression and digital rights. Given the contemporary challenges to human rights online, there is a need for the increased utilisation of strategic litigation to hold both state and non-state actors accountable. This training module seeks to give an overview of some of the basic principles involved in litigation, as well as an overview of litigating in various courts across the African continent.

This module should be read in conjunction with the following resources:

- Module 6 : Litigating Digital Rights Cases in Africa, Media Defence Advanced Modules on Digital Rights and Freedom of Expression Online
- Media Defence Report Mapping digital rights and online freedom of expression in East, West, and Southern Africa.
- Media Defence manual on litigating freedom of expression cases in East Africa.
- Media Defence West Africa Regional Mechanisms Manual.
- Media Defence Digital Rights Litigation Guide.

FOUNDING JURISDICTION AND STANDING

Founding jurisdiction

Jurisdiction refers to determining the ability or competency of a court or forum to consider and decide a particular matter. Jurisdiction can either be based on geographic areas or on the type of legal issue. It can also be based on where the violation occurred. It is an important and well-established principle that needs be addressed early on in the development of a litigation strategy as it can have a significant impact on the direction of a case.

One challenge in litigating digital rights issues in Africa is that many cases may involve one of the major multinational technology platforms in some way. While the African Commission on Human and Peoples' Rights (ACHPR) has not yet fully reflected on the establishment of jurisdiction for big tech companies, there may be some insights to draw from cases brought against multinational oil companies across Africa. The case of *Friends of the Earth v Shell*[470] provides insight into how to establish jurisdiction when litigating cases involving multinational companies. A judge in the Netherlands agreed to allow a Dutch NGO and four Nigerian farmers to bring a compensation case against Shell for environmental degradation said to be caused by the company's operations in the Niger Delta.[471]

In South Africa, an ongoing case is seeking to compel Facebook to disclose the identity of a perpetrator who sent anonymous graphic threats to a 13-year old child on Instagram. While the applicant's lawyers argue that the relief she sought in this case is a generally-established principle of law, they say that since Facebook is incorporated in the United States of America and has made it difficult for users to contact the company directly has left them no choice but to pursue the matter in court.[472]

Establishing standing

[470] Business & Human Rights Resource Center, 'Shell lawsuit (re oil pollution in Nigeria)' (2010) (accessible at: https://www.business-humanrights.org/en/latest-news/shell-lawsuit-re-oil-pollution-in-nigeria/).
[471] The Guardian 'Shell must face Friends of the Earth Nigeria claim in Netherlands' (2009) (accessible at: https://www.theguardian.com/business/2009/dec/30/shell-oruma-alleged-pollution-claim).
[472] Daily Maverick, 'Anonymously threatened with gang rape and murder, SA teenager takes Facebook Inc to court to disclose perpetrator' (2020) (accessible at: https://www.dailymaverick.co.za/article/2020-07-24-anonymously-threatened-with-gang-rape-and-murder-sa-teenager-takes-facebook-inc-to-court-to-disclose-perpetrator/).

The doctrine of standing is commonly understood as the ability of a party to bring a matter to a particular court. This involves an evaluation of any existing applicable restrictions on whether an individual or a civil society organisation (CSO) can file a case. It usually boils down to a litigant establishing their interest in a matter: who they are, how they are affected, who they represent, or what interests they represent. To establish standing, a potential litigant needs to demonstrate to the court that there is a sufficient connection between the issue and their interest in the issue. Different courts and tribunals engage with standing differently. Standing is usually the first procedural hurdle that needs to be overcome, so it is important to ensure what the standing requirements are before committing to a litigation strategy.

GENERAL PRINCIPLES AND INTRODUCTION TO DIGITAL RIGHTS LITIGATION

What are digital rights?

It is now firmly entrenched by both the ACHPR[473] and the United Nations[474] (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. Digital rights are basically human rights in the digital era, comprising the rights that are implicated in our access to and use of technologies as well as how fundamental rights play out in the online environment.

The internet does give rise to particular challenges that need to be noted when considering litigation on digital rights issues. The ability to publish immediately on the internet and reach an expansive audience can create difficulties. For example, the borderless nature of the internet can make establishing the true identity of an online speaker more challenging, founding jurisdiction for a claim more complex, or achieving accountability for wrongdoing that has been perpetrated online more difficult. Moreover, it can be challenging to fully remove content once it has been published online, or to contain its impact and spread.

