Module 1

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

ISBN 978-0-9935214-1-6
Published by Media Legal Defence Initiative: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in April 2024

TABLE OF CONTENTS

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 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.**

1. 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 has become 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, and soft law instruments, and is 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.

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.

[1] *Madanhire and Another v Attorney General* (2014) (accessible here).
[2] Statute of the International Court of Justice (1948) (accessible here) at Article 38, which documents the four recognised sources of international law.

2. KEY PRINCIPLES OF INTERNATIONAL LAW

2.1. 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; are interconnected and thus 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 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 for the creation of 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.

In 2023, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) was ratified by Mauritania, the 15th country to do so, thereby bringing the convention into effect. By ratifying treaties, states commit to putting in place domestic measures, such as legislation, to give effect to their treaty obligations.

2.2. 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 in which 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.

3. THE RIGHT TO FREEDOM OF EXPRESSION UNDER INTERNATIONAL LAW

3.1. Freedom of expression under international law

The United Nations was the first international entity to enshrine the right to freedom of expression in international law in 1948 with the UDHR. 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

[3] African Commission on Human and Peoples' Rights, 'State Parties to the African Charter' (accessible here).

regardless of frontiers."[4] This was the foundation of what later became Article 19 of the ICCPR. The rights contained under Article 19 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 right was further elaborated on in General Comment No. 34 by the UNHRCtte.[5] 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 rights;
- journalism, cultural and artistic expression, teaching, and religious discourse.[6]

It also embraces expressions that may be regarded by some as deeply offensive.[7] 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.[8]

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:

- the limitation must be provided for in law;
- it must pursue a legitimate aim; and
- it must be necessary for a legitimate purpose.[9]

---

[4] UN, 'Universal Declaration of Human Rights' (1948) (accessible here).
[5] See above n 4 at para 11.
[6] OHCHR, General Comment No. 34 (2011) (accessible here) at para 11.
[7] *Id*. 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) (accessible here) at pp 7-9.
[8] See above n 6 at para 12.
[9] 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' (2018) (accessible here) at pp 14-16. For more on proportionality see the 2002 decision of *Attorney-General v 'Mopa* in the Lesotho Court of Appeal (accessible here) and *Zimbabwe Lawyers for Human Rights & Associated Newspapers of Zimbabwe v Zimbabwe* in the ACHPR (2009) (accessible here).

This test applies similarly to limitations of the right to freedom of expression under other legal instruments, including the African Charter.

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 about 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."[10]

3.2. 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.[11]

In a 2016 resolution, the UN Human Rights Council (UNHRC) affirmed that:[12]

> "[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 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."

3.3 African regional standards

In 2016, the African Commission on Human and Peoples' Rights (ACHPR) affirmed the UNHRC's declaration and called on states to respect and take legislative and other measures

[10] UNHRCtte General Comment No. 25 (1996) (accessible here) at para 8.
[11] See above n 6 at para 12.
[12] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet' A/HRC/32/L.20 (2016) (accessible here) at para 1.

to guarantee, respect, and protect citizens' rights to freedom of information and expression through access to internet services.[13] This was supplemented in 2019 by the Declaration of Principles on Freedom of Expression and Access to Information in Africa adopted by the ACHPR, which recognises the role of new digital technologies in the realisation of the rights to freedom of expression and access to information, and also affirms that the same rights that people have offline should be protected online in accordance with international human rights law and standards.[14]

The 2019 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, whereas the 2002 Declaration mentioned it only in the Preamble.
- 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]
- It "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]

In 2023 the ACHPR, together with other international bodies, issued a Joint Declaration on Media Freedom of Democracy due to the concern about the impact of online platforms on media freedom and freedom of expression. This declaration provides recommendations to States to secure and facilitate the media's role as a vital institution and pillar of democracy, with particular attention to online media.[19]

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.[20] Most human rights treaties, including those dedicated to the protection of the rights of specific groups — such as

[13] ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa' ACHPR/Res.362, (2016) (accessible here).
[14] ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2019) (accessible here). The Declaration replaces the Declaration of Principles on Freedom of Expression in Africa which the African Commission adopted in 2002 (accessible here).
[15] ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa', Principle 37(2) (2019) (accessible here).
[16] International Justice Resource Center, 'New ACHPR Declaration on Freedom of Expression & Access to Information' (2020) (accessible here).
[17] ACHPR above n 11 at Principle 39(4).
[18] *Id* at Principle 42.
[19] ACHPR, 'Joint Declaration on Media Freedom and Democracy' (2023) (accessible here).
[20] See above n 7 at p 5.

women, children, and people with disabilities — also make explicit mention of freedom of expression.[21]

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.
- Second, the rise of the internet has upended the traditional information ecosystem. 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.[22]

Ethiopia has recently passed a controversial social media law that was criticised for restricting online speech, and Nigeria is attempting to do the same with the so-called 'Social Media Bill.'[23] In 2022, **South Africa's** Film and Publications Regulations came into force.[24] These Regulations have been heavily criticised as they essentially give an authority power to censor digitally distributed content. Other trends. such as the rise of disinformation and States' responses thereto, pose serious and increasing threats to freedom of expression online. Similarly, the increase in the use of sophisticated surveillance technology on mobile phones has given rise to restrictions on freedom of expression, particularly among journalists.[25]

4. JOURNALISM AND FREEDOM OF EXPRESSION

4.1. The changing role of journalists

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

[21] *Id.*
[22] For more see Washington Post, 'There's a worrying rise in journalists being arrested for 'fake news' around the world' (2019) (accessible here) and Freedom House, 'The Rise of Digital Authoritarianism: Fake news, data collection and the challenge to democracy' (2018) (accessible here).
[23] Al Jazeera 'Nigerians raise alarm over controversial Social Media Bill' (2019) (accessible here) and Al Jazeera, 'Ethiopia passes controversial law curbing 'hate speech' (2020) (accessible here).
[24] Business Tech 'New internet censorship regulations for South Africa' (2022) (accessible here).
[25] Forbidden Stories 'Journalists under surveillance' (2021) (accessible here).

more complicated and needs to be tailored to the new and evolving dynamics of the media ecosystem.

Nevertheless, General Comment No 34[26] 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[27] "[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." 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:[28]

> "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, state parties should take particular care to encourage an independent and diverse media."

Recently, the Constitutional 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 2021 case of *amaBhungane v Minister of Justice*.[29] In defending the right of journalists to protect the confidentiality of their sources and to be safe from surveillance, the judgment stated:

> "I agree that keeping the identity of journalists' sources confidential is protected by the rights to freedom of expression and the media. This Court has acknowledged the constitutional importance of the media in our democratic society, and has confirmed that "[t]he Constitution thus asserts and protects the media in the performance of their obligations to the broader society, principally through the provisions of section 16". It follows that the confidentiality of journalists' sources, which is crucial for the performance by the media of their obligations, is protected by section 16(1)(a)."[30]

---

[26] See above n 4.
[27] Report of the UNSR on Freedom of Expression to the UN General Assembly (UNGA), A/65/284 (2013) (accessible here) at para 21.
[28] See above n 4.
[29] *amaBhungane v Minister of Justice* (2021) (accessible here).
[30] *Id* at para 115.