Nevertheless, while the new digital world has certainly created some new issues, there are many that can be readily dealt with by applying a reasonable approach to the established principles of law.

General principles in litigating digital rights

In addition to jurisdiction and standing, there are a number of procedural requirements that form an essential part of any litigation strategy.

---

[473] 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).

[474] 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).

Admissibility

Admissibility refers to the process applied by international human rights fora to ensure that only cases that need international adjudication are brought before them. The principle of admissibility requires that all local remedies are exhausted and that consideration be given to whether there are rules relating to prescription and whether the forum recognises the concept of ongoing harm. In effect, admissibility dictates that an attempt to resolve a matter domestically should have taken place before approaching a regional or international forum.

Representation

Different courts and fora might have different rules relating to legal representation. Sometimes legal representation is not required, but might be useful; other times, the court or forum might facilitate the provision of free legal aid. Representation does not always have to be legal and litigants can sometimes be represented by a person of their choice.

Amicus curiae

An *amicus curiae* is a 'friend of the court'. It is not a main party to the litigation but is accepted by the court or forum to join the proceedings to advise and assist it in respect of a question of law or other issues that affects the case in question. Interested parties usually need to apply to the court or forum requesting permission to intervene in the matter and typically need to prove that they have an interest in the matter, their submissions will be of use to the court or forum, and that they will not be repeating the arguments of the main litigants. Courts and fora usually have the discretion to grant or refuse an *amicus* application. It is worth noting that *amicus* interventions can be particularly useful when litigating digital rights matters as there is often a need for technical and expert analysis given the constant progression within the digital environment.

OVERVIEW OF REGIONAL AND CONTINENTAL COURTS

Litigating at the African Commission on Human and Peoples' Rights

The ACHPR is a quasi-judicial body that is empowered to make non-binding recommendations. It has three main functions:

- The protection of human and peoples' rights.
- The promotion of human rights.
- The interpretation of the African Charter on Human and Peoples' Rights (African Charter).

Beyond the obligation to consider reports submitted by states, and shadow reports submitted by CSOs regarding states' compliance with the African Charter, the ACHPR is empowered to

receive and consider communications, which are like complaints. Communications are the mechanism through which the ACHPR fulfils its function to protect the rights and freedoms guaranteed in the African Charter.

There are several stages involved in the communications process, which are governed by the Communication Procedure.

The ACHPR has broad standing provisions. Anyone can register a communication, including CSOs. This includes a state claiming that another state party to the African Charter has violated one or more of the provisions in the African Charter; CSOs (which do not need to be registered with the AU or have observer status); victims of abuses; or interested individuals acting on behalf of victims of abuses.[475]

The matter can also be brought for the public good, as class or representative actions under the *actio popularis* approach, which means that the author of a communication need not know or have any relationship with the victim. This is to enable victims of human rights violations on the continent to receive assistance from NGOs and individuals far removed from their locality.[476] Furthermore, it is not necessary for cases to be submitted by lawyers, although legal representation can be helpful. Rule 99(16) of the Rules of Procedure provides for the ACHPR to receive *amicus curiae* briefs on communications.

Once a communication has been successfully submitted, a decision by a simple majority of the eleven commissioners is needed for the ACHPR to be seized with a matter, and the ACHPR will then proceed to consider whether the communication is admissible in terms of article 56 of the African Charter, including that all local remedies were exhausted before submitting the communication.[477]

Following a confirmation of admissibility, the ACHPR will give the parties time to present their written arguments. The ACHPR tends to prefer deciding matters on the papers, and it is advisable to only insist on an oral hearing if there are exceptional circumstances to argue or an argument to make that is new to the ACHPR.

After an evaluation of the factual and legal arguments put forward, the ACHPR will make a determination on whether there has been a violation of the African Charter or not. If it finds a violation, a recommendation will then be made. The recommendations are not legally binding but can become binding if they are adopted by the African Union. The Secretariat of the

[475] For more on standing see Pedersen, 'Standing and the African Commission on Human and Peoples'
Rights' African Human Rights Law Journal (2006) (accessible at https://www.ahrlj.up.ac.za/pedersenm-p) and Mayer, 'NGO Standing and Influence in Regional Human Rights Courts and Commissions' Notre Dame Law School (2011) (accessible at https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1053&context=law_faculty_scholarship).
[476] For more on *actio popularis*, see *Article 19 v Eritrea* at the ACtHPR (2007) (accessible at: https://africanlii.org/afu/judgment/african-commission-human-and-peoples-rights/2007/79).
[477] For more on the criteria for exhausting local remedies, see *Sir Dawda K. Jawara v The Gambia* (2000) (accessible at: http://hrlibrary.umn.edu/africa/comcases/Comm147-95.pdf) and *SERAC v Nigeria* (2002) (accessible at: https://www.escr-net.org/sites/default/files/serac.pdf).

ACHPR typically issues correspondence reminding states that have been found to have violated provisions of the African Charter and calling on them to honour their obligations.

Commentary on the contribution of the ACHPR

Responding to Human Rights Violations in Africa Assessing the Role of the African Commission and Court on Human and Peoples' Rights (1987–2018)
International Human Rights Law Review (2018)

Manisuli Ssenyonjo has taken the following view in relation to the impact of the ACHPR:

> "While there is much progress still to be made, the African Commission has greatly contributed to the regional protection of human rights in Africa. The Commission has exposed human rights violations in most authoritarian African States. Through its decisions on communications, it has developed human rights jurisprudence in Africa on several aspects consistent with the jurisprudence of other human rights bodies. Nevertheless, the African Commission has only received and decided very few communications related to economic, social and cultural rights.
>
> Initially, it was thought the Commission would be unable to hold States accountable for violations of human rights and to provide reparations to victims. However, over the years the Commission has confronted human rights violations through its decisions on communications; adoption of resolutions, principles/guidelines, general comments, model laws and advisory opinions; special rapporteurs and working groups to deal with thematic human rights issues; conducting on-site visits; consideration of State reports and adoption of concluding observations; as well as the referral of communications to the African Court.
>
> Nevertheless, compliance with the Commission's 'requests' for provisional measures/letters of urgent appeals, decisions and recommendations of the Commission, as set out in the Communications and concluding observations on State reports, has been low."

Litigating at the African Court on Human and Peoples' Rights

The African Court has a mandate to adjudicate matters dealing with states' compliance with the African Charter and other instruments on the protection of human rights ratified by that state. It became operational in 2009.[478] It complements and reinforces the functions of the ACHPR, but has different procedures to the ACHPR, which are laid out in the African Court Protocol and the Rules of Court.

The relationship between the ACHPR and the African Court has been described as follows:

> "The African Commission can bring cases to the Court for the latter's consideration. In certain circumstances, the Court may also refer cases to the Commission, and may

[478] International Federation for Human Rights, 'Practical Guide: The African Court on Human and Peoples' Rights towards the Africa Court of Justice and Human Rights' (2010) (accessible at: https://www.fidh.org/IMG/pdf/african_court_guide.pdf).

> request the opinion of the latter when dealing with the admissibility of a case. The Court and the Commission have met and harmonised their respective rules of procedure, and institutionalised their relationship. In terms of their Rules, the Commission and the Court shall meet at least once a year, to discuss questions relating to their relationship."[479]

The Practice Directions Guide to Litigants provides guidance on filing a submission. Article 5 of the African Court Protocol indicates who can submit a case to the African Court, including state parties, African intergovernmental organisations, NGOs with observer status before the ACHPR and individuals, but only against states that have made a declaration accepting the competence of the African Court to receive such cases in accordance with article 34(6) of the African Court Protocol. In November 2018, The Gambia became the ninth country to allow NGOs and individuals to access the African Court directly.[480] However, in 2019, Tanzania withdrew the right of individuals and NGOs to directly file cases against it.[481]

In respect of legal representation, rule 22 of the Rules of Court provides that "[e]very party to a case shall be entitled to be represented or to be assisted by legal counsel and/or by any other person of the party's choice." *Amici curiae* are also permitted in the African Court in terms of rules 45(1) and 45(2) of the Rules of Court, and the process for doing so is contained in section 42-47 of the Practice Directions of the African Court.