In the earlier High Court judgment of the same case, the Court pertinently held that:

> "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."[31]

The proliferation of Strategic Lawsuits Against Public Participation (SLAPP) by political and corporate entities is becoming an increasingly prevalent threat to journalists. In **South Africa**, numerous instances of defamation and urgent proceedings have been employed in efforts to suppress activists and journalists:

- In the case of *Maughan v. Zuma*, former President Jacob Zuma initiated a private criminal prosecution against a journalist for an article she authored about him. However, the High Court, in dismissing Zuma's case, underscored the importance of protecting journalists from intimidation through SLAPP suits, affirming the fundamental freedoms of expression and the press.

- In *Mazetti Management Services v. Amabhungane*, a private company obtained an ex-parte and in-camera court order, compelling journalists to surrender documents and restraining them from reporting on the matter. Upon reconsideration, the High Court denounced this order as an abuse of the ex-parte procedure, citing international principles advocating for the protection of journalists from such misuse of legal and judicial processes.

While South African courts remain vigilant against SLAPP tactics, the persistence of powerful actors in seeking to silence dissent is anticipated. Fortunately, international, regional, and comparative legal frameworks offer valuable tools to counteract these attempts at intimidation and censorship.

4.2. New threats to journalism

The rise of social media and the internet has not only changed the environment in which journalists work and the role that they play in society, as well as the financial model that supports journalism as an industry, it has also given rise to a host of new threats to journalists and press freedom. The internet has become a central platform for the dissemination of journalistic content, as well as a primary mechanism through which journalists engage, on an individual and professional level, with their audiences. The proliferation of mis- and disinformation online has further exacerbated these trends by undermining the credibility of traditional media and creating toxic online communities in which journalists are forced to engage.

[31] *amaBhungane v Minister of Justice* (2017) (accessible here) at para 131.

Using competition and copyright law to ensure media sustainability

There is a new trend in media regulation, focusing on using competition and copyright regulation to ensure the sustainability of journalism, as a response to the growing challenges media faces in the digital age and to the dominance of large tech platforms, such as Google and Facebook. In 2024 in **South Africa**, the Competition Commission is conducting a media and digital platforms inquiry where it is exploring mechanisms for big tech platforms to fairly distribute online advertising revenue to media companies that argue that they produce the content that attracts users to these platforms.[32] Australia's News Media and Digital Platforms Mandatory Bargaining Code, although not yet in effect, is an example of a copyright reform used to require digital platforms to pay media for the use of their content on their platforms.[33]

4.3 Threats faced by women journalists

While all journalists are at risk of online violence and harassment, women journalists uniquely face this harassment due to their sex or gender and are particularly prone to it. A survey by the UN Educational, Scientific, and Cultural Organisation (UNESCO) found:

- Nearly three-quarters of women journalists have experienced online violence,
- 30% responded to online violence by self-censoring on social media. Black, indigenous, Jewish, Arab, and lesbian women journalists experienced both the highest rates and most severe impacts of online violence.
- 20% of women surveyed were physically attacked or abused offline in connection with online violence that they had experienced.[34]

The online assaults against women journalists represent a significant menace to their safety, gender parity, and press freedom.[35] These attacks, often orchestrated, sexually explicit, and malevolent, frequently focus on women belonging to religious or ethnic minorities, or individuals who identify as gender nonconforming.

The systemic harassment and abuse faced by women and gender minority journalists online have serious consequences for diversity and representation in the media by chilling the participation of diverse voices. It also results in physical, medical, psychological, professional, and other impacts in the real world that can be devastating.

As stated by UNESCO, such harassment "amounts to an attack on democratic deliberation and media freedom, encompassing the public's right to access information, and it cannot

[32] Competition Commission of South Africa 'Media and Digital Platforms Market Inquiry' (accessible here).
[33] Australian Competition and Consumer Commission 'News media bargaining code' (accessible here).
[34] UNESCO, The chilling global trends in online violence against women journalists' (2021) (accessible here).
[35] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on reinforcing media freedom and the safety of journalists in the digital age' (2022) (accessible here).

afford to be normalised or tolerated as an inevitable aspect of online discourse, nor contemporary audience-engaged journalism." It, therefore, amounts to a new and emerging threat to freedom of expression that can and should be addressed under existing international standards and human rights law.

In a significant and welcome development, the 2019 ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa (African Declaration) calls on states to guarantee the safety of journalists and media practitioners, and to "take specific measures to ensure the safety of female journalists and media practitioners by addressing gender-specific safety concerns, including sexual and gender-based violence, intimidation and harassment."[36]

The ACHPR in a 2022 Resolution further reaffirms that States must "[p]rotect women journalists from digital violence by repealing overly wide surveillance laws that perpetuate their vulnerability".[37] Further, the ACHPR in its 2023 Joint Declaration on Media Freedom and Democracy recommends to online platforms that they consider the disproportionate risks of online attacks faced by women journalists in their human rights impact assessments and recommends that States adopt comprehensive measures for the safety of journalists in a manner that integrates gender and intersectionality perspectives.[38]

5. 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 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."[39]

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.[40]

It should be noted that reference to "within the law" in article 9(2) of the African Charter should not be seen as permitting states to enact laws that violate the right to freedom of expression. The ACHPR made clear in *Constitutional Rights Project v Nigeria* 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."[41]

---

[36] ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (2019) (accessible here) at Principle 20.
[37] ACHPR, 'Resolution on the Protection of Women Against Digital Violence in Africa' ACHPR/Res.522 (2022) (accessible here).
[38] ACHPR, 'Joint Declaration on Media Freedom and Democracy' (2023) (accessible here).
[39] African Charter on Human and Peoples' Rights (1981) (accessible here).
[40] *Id.*
[41] *Constitutional Rights Project v Nigeria* (1998) (accessible here) at pp 57-58.

The right to freedom of expression is further underscored in the African Declaration and the ACHPR Guidelines on Freedom of Association and Assembly in Africa.[42] Nuanced aspects of the right to freedom of expression are explained and recommendations to States and other bodies in relation to these aspects in instruments such as the Resolution on the Deployment of Mass and Unlawful Targeted Communication Surveillance and its Impact on Human Rights in Africa,[43] and the Joint Declaration on Media Freedom and Democracy.[44]

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)[45],
- Revised Treaty of the Economic Community of West African States (ECOWAS),[46] and
- Protocol on Culture, Information and Sport of the Southern African Development Community (SADC).[47]

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[48] 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 provides a jurisprudence booklet on freedom of expression.[49]

6. 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.