At the African Court, jurisdiction needs to be established alongside the determination of admissibility, which is different to the ACHPR. Article 3 of the African Court Protocol and rule 26 of the Rules of Court stipulate the rules regarding jurisdiction.[482]

Ordinary sessions of the African Court are held every year in March, June, September and December, or at any other period as it may deem fit, and it may also hold extraordinary sessions. The African Court live streams and makes recordings of its hearings publicly available, which is an advantage for transparency as well as for potential litigants to understand its workings. The African Court consists of eleven judges, although a bench of seven judges constitutes a quorum.

The African Court, as a full judicial body with binding decision-making authority, is likely to grant more effective remedies than the ACHPR. It can order specific amounts of damages, give supervisory interdicts that require the state party to report on implementation of the remedy, and require positive action to guarantee non-repetition.[483]

---

[479] African Court on Human and People's Rights, 'Frequently Asked Questions' (accessible at https://en.african-court.org/index.php/faqs/frequent-questions).
[480] African Court on Human and Peoples' Rights 'The Gambia becomes the ninth country to allow NGOs and individuals to access the Court directly' (2018) (accessible at https://www.africancourt.org/en/index.php/news/press-releases/item/257-the-gambia-becomes-the-ninth-country-toallow-ngos-and-individuals-to-access-the-african-court-directly).
[481] Amnesty International, 'Tanzania: Withdrawal of individual rights to African Court will deepen repression' (2019) (accessible at https://www.amnesty.org/en/latest/news/2019/12/tanzaniawithdrawal-of-individual-rights-to-african-court-will-deepen-repression/).
[482] For more on jurisdiction, see *Konaté v. Burkina Faso* in the African Court (accessible at: https://en.african-court.org/images/Cases/Judgment/Judgment%20Appl.004-2013%20Lohe%20Issa%20Konate%20v%20Burkina%20Faso%20-English.pdf).
[483] For more on the African Court's deliberations on reparations, see the judgment from *Norbert Zongo and Others v Burkina Faso* (2015) (accessible at: https://en.african-

The African Court Protocol provides that "[t]he State Parties to the present Protocol undertake to comply with the judgment in any case to which they are parties within the time stipulated by the Court and to guarantee its execution". Failures by states to comply with judgments are noted in the African Court's report to the Assembly of the African Union in terms of article 31 of African Court Protocol.

Commentary on the African Court

Responding to Human Rights Violations in Africa Assessing the Role of the African Commission and Court on Human and Peoples' Rights (1987–2018)
International Human Rights Law Review (2018)

Manisuli Ssenyonjo has taken the following view in relation to the impact of the African Court:

> "First, [there is] limited direct access by individuals and NGOs to the Court due to a limited number of States that have accepted the Court's jurisdiction and allowed individuals and NGOs direct access to the Court…
>
> Second, the non-implementation of the Court's decisions, including refusals to implement, failure to inform the Court of what measures have been taken, and the slow pace or 'reluctance' to comply limits the Court's effectiveness… Thus, the ability of the AU organs to impose sanctions consistently on non-complying States is necessary in order to strengthen the credibility of the African Court's orders and judgments."

Litigating at the East African Court of Justice

The East African Court of Justice (EACJ) is a sub-regional court that is mandated to resolve disputes involving the East African Community and its member states. The EACJ was established by article 9 of the Treaty for the Establishment of the East African Community and is tasked with interpreting and enforcing it.[484] The East African Court of Justice Rules of Procedure (EACJ Rules) govern its functioning. The EACJ serves the East African Community (EAC), namely Burundi; Kenya; Rwanda; South Sudan; United Republic of Tanzania; and Uganda. It has a First Instance Division and an Appellate Division. The former administers justice and applies relevant law, while the latter confirms, denies or changes decisions taken by the former.

At the EACJ, a statement of reference is the equivalent of a claim or complaint in domestic litigation and includes allegations of a human rights violation made by a Partner State, the

court.org/images/Cases/Ruling%20on%20Reparation/Application%20No%20013-2011%20-%20Beneficiaries%20of%20late%20Norbert%20%20Zongo-Ruling%20on%20Reparation.PDF).

[484] For more see International Justice Resource Center 'East African Court of Justice' (accessible at: https://ijrcenter.org/regional-communities/east-african-court-of-justice/).

Secretary-General, or a legal or natural person. Articles 24 and 25 of the EACJ Rules provide for the lodging of a statement of reference.[485]

Rule 30(1) of the EACJ Rules provides that any legal or natural person who is resident in a partner state may bring a case to the EACJ to challenge the legality of any Act, regulation, directive, decision, and action of a Partner State or an institution of the Community on whether it is an infringement of the EAC Treaty. Cases could fall within the temporal jurisdiction of the EACJ if they occurred after the EAC Treaty came into force. Further jurisdictional requirements are set out in articles 27 and 30 of the EAC Treaty.[486] In terms of rule 36 of the EACJ Rules, *amici curiae* are allowed to apply to be involved in a matter.

In terms of admissibility, article 30(2) of the EAC Treaty requires references to be filed with the EACJ within two months of the alleged violation.[487] There is also no provision in the EAC Treaty that recognises the concept of continuing violations, but there is no requirement that all domestic remedies must be exhausted first before approaching the EACJ.[488]

Article 37 of the EAC Treaty allows for parties to be represented when they appear before the EACJ. Parties can be represented by an advocate entitled to appear before a superior court of any of the Partner States. Chapters VII and XII of the EACJ Rules and the User Guide provide for the procedures for hearing cases.

In terms of enforcement, article 44 provides, among others, that the rules of civil procedure applicable in the state in question will govern the execution of a judgment of the EACJ that imposes a pecuniary obligation.

For more information, see Media Defence's Manual on Litigating Freedom of Expression Cases in East Africa.

Litigating at the ECOWAS Community Court of Justice

The ECOWAS Community Court of Justice (ECOWAS Court) is the judicial body of the Economic Community of West African States (ECOWAS). The ECOWAS Court was established in terms of the Revised Treaty of the ECOWAS (Revised Treaty). Article 9(4) of

[485] See the EACJ User Guide for more information: https://eacj.org/wp-content/uploads/2014/05/User-Guide.pdf.

[486] It is necessary to note that the EACJ does not explicitly have jurisdiction over human rights matters. However, articles 6(d) and 7(2) of the EAC Treaty create scope for human rights matters to be brought before the EACJ. For more, see *Burundi Journalists' Union v Attorney General of the Republic of Burundi* (2015) (accessible at: https://www.eacj.org/?cases=burundi-journalists-union-vs-the-attorney-general-of-the-republic-of-burundi).

[487] In *Attorney General of Uganda and Another v Awadh and Others* (2011), the EACJ held that it would not be flexible on this requirement (accessible at: https://www.eacj.org/?cases=omar-awadh-and-6-others-vs-attorney-general-of-uganda).

[488] In *Democratic Party v Secretary-General and the Attorneys General of the Republics of Uganda, Kenya, Rwanda and Burundi* (2013), the EACJ held that this jurisdiction is not voluntary and that once an applicant can show an alleged violation of the EAC Treaty, the EACJ must exercise jurisdiction (accessible at: https://www.eacj.org/?cases=democratic-party-vs-the-secretary-general-east-african-community-and-the-attorney-general-of-the-republic-of-uganda-and-the-attorney-general-of-the-republic-of-kenya-and-the-attorney-general-of-the-r).

the ECOWAS Protocol, as amended by the ECOWAS Supplementary Protocol, formally recognises that the ECOWAS Court "has jurisdiction to determine cases of violation of human rights that occur in any Member State."

The mandate of the ECOWAS Court includes ensuring the observance of law and of the principles of equity in the interpretation and application of the provisions of the Revised Treaty and all other subsidiary legal instruments adopted by ECOWAS. It serves the ECOWAS member states: Benin, Burkina Faso, Cape Verde, Cote d'Ivoire, The Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Sierra Leone, Senegal and Togo. The ECOWAS Protocol, the ECOWAS Supplementary Protocol, and the Rules of the Community Court of Justice provide guidance on the procedures of the ECOWAS Court.

Article 11 of the ECOWAS Protocol sets out how cases may be filed to the ECOWAS Court. It has fairly broad standing provisions detailed in article 10 of the Revised Treaty, including that community institutions or their staff, individuals, corporate bodies, member states and the national courts of ECOWAS countries may approach it.[489] Applications from organisations acting on behalf of a group of people whose rights have been violated are also accepted.

Human rights cases must be brought within three years of the cause of action arising. In instances where violations are ongoing, it will give rise to a cause of action *die in diem* (day in and out) and postpones the running of time.