[42] ACHPR, 'Guidelines on Freedom of Association and Assembly in Africa' (accessible here).
[43] ACHPR, 'Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa' (2023) (accessible here).
[44] ACHPR, 'Joint Declaration on Media Freedom and Democracy' (2023) (accessible here).
[45] See, for instance, *Burundi Journalists' Union v The Attorney General of the Republic of Burundi*, Reference No. 7 of 2013 (2015) (accessible here).
[46] Economic Community of West Africa States, 'Revised Treaty' (1993) (accessible here).
[47] Southern African Development Community, 'Protocol on Culture, Information and Sport' (2001) (accessible here).
[48] European Court of Human Rights, 'Guide on Article 10 of the European Convention on Human Rights' (2020) (accessible here). For more, see also the ECHR's Factsheets on Access to the Internet and Freedom to Receive and Impact Information and Ideas (accessible here), on Hate Speech (accessible here), on the Protection of Journalistic Sources (accessible here), and on the Protection of Reputation (accessible here).
[49] Inter-American Court of Human Rights, 'Cuadernillo de Jurisprudencia de la Corte Interamericana de Derechos Humanos nº 16: libertad de pensamiento y de expresión' (accesible here in Spanish).

Module 2

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

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

Originally published in November 2022
Revised in April 2024

TABLE OF CONTENTS

MODULE 2

INTRODUCTION TO DIGITAL RIGHTS

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

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

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

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

1. INTRODUCTION

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

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

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

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

2. WHAT ARE DIGITAL RIGHTS?

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

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

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

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

Examples of digital rights issues

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

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

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

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

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

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

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

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

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

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

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

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

3. WHAT IS AN INTERNET INTERMEDIARY?

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

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

Examples of internet intermediaries are:

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

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

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

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

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

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

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

3.1. Laws on the limitation of intermediary liability

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

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

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

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

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

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

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

4. THE BORDERLESS ENJOYMENT OF FREEDOM OF EXPRESSION

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

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

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

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

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

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

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

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

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

5. THE RIGHT TO FREEDOM OF EXPRESSION ONLINE

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

Challenges to freedom of expression online

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

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

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

6. CONCLUSION

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

Module 3

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

ISBN 978-0-9935214-1-6
Published by Media Legal Defence Initiative: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in April 2024

TABLE OF CONTENTS

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 have rarely been found to constitute a justifiable limitation.**

- **National security is frequently relied upon as the justification for 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 when 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.**

1. IS THERE A RIGHT TO THE INTERNET UNDER INTERNATIONAL LAW?

The internet has transformed the free flow of information, empowering anyone with an internet connection to gather and share information and ideas, thereby profoundly impacting the exercise and protection of the triad of information rights: privacy, freedom of expression, and access to information.[1] The United Nations Human Rights Council's (UNHRC) 2016 Resolution on the promotion, protection, and enjoyment of human rights on the internet affirmed that these rights are essential for the full realization of other fundamental rights and should be safeguarded with equal rigour in the online sphere as they are offline.

However, notwithstanding this affirmation, 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 the right of access to the internet are numerous.

[1] ARTICLE 19, 'Digital Rights' (accessible here).

In 2023, the United Nations High Commissioner for Human Rights stated that it may be time to reinforce universal access to the internet as a human right, and not just a privilege.[2]

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:

- the ability to see and disseminate content online; and
- the ability to use the physical infrastructure to enable access to such online content.

In 2003, UNESCO was among the first international bodies to call on states to take steps to realise the right of access to the internet. In this regard, it stated that:[3]

> "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 the 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 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."[4]

1.1. The UN Sustainable Development Goals

This has been expanded upon in the United Nations 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

[2] United Nations Human Rights Office of the High Commissioner 'It May be Time to Reinforce Universal Access to the Internet as a Human Eight, Not Just a Privilege, High Commissioner tells Human Rights Council' (2023) (accessible here).
[3] UNESCO, 'Recommendation concerning the promotion and use of multilingualism and universal access to cyberspace' (accessible here) at paras 7 and 15.
[4] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet' (2012) (accessible here) at para 2. This was expanded upon further the following year in UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet' (2014) (accessible here).

divide and to develop knowledge societies."[5] 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,[6] and to strive to provide universal and affordable access to the internet in least-developed countries by 2020.[7]

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 providing and expanding access to the internet.[8] Notably, it affirms the importance of applying a comprehensive rights-based approach in providing and expanding access to the internet[9] 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.[10]

Status of the SDG goal around internet access

The SDGs call on states to enhance the use of ICTs and other enabling technologies to promote the empowerment of women,[11] and to strive to provide universal and affordable access to the internet in least developed countries by 2020.[12] At the end of 2020, it was clear that this goal had not been met, with more than 3.5 billion people still without internet access. In 2023 33% of the global population did not have internet access, which was an improvement from the previous year.[13] In Africa internet access varies largely between countries, illustrating the inequitable access to the internet.[14]

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 been firmly 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 at both the individual and state levels, inadequate locally-relevant content, insufficient levels of digital literacy, and a lack of political will to make this a priority.

[5] UNGA, 'Transforming our world: The 2030 agenda for sustainable development' A/Res/70/1, 21 October 2015 (accessible here) at para 15.
[6] *Id* at goal 5(b), p 18.
[7] *Id* at goal 9(c), p 21.
[8] UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', (2016) (accessible here) at para 2.
[9] *Id* at para 5.
[10] *Id* at para 12.
[11] *Id* at goal 5(b), p 18.
[12] *Id* at goal 9(c), p 21.
[13] International Telecommunication Union 'Facts and Figures 2023: Internet Use' (2023) (accessible here).
[14] Statista 'Share of internet users in Africa as of January 2023, by country' (2023) (accessible here).

2. INTERFERENCES WITH ACCESS TO THE INTERNET

Some of the ways in which access to the internet is interfered with are 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, access to education, 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.[15] 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 and Political Rights (ICCPR) has been interpreted as providing for an effective prohibition on most forms of prior restraint on speech.[16] 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.

3. 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.[17] 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.[18] This is sometimes also referred to as a 'kill switch.' Shutdowns remain a pressing concern:

- In 2022, 187 internet shutdowns access 35 countries were recorded.[19]
- Between January and May 2023, Access Now recorded 80 internet shutdowns in 21 countries.[20]

The scope and scale of a shutdown may vary:

- In some instances, this may entail there being a total network outage, whereby access to the internet is shut down in its entirety.
- In others, it may be access to mobile communications, websites, or social media and messaging applications that are blocked, throttled, or rendered effectively unusable.[21]

---

[15] Council of Europe, 'Prior Restrains and Freedom Of Expression: The Necessity of Embedding Procedural Safeguards in Domestic System' (2018) (accessible here).
[16] 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 398.
[17] Access Now, 'What is an internet shutdown?' (accessible here).
[18] *Id.*
[19] Access Now 'Who is shutting down the internet in 2023? A mid-year update' (2023) (accessible here).
[20] *Id.*
[21] UNHRC, 'Report of the UNSR on Freedom of Expression' (2017) (accessible here) at para 8.

- Shutdowns may affect an entire country, specific towns or regions within a country, or even multiple countries, and have been seen to range from several hours to several months.[22]

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.[23] As noted by the United Nations Special Rapporteur on Freedom of Expression (UNSR on FreeEx), 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.

Jurisprudence on internet shutdowns

- In a landmark case confirming that internet shutdowns constitute a form of prior restraint and an unjustifiable infringement on freedom of expression, in June 2020, the Economic Community of West African States (ECOWAS) Community Court of Justice (ECOWAS Court) ruled in *Amnesty International v. Togo* that the internet shutdowns implemented by the **Togolese** government in 2017 were illegal.[24] In the judgment, the ECOWAS Court held that access to the internet is a "derivative right" as it "enhances the exercise of freedom of expression" and as such is "a right that requires protection of the law."

- In a similar case in 2022 relating to the blocking of specific content, rather than a wholesale internet shutdown, the ECOWAS Court in *SERAP v. Federal Republic of Nigeria* considered the government of **Nigeria's** banning of social media platform Twitter, underscoring that modern technology has enabled the exchanges of ideas, views, and opinions and thus furthers freedom of expression, and held that access to Twitter is a "derivative right" that is "complementary to the enjoyment of the right to freedom of expression."[25]

- In 2023, the **Colombian** Constitutional Court held in *Bejarano v. Ministry of Defense* that the government had violated the rights to freedom of expression, association and assembly due to their failure to provide petitioners with timely, truthful, and complete information about internet shutdowns during public protests that occurred in 2021.[26] The Court ordered the State to respond publicly on these issues.

- In 2023 the ECOWAS Court held, in *Association des Blogueurs de Guinée and Others v The State of Guinea*, that States not only have an obligation to not interfere with the right to freedom of expression – they also must adopt all necessary measures to give effect to it.[27] By shutting down the internet amidst protests concerning the President

[22] *Id.*
[23] *Id.*
[24] *Amnesty International Togo v The Togolese Republic* (2020) (accessible here).
[25] *SERAP v. Federal Republic of Nigeria* (2022) (accessible here).
[26] Global Freedom of Expression: Columbia University, '*Bejarano v. Ministry of Defense*' (2023) (accessible here).
[27] *Association des Blogueurs de Guinée and Others v The State of Guinea*, ECW/CCJ/JUD/38/23/22 (2023) (accessible here).

of **Guinea's** amendment of the Constitution, the State infringed upon the Applicants' rights to freedom of expression.

4. 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."[28]

There have been several examples of blocking and/or filtering across the continent:

- In 2023 **Gabon** was reported as having blocked access to social media platforms on the day of elections. 4 days later, access was restored along with the announcement by military officers that they had taken over power of the country.[29] Gabon is unfortunately far from the only African country to implement such techniques in recent years.
- Similar social media blocks have been implemented over election times in **Zambia**,[30] **Uganda**,[31] and **Cameroon**.[32]
- In 2018, after an extensive period of blocking a long list of websites, including media outlets and prominent websites known for their reporting on protests in the country, the **Ethiopian** government unblocked 264 websites, although instances of blocking of social media occurred again in 2022.[33]
- In 2021, the **Eswatini** government ordered all operators to suspend access to certain social media sites as they were being used to "spread misinformation" contributing to violence around the country.[34] However, this and other internet disruptions at the time are reported to have been ordered in order to quell pro-democracy protests and reports about police brutality.[35]

[28] ARTICLE 19, 'Freedom of expression unfiltered: How blocking and filtering affect free speech' (2016) (accessible here) at p 7.
[29] Netblocks, 'Internet cut in Gabon on election day' (2023) (accessible here).
[30] Netblocks, 'Social media and messaging apps restricted in Zambia on election day' (2021) (accessible here).
[31] Netblocks, 'Social media and messaging restricted, internet shut down for Uganda elections' (2021) (accessible here).
[32] Netblocks, 'Facebook and WhatsApp restricted in Cameroon on eve of election results' (2018) (accessible here).
[33] Freedom on the Net, 'Ethiopia' (2022) (accessible here).
[34] MISA, 'Eswatini shuts down internet as protests rock monarchy' (2021) (accessible here).
[35] Access Now, 'Eswatini authorities shut down internet to quell protests, ask people to email grievances' (2021) (accessible here).

5. 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.[36] In other words, it promotes the idea that ISPs should treat all data that travels over their networks fairly, without improper discrimination in favour of a particular application, website, or service.[37] Discrimination in this regard may relate to halting, slowing or otherwise tampering with the transfer of any data, except for a legitimate network management purpose, such as easing congestion or blocking spam.[38]

The 2017 Report of the UNSR on FreeEx describes two key ways in which net neutrality may be compromised:[39]

- **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, while other services or applications are subject to metered cost.

In various countries around Africa, there has been significant debate about access to zero-rated content, particularly as social networking sites have begun to 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 provide critical free information on topics of public importance. For example, zero-rating was used extensively during the COVID-19 pandemic in South Africa to enable wider access to public health information about the disease and its prevention.[40] On the other hand, critics argue that zero-rating can lead to unfair competition and distort users' perceptions by only allowing access to particular sites, thereby limiting access to information.[41]

The 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa (African Declaration) protects network neutrality by calling on states to require internet intermediaries to enable access to all internet traffic equally and not to interfere with the free flow of information by giving preference to particular internet traffic.[42] In 2021 the UN Human Rights Council adopted a resolution that calls upon States to ensure net neutrality and prohibit attempts by internet service providers to discriminate between content.[43]

---

[36] See above n 21 at para 23.
[37] Electronic Frontier Foundation, 'Net neutrality' (accessible here).
[38] American Civil Liberties Union, 'What is net neutrality?' (accessible here).
[39] See above n 21 at paras 24-28.
[40] ISPA, 'Press Release : ISPA Helps Consumers Verify Zero-Rated Websites in SA' (2020) (accessible here).
[41] For a discussion on zero-rating in Africa, see Research ICT Africa, 'Much ado about nothing? Zero-rating in the African context' (2016) (accessible here).
[42] ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019' (2019) (accessible here) at Principle 39.
[43] ARTICLE 19, 'UN: Human Rights Council adopts resolution on human rights on the Internet' (2021) (accessible here).

6. LIMITATION OF TE RIGHT TO FREEDOM OF EXPRESSION

In 2016, the UNSR on FreeEx 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".[44] 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 of these limitations:[45]

> "(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.
> (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.[46] 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".[47]

As set out in General Comment No. 34:[48]

> "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."

---

[44] UNHRC, 'Report of the UNSR on Freedom of Expression' (2016) (accessible here) at para 22.
[45] International Mechanisms for Promoting Freedom of Expression, 'Joint declaration on freedom of expression and the internet' (2011) (accessible here).
[46] See above n 21 at para 8.
[47] UNHRC, 'The promotion, protection and enjoyment of human rights on the internet' (2016) (accessible here) at para 10.
[48] UNHRC 'General comment No. 34 Article 19: Freedoms of opinion and expression' (2011) (accessible here).