The ECOWAS Protocol and the Rules of the Community Court of Justice do not explicitly provide for *amicus curiae* briefs. However, in *Federation of African Journalists and Others v The Gambia*,[490] interveners were accepted as *amici curiae*. In that matter, the Court granted an application in terms of article 89 of the Rules of the Community Court of Justice, allowing the CSOs to join the suit as *amici curiae* interveners.

Admissibility at the ECOWAS Court is not as strictly applied as it is in the other courts; however, it is important to note that applications that are brought cannot be pending before another court of similar status. The ECOWAS Court does not require the exhaustion of domestic remedies but will neither hear matters that have been determined on the merits by domestic courts nor hold appellate jurisdiction over domestic courts.

The remedies available to the ECOWAS Court are similar to those offered at a domestic level. Remedies can include declarations and mandatory orders, but the ECOWAS Court does not have scope to create remedies and is accordingly limited to base the remedy on what was put before it by the parties.

The judgments of the ECOWAS Court are binding: the Member States are required to take immediate steps to comply with the remedy. Despite this, concerns have arisen regarding the

[489] See *Ocean King v Senegal* for more on how strictly adherence to the standing provision is applied by the ECOWAS Court (accessible at: http://www.worldcourts.com/ecowasccj/eng/decisions/2011.07.08_Ocean_King_Nigeria_Ltd_v_Senegal.pdf).
[490] ECOWAS Court Suit No. ECW/CCJ/APP/36/15 (2018) (accessible at: http://prod.courtecowas.org/wp-content/uploads/2019/02/ECW_CCJ_JUD_04_18.pdf).

legitimacy of the enforceability of the ECOWAS Court, as the power given by the ECOWAS Revised Treaty to heads of state and governments to impose sanctions has yet to be exercised.[491]

For more information, see Media Defence's Training Manual on Litigation of Freedom of Expression in West Africa.

The practicalities of litigating digital rights

1. **Determining a strategy.** There are three key tenets for every litigation strategy: procedural considerations, administrative capabilities, and substantive goals. These considerations are largely interdependent and need to be given equal consideration.
2. **Gathering evidence.** Different types of evidence can be useful for proving a case and provide clarification regarding the facts: this can include evidence of a violation, expert evidence, digital evidence and witness evidence and testimony. The rapidly evolving digital landscape is providing both opportunities and challenges in relation to the gathering of evidence. On the one hand, there is a large quantity of available digital information, whereas on the other hand, collecting and analysing the evidence can be challenging and technical.[492] The ordinary rules of evidence apply to digital evidence, which must still meet the minimum standards of relevance and reliability in order to be admitted.[493]
3. **Advocacy strategies**. Litigation alone is not enough to effect substantive change or effectively disrupt the status quo — advocacy is an essential component.[494] This can include social media campaigns, public awareness, parallel processes to other non-judicial fora, media statements, protests and any other creative activity that elevates the profile of the case, informs the public and tells a story.

CONCLUSION

Litigating digital rights involves some particular challenges related to the digital realm. However, jurisprudence is beginning to develop in domestic as well as regional courts that defends freedom of expression and information online. While some African regional courts struggle with enforcement of their rulings, and not all are easily accessible, they have demonstrated their willingness to rule to defend fundamental human rights, and provide an important avenue for using litigation to advance digital rights in Africa.

[491] For more, see Olisa Agbakoba Legal 'Enforcement of the Judgments of the ECOWAS Court' (2018) (accessible at: https://oal.law/enforcement-of-the-judgments-of-the-ecowas-court/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration).
[492] Human Rights Center UC Berkley School of Law 'Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court' (2014) (accessible at https://www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf).
[493] For more see UNODC E4J University Module Series: Cybercrime, 'Module 4: Introduction to Digital Forensics' (2019) (accessible at: https://www.unodc.org/e4j/en/cybercrime/module-4/index.html).
[494] See APC, 'Advocacy Strategies and Approaches' (accessible at: https://www.apc.org/en/advocacy-strategies-and-approaches-overview); Call Hub, 'Advocacy Strategies' (accessible at: https://callhub.io/advocacy-strategies/), and Call Hub, 'Grassroots Advocacy' (accessible at: https://callhub.io/grassroots-advocacy-definition-strategies-and-tools/.

For more comprehensive information on how to litigate digital rights in Africa, see Module 6 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online.