The African Declaration also calls on states not to condone or engage in any disruption of access to the internet or other digital technologies, and not to interfere with the rights to freedom of expression and access to information "through measures such as the removal, blocking or filtering of content, unless such interference is justifiable and compatible with international human rights law and standards."[49]

The UNSR on FreeEx 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.[50] 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.[51] In some countries, this has led to the government enacting new laws to expressly allow for shutdowns to take place.[52]

The UNSR on FreeEx has further noted that network shutdowns invariably fail to meet the standard of necessity,[53] and are generally disproportionate.[54] States frequently seek to justify this on the grounds of national security, which is discussed further below. For example, **Chad** blocked social media for a period of 472 days in 2018,[55] ostensibly for security reasons. A case was filed against two internet providers,[56] but access was restored shortly after.

Litigating the internet shutdown in Cameroon

In January 2020, the Internet was shut down in regions of Cameroon following protests against the arrest of civil society leaders resisting government efforts to impose the Francophone legal and education systems in predominantly Anglophone regions.[57] The internet remained shut down for 93 days and was switched back on hours after Veritas Law filed a legal challenge with the Constitutional Council, with the assistance of Media Defence.[58] The constitutional challenge was brought to compel the government to restore the Internet so that the Constitutional Council could prevent the government from shutting the Internet down in the future. Although the matter was eventually dismissed for lack of

[49] See above n 42 at Principle 38.
[50] See above n 21 at para 9.
[51] *Id* at para 10.
[52] 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 here for instance.
[53] See above n 21 at para 14.
[54] *Id* at para 15.
[55] Quartz Africa 'Chad has now spent a full year without access to social media' (2019) (accessible here).
[56] Africa News 'Chadian lawyers challenge ongoing social media shutdown' (2018) (accessible here).
[57] Access Now 'Victory in Cameroon: after 94 days, the internet is back on' (2017) (accessible here).
[58] *Id.*

locus standi, it is an example of the potential positive impact of litigious efforts to hold the perpetrators of internet shutdowns to account, even where a positive judgment cannot be achieved.[59]

6.1. Justified limitations on freedom of expression

In relation to the blocking and filtering of content, there may indeed be circumstances where such measures are justifiable, such as websites distributing child sexual assault material (CSAM). Such measures are still required to meet the three-part test for a justifiable limitation, which must be assessed on a case-by-case basis.[60]

Similarly, limitations to network neutrality may also be permissible in certain circumstances, for example for legitimate network management purposes, or in circumstances in which zero rating is implemented fairly and transparently by public authorities with a mandate to do so and for a valid purpose. 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.[61] 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.[62]

6.2. Trends in Africa

It should also be noted that other, increasingly sophisticated ways to limit and control access to the internet and online content are also on the rise in Africa. This includes the adoption of social media taxes that increase prices for users and legal mandates for online publishers to register or obtain licenses, sometimes including all social media users. In Benin, the government attempted to introduce a tax that specifically targeted the use of social media networks. This sparked thousands to use the hashtag 'TaxePasMesMo' (don't tax my megabytes) and ultimately led to the tax being removed.[63] In 2021, **Nigeria's** Information Minister stated that social media firms wanting to operate in Nigeria must obtain a local license. Critics have commented that this comes amidst a broader campaign against freedom of expression.[64]

7. NATIONAL SECURITY AS A GROUND OF JUSTIFICATION

National security is frequently relied upon as the justification for interference with access to the internet, as well as other interferences with the right to freedom of expression.[65] While this

[59] *Id.*
[60] For more on the three-part test, refer to Media Defence 'Advanced Module 2 on Digital Rights' and 'Freedom of Expression Online', which deal with restricting access and content.
[61] See above n 45 at para 5(a).
[62] *Id* at para 5(b).
[63] Internet without Borders '#TaxePaMesMo: A Campaign to Cancel the Facebook Tax in Benin' (2018) (accessible here).
[64] Arab News 'Nigeria demands social media firms get local license' (2021) (accessible here).
[65] For a fuller discussion on national security more broadly see Richard Carver 'Training Manual on International and Comparative Media and Freedom of Expression Law' (accessible here) at pp 77-88.

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 decisions, as well as the refusal by states to disclose information about particular national security threats, 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:[66]

> "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 9(3) of the African Declaration provides that national security, public order, or public health are legitimate aims for a limitation on freedom of expression, but only if it is prescribed by law and necessary and proportionate. This means that it should:

> "(a) originate from a pressing and substantial need that is relevant and sufficient;
> (b) have a direct and immediate connection to the expression and disclosure of information, and be the least restrictive means of achieving the stated aim; and
> (c) be such that the benefit of protecting the stated interest outweighs the harm to the expression and disclosure of information, including with respect to the sanctions authorised."

7.1. Principles governing the Intersection of freedom of expression and national security

In 1995, a group of international experts drew up the Johannesburg Principles on Freedom of Expression and National Security, [67] which were endorsed by the then UNSR on FreeEx.[68] 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 some which were involved in the drafting of the Johannesburg Principles, published an updated version known as the Tshwane Principles. As set out in the Tshwane Principles:[69]

[66] Report of the UNSR on freedom of expression to the UNGA, A/HRC/23/40, 17 April 2013 (accessible here) at para 60.
[67] Principle 2 of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, November 1996 (accessible here). 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.
[68] 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 here).
[69] Open Society Justice Initiative, 'The Tshwane Principles on National Security and the Right to Information: An Overview in 15 Points' (2013) (accessible here).

- 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.
- Disclosure requirements apply to all public entities, including the security sector and intelligence authorities.
- 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.

Although not binding, the principles were developed with wide consultation and have received wide consensus from various international and regional bodies.[70] 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.

7.2. Counter-terrorism

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.[71] 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.[72]

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.

8. INTERMEDIARY LIABILITY

Intermediary liability occurs when 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.[73] This can occur in various circumstances, including:

- copyright infringements;
- digital piracy, trademark disputes;
- network management;
- spamming and phishing;

[70]Open Society Justice Initiative ‘Understanding the Global Principles on National Security and the Right to Information’ (2013) (accessible here).
[71] See above n 48 at para 46.
[72] See above n 21 at para 14.
[73] Alex Comninos, ‘The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain’ (2012) (accessible here) at p 6.

- cybercrime
- defamation;
- hate speech;
- child sexual exploitation material;
- illegal content;
- offensive but legal content;
- censorship;
- broadcasting and telecommunications laws and regulations; and
- privacy protection.[74]

A report published by UNESCO identifies the following challenges facing intermediaries:[75]

- Limiting the liability of intermediaries for content published or transmitted by third parties is essential to the flourishing of internet services that facilitate expression.
- 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.[76] The African Declaration provides in Principle 39 that states should not require internet intermediaries to "proactively monitor content which they have not authored or otherwise modified" and to ensure that in moderating online content human rights safeguards are mainstreamed and all such decisions are transparently made with the possibilities for appeals and other remedies. It further provides that where law enforcement agencies request the immediate removal of online content because it poses an imminent risk of harm, such requests should be subject to judicial review.[77]

---

[74] *Id*.
[75] Rebecca MacKinnon et al, 'Fostering freedom online: The orle of internet intermediaries' (203) (accessible here) at pp 179-180.
[76] See above n 45at paras 2(a)-(b).
[77] See above n 42 at Principle 39.

8.1. Jurisprudence around the world

While questions around intermediary liability have not yet been thoroughly considered by courts in Africa, a substantial body of jurisprudence is building up in other regions of the world, particularly Europe, Latin America, and India. For example, in 2023 the **Malaysian** Communications and Multimedia Commission (MCMC) announced that it would take legal action against Meta for what it saw as a failure to promptly remove content deemed harmful.[78] This reportedly included matters related to race, royalty, religion, and instances of defamation, impersonation, online gambling, and fraudulent advertisements. Digital rights advocates argued that the MCMC's threat of legal action against a social media platform for its content moderation decisions poses a potential risk to intermediary liability principles and online freedom of expression.[79]

The **European Court of Human Rights** (ECtHR) has considered intermediary liability in several cases:

- In *Delfi AS v Estonia*, the ECtHR examined the liability of an internet news portal for offensive comments posted by readers on its website.[80] The ECtHR ruled that holding the portal liable did not violate its right to freedom of expression, as the comments were highly offensive, the portal failed to prevent their publication, profited from them, and allowed anonymity for their authors.

- In M*agyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*, the ECtHR addressed the liability of an internet news portal and a self-regulatory body for vulgar comments on their platforms.[81] While recognizing the duty of internet news portals to assume responsibilities, the ECtHR found that the comments did not constitute unlawful speech, upholding the right to freedom of expression.
- In *Sanchez v France*, the ECtHR departed from its previous decisions on imposing liability on social media users for third party content.82 Sanchez, a French politician, was fined by a French domestic court for failing to remove hateful comments against the Muslim community from his Facebook wall. Before the ECtHR, Sanchez argued that this fine violated his right to freedom of expression by requiring him to bare the disproportionate burden of monitoring all comments posted on his open and public Facebook wall. The Court ultimately held that Sanchez's right to freedom of expression had not been violated – France had interfered with it in a lawful and necessary manner, in a democratic society and to pursue a legitimate aim. It held that it was not disproportionate to attribute liability to all actors involved, including Sanchez for failing to take action in relation to blatantly discriminatory comments. Importantly, the Court held that Sanchez's duty to act reasonably was greater in his capacity as a politician.

[78] Malaysian Communications and Multimedia Commission, 'Non-cooperation to remove undesirable contents from its platform: MCMC to take legal action against Meta' (2023) (accessible here).
[79] ARTICLE 19 'Malaysia: Halt legal action against Meta over content moderation' (2023) (accessible here).
[80] Application No. 64569/09, 10 October 2013 (accessible here).
[81] Application No 22947/13, 2 February 2016 (accessible here).
82 Sanchez v. France (45581/15) (2023) (accessible here).

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.[83]

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.[84]

8.2. Non-consensual dissemination of intimate images

The case of the non-consensual dissemination of intimate images (NCII), provides a challenge with regard to questions of intermediary liability. Courts around the world have frequently ordered the immediate and unequivocal removal of such content from online platforms, citing the significant and adverse consequences on victims' and survivors' rights to privacy and dignity.

- The High Court of Delhi, **India,** for example, ordered that intermediaries must remove all offending content from their platform in the case of NCII and not just the specific links provided by victims. The Court highlighted the damage caused by the posting of NCIIs and how victims being required to search the internet for new uploads for the purpose of requesting their removal can cause further trauma.[85]

- In an earlier case, the same Court ordered the immediate removal of content not only from the website on which it had been published, without consent but also ordered search engines to de-index the content from their search results, stressing the need for "immediate and efficacious" remedies for victims of such cases.[86]

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

[83] *Shreya Singhal v Union of India*, Application No. 167/2012 (accessible here).at paras 112-118.
[84] *María Belén Rodriguez v Google*, Fallo R.522.XLIX (accesible here). The decision has been described in the 2016 Report of the UNSR on Freedom of Expression at para 52.
[85] *Mrs X v. Union of India* (2023) (accessible here).
[86] *X v. Union of India* (2021) (accessible here).

on a shutdown.[87] However, this can only truly be realised in circumstances where intermediaries are able to do so without fear of sanction or penalties.

At the same time, it is vital that appropriate remedies are established for the removal of illegal or harmful content, and that powerful private platforms are held accountable for the decisions they make with regard to moderating content in the digital sphere, where such decisions may infringe on the rights to freedom of expression and access to information.

9. THE RIGHT TO BE FORGOTTEN

This also relates to a concept known as 'the right to be forgotten,' which supporters argue creates an obligation on internet intermediaries to delete certain content at the request of a person who is the subject of such content. At present, the issue is being considered in multiple jurisdictions as the appropriate balance is sought between protecting the right to privacy and dignity and the right to access information of public importance. For example:

- The Supreme Court of **Argentina** in 2022 rejected a petition by an anchor-women to have Google de-index embarrassing content from her past, as it considered this to be an extreme measure that would restrict the flow of public interest information. It held that the mere passing of time did not render the information irrelevant.[88]

- The **Italian** Supreme Court held in 2019 that a newspaper had violated the right to be forgotten of a man who had been convicted of murder 27 years before by publishing an article about it and enabling his identification. It held that any re-evocation of the past without a connection to current events must be done in such a way that anonymizes the person involved when they do not play a relevant public role.[89]

- The ECtHR in 2021 confirmed a district **Italian** Court's decision that a publisher's decision not to remove and de-index an online article when requested to do so, given the facts at hand, constituted a violation of the requestor's right to reputation. In this matter, the article in question described a fight in a restaurant and the criminal proceedings that ensued. The editor failed to remove and de-index the article upon request from the subject of the article. The ECtHR held that the district court's decision did not violate the publisher's right to freedom of expression, and upheld the damages that had been awarded against the editor.90

- Similarly, the ECtHR held in 2023 that an order to anonymise an article in a newspaper's electronic archive did not breach the publisher's right to freedom of expression. The article referred to a person's involvement in a fatal traffic accident for which they were subsequently convicted. The ECtHR upheld the **Belgium** court's decision, and emphasised that a person who is not a public figure may acquire notoriety though a criminal act. However, that this may declare as time goes on and, consequently, they

[87] See above n 21 at para 50.
[88] *Natalia Denegri v. Google Inc*., Supreme Court (2022) (accessible here).
[89] *S.G. v. Unione Sarda S.P.A*. (2019) (accessible here).
90 *Biancardi v. Italy*, case no.: 77419/16 (2021) (accessible here).

may be able to rely on the right to be forgotten in order to go back to someone who is unknown to the public.91

10. 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 is being leveraged equally by those seeking to defend fundamental rights and those seeking to limit them. An informed 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.

91 Hurbain v. Belgium, application no.: 57292/16 (2023) (accessible here).

Module 4

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

ISBN 978-0-9935214-1-6
Published by Media Legal Defence Initiative: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in April 2024

TABLE OF CONTENTS

MODULE 4

DATA PRIVACY AND DATA PROTECTION

- **The right to privacy and data protection is a growing concern due to increasing data flows and the resulting need for the protection of personal information.**
- **In the African context, there has been progress with the passage of several new data protection laws in recent years, and the coming into force of the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention).**
- **The right to be forgotten continues to be an issue of contestation through the courts, although case law in Africa is limited.**
- **Nevertheless, attacks against encryption and anonymity continue, and there are many new threats to privacy and data protection including the expansion of surveillance capabilities and the growth of artificial intelligence (AI).**
- **Journalistic activity warrants particular protections from threats to encryption as well as communications surveillance by both state and private actors because of the special risks this poses for freedom of expression due to the potential disclosure of confidential sources and the risk of a chilling effect on media freedom.**

1. INTRODUCTION

The right to privacy and the concomitant requirement to protect personal information has become increasingly relevant in the information age. As access to the internet has expanded and many parts of public and private life have become increasingly digitised, there has been a sharp increase in online information-sharing and data collection, with the associated risk that this information can be accessed and abused by hostile actors. At the same time, legislative developments have failed to keep pace and adequately protect personal information. However, in recent years, the passing of data protection legislation by many African states, as well as the development of guidelines and instruments by regional and continental bodies, have provided some protections to remedy and vindicate the privacy rights of African peoples.

This module focuses on the right to privacy in the digital age in Africa by evaluating the state of data protection, the related concepts of the 'right to be forgotten' and encryption assesses the growing risks of government and commercial surveillance as well as the emerging challenges of the use of artificial intelligence (AI) to perpetrate privacy violations, and sets out emerging principles and safeguards in this rapidly advancing digital environment.

2. THE RIGHT TO PRIVACY

Around the world, there is an increasing recognition that the right to privacy is vital both in itself and due to its role in facilitating the right to freedom of expression. For instance, the right to privacy allows individuals to share views anonymously in circumstances where they may face repression or discrimination for those views; it also allows whistle-blowers to make protected disclosures and enables journalists and activists to communicate securely beyond the reach of unlawful government interception. It is also an inherent part of the right to dignity.

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 the right to privacy is not explicitly contained in the African Charter on Human and Peoples' Rights (African Charter), article 9 of the Charter does encode protections for the right to receive information and express opinions:

> "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."

These, in addition to the African Charter's protections for freedom against discrimination, liberty and security, freedom of assembly, health, and others, have prompted the argument that the implicit right to privacy should be 'read into' the African Charter as an inalienable component of those other rights.[1]

'Reading in' the right to privacy: the example of India

While this approach has not been tested in relation to the African Charter, it would follow the approach of the Supreme Court of India in its 2017 ruling 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.[2] 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.

[1] Ayalew, 'Untrodden Paths Towards the Right to Privacy in the Digital Era under African Human Rights Law' *12 International Data Privacy Law 1* (2022) (accessible here).
[2] *Justice K.S. Puttaswamy and Another v Union of India and Others*, Petition No. 494/2012 (2017) (accessible here).

The right to privacy of children is, however, explicitly contained in other regional and continental instruments. For example, article 10 of the African Charter on the Rights and Welfare of the Child (ACRWC) 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 revised 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa, adopted by the African Commission on Human and Peoples' Rights (ACHPR), also explicitly acknowledges the right to privacy and calls on states to provide extensive protections for privacy and personal information.[3] Moreover, all but one African state guarantees this right under their domestic constitutions.[4]

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:[5]

> "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 of the internet on the enjoyment of this right.

3. DATA PROTECTION

Data protection is one of the primary ways through which the right to privacy is given effect. At least 36 African states have so far enacted data protection laws, and more are in the process of doing so.[6] In addition to giving effect to the right to privacy, data protection legislation also facilitates trade among 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. Framed more positively, data protection laws enable the regulated transfer of personal information across borders where both jurisdictions have put in place adequate data protection laws and procedures to protect data subjects' rights.

---

[3] ACHRP, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019' (2019) (accessible here) at Principles 40-42.
[4] ALT Advisory, 'Data Protection Africa,' (accessible here).
[5] *NM and Others v Smith and Others*, [2007] ZACC 6 (accessible here) at para 33, citing with approval *Bernstein and Others v Bester NO and Others*, [1996] ZACC 2 (accessible here) at para 77.
[6] See https://dataprotection.africa/ for more information.

3.1. Key data protection principles

Data protection laws are aimed at protecting and safeguarding the processing of personal information (also sometimes called personal data). Personal information is typically defined as 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, also sometimes called the responsible party, can typically be either a public or private body and is the person or entity responsible for processing personal information about the data subject.

Key data protection principles

Most comprehensive data protection laws in Africa make provision for a core set of principles which can be summarised as follows:[7]

- 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 was collected.
- 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.
- Personal information must be processed in accordance with the rights of data subjects provided for under the data protection law.
- The data controller must take appropriate technical and organisational measures 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 addition, most data protection laws establish a regulatory body to monitor and enforce the provisions of the law: this type of regulatory body is often referred to as a data protection authority (DPA).

3.2. International law standards

The United Nations Special Rapporteur (UNSR) on the Right to Privacy released a report in 2022 providing an in-depth analysis of the principles of legality, lawfulness and legitimacy, consent, transparency, purpose, fairness, proportionality, minimisation, quality, responsibility,

[7] Information Commissioner's Office, 'A guide to the data protection principles' (accessible here).

and security in the context of data protection legislation, which serves as a seminal guide for the development and harmonisation of data protection regulations around the world.[8]

In relation to the protection of personal information, General Comment No. 16 on Article 17 of the ICCPR (General Comment No. 16) provides as follows:[9]

> "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 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."

In 2023, in response to the rapid and widespread collection of personal information ostensibly to combat the COVID-19 pandemic from 2020-2022, the UNSR on Privacy released a report elaborating on the implementation of the principles of purpose limitation, deletion of data and demonstrated or proactive accountability in the processing of personal data collected by public entities in the context of the pandemic.[10]

3.3. Regional law standards

There are several African regional instruments that deal with data protection:

- **The African Union (AU) Convention on Cyber Security and Personal Data Protection 2014**[11] (the 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. After finally receiving ratification from the required 15th state, the Malabo Convention came into force in 2023.[12]

[8] UNSR on Privacy, 'Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms' (2022) (accessible here).
[9] UNHCHR, 'CCPR General Comment No. 16: Article 17 (Right to Privacy)' (1988) (accessible here) at para 10.
[10] UNSR on Privacy, 'A/HRC/52/37: Implementation of the principles of purpose limitation, deletion of data and demonstrated or proactive accountability in the processing of personal data collected by public entities in the context of the COVID-19 pandemic - Report of the Special Rapporteur on the right to privacy' (2023) (accessible here).
[11] AU, 'African Union Convention on Cyber Security and Personal Data Protection' (2014) (accessible here).
[12] ALT Advisory, 'Africa: AU's Malabo Convention set to enter force after nine years' (2023) (accessible here).

- **EAC Legal Framework for Cyberlaws 2008**[13] (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 inform the development of their laws. Data protection is dealt with briefly in paragraph 2.5 of the EAC Legal Framework, as part of Phase I which was adopted by the EAC Council of Ministers in 2010.[14]

- **Supplementary Act on Personal Data Protection within ECOWAS 2010**[15] (ECOWAS Supplementary Act): This instrument is designed to be directly transposed into a domestic context among West African states and provides in detail the conditions for the lawful processing of personal information and the rights of data subjects. Importantly, it is also legally binding on ECOWAS States. ECOWAS also adopted the Directive on Fighting Cyber Crime in 2011 in an effort to harmonise member states' cybercrime legislation.

- **SADC Data Protection Model Law 2013**[16] (SADC Model Law): This is a model law that can be adapted into domestic contexts among southern African states. It seeks to ensure the harmonisation of information and communications technologies (ICT) policies and recognises that ICT developments impact the protection of personal data, including in government and commercial activities. It also deals with whistle-blowing, by providing that the data protection authority must establish rules to govern the whistleblowing system that preserve 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 often further facilitate a right of access to information, by providing 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 determine whether their personal information is being processed in line with applicable data protection laws and whether their rights are being upheld.

Mapping the state of data protection in Africa

Given the importance of data protection legislation in protecting the right to privacy in the digital age, as well as the rapid progression of legislation and regulation in this area, it can be hard to keep up to date with the state of data protection in Africa. Data protection is an open, online resource that aims to provide a detailed analysis of the governance of data protection across the continent, mapping and analysing the legislation in place in all 55 member states of the African Union.

As of February 2024, it notes that 36 out of the 55 AU-recognised states have passed data protection legislation, with three draft bills also being under consideration.

[13] EAC, 'EAC Legal Framework for Cyberlaws' (20228) (accessible here).
[14] UNCTAD, 'Harmonizing Cyberlaws and Regulations: The experience of the East African Community' (2012) (accessible here).
[15] ECOWAS, 'Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWS' (2010) (accessible here).
[16] HIPSSA, 'Data Protection: SADC Model Law' (2013) (accessible here).

3.4. Emerging challenges to data protection

As more states across the continent have passed data protection legislation, so too have the risks and challenges of regulating and protecting privacy in the digital age become more complex. Many states, particularly those in West Africa, passed their laws some time ago,[17] raising concerns that they may no longer be suited to the challenges of the modern age. In South Africa, for example, the Protection of Personal Information Act was passed in 2013 but only came into effect in July 2020 with a further grace period given for full compliance. This has raised concerns among critics that the Act already requires amendments to stay up to date with new issues such as AI.[18]

In addition, the enforcement challenges of these many new data protection laws have become increasingly apparent. For example, research has found that 14 countries' laws provide for the data protection authority to be established within or to receive instructions from another public body, such as a government ministry, raising questions about regulatory independence.[19] 11 countries were found not to have adequate protections in place to prevent the undue removal of members of the Authority for political or other reasons.[20]

Enforcement challenges: example from Kenya

Many data protection authorities across the content have struggled to meaningfully hold accountable violators of data protection legislation, particularly powerful multinational corporations.

For example, in 2023, Tools for Humanity piloted a new cryptocurrency campaign called Worldcoin that paid people a small sum of money in the cryptocurrency to have their biometric data collected, resulting in thousands taking up the opportunity,[21] with very little information about how the data would be used. In May, **Kenya's** Office of the Data Protection Commissioner (OPDC) ordered the company to halt processing,[22] an order which was reportedly ignored. The company finally stopped data collection only when, in August, the Ministry of the Interior ordered the suspension of Worldcoin's operations in the country, citing data protection concerns.[23] The OPDC subsequently launched litigation against Tools for Humanity in the High Court.[24]

This demonstrates the challenges data protection authorities face in holding these powerful international companies to account.

[17] Data Protection Africa, 'Standing Alone: The Independence of African Data Protection Authorities' (2024) (accessible here).
[18] IT Web, 'POPIA principles must align with AI governance, say experts,' (2023) (accessible here).
[19] See above n 17.
[20] *Id*.
[21] Njenga, Schmitz, 'Worldcoin: Thousands flock KICC to have eyeballs scanned for Ksh.7k' (2023) (accessible here).
[22] TechCrunch, 'Worldcoin ignored initial order to stop iris scans in Kenya, records show' (2023) (accessible here).
[23] Kenya Ministry of Interior, 'Statement on Worldcoin' (2023) (accessible here).
[24] See above n 22.

Another barrier to the advancement of data protection on the continent is the limited scope of data protection laws, with many containing extensive national security or private sector exemptions that undermine their efficacy. In this regard, it is also important to note the track record on the continent of national security justifications being abused, as detailed in Module 9 in this series.

4. THE RIGHT TO BE FORGOTTEN

4.1. Definitions

The 'right to be forgotten'[25] — which can also be described as 'the right to erasure' or 'the right to be de-listed' — entails the right of a data subject to request that commercial search engines or other websites that gather or publish personal information remove links to the personal information relating to the subject on request. The issue is highly contextual and often fraught because it usually involves a complicated balancing of public and individual interests. 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 in which it is inadequate, irrelevant, no longer relevant, or excessive in relation to purposes for which it was collected. However, in some cases, there may be a valid justification for keeping the information in the public domain because it is in the public interest.

4.2. A growing body of jurisprudence

Establishing the right to be forgotten in the CJEU

The right to be forgotten was established in a 2014 ruling of the Court of Justice of the European Union (CJEU) in the case of *Google Spain v Gonzalez*.[26] Mr Gonzalez, a Spanish national, lodged a complaint in 2010 with the Spanish information regulator. The cause of Mr Gonzalez's complaint was that any search for his name on Google's search engine prominently displayed old news articles about debt proceedings against him. Mr Gonzalez requested that the personal data relating to him, which was over a decade old, be removed or concealed because the proceedings had been fully resolved and the reference to him was now irrelevant.

The CJEU upheld the claim, relying on the **European Union** data protection law in effect at the time. The CJEU noted that the very display of personal information on a search results page constitutes the processing of the information[27] and that there was no reason why a search engine should not be subject to the obligations and guarantees laid out under the law.[28] Further, it was noted that the processing of personal information carried out by a

[25] 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 here).
[26] *Google Spain SL and Another v Agencia Española de Protección de Datos (AEPD) and Another*, Case No. C-131/12, (2014) (accessible here).
[27] *Id* at para 57.
[28] *Id* at para 58.

search engine can significantly affect the fundamental rights to privacy and the protection of personal data when a search is carried out of a person's name, as it enables any internet user to establish a profile of the person.[29] 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."[30]

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 the legitimate interests of internet users seeking access to that information.[31] This would require a fair balance to be struck between those interests and the data subject's fundamental rights, taking into account the nature of the information, its sensitivity to 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.[32]

The CJEU went on to hold that a data subject is permitted to request that information about them be removed from 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.[33] In such circumstances, the information and links concerned in the list of results must be erased.[34]

Since then, the jurisprudence on the right to be forgotten has developed significantly, particularly in the EU. See the European Court of Human Rights' Guide to the Case Law on Data Protection for some examples of the nuances that have since been developed.

The right to be forgotten has also been recognised in domestic contexts, although not as yet in sub-Saharan Africa. However, it has been recognised in South America in, for example, the State Court of Appeals of São Paulo, **Brazil**.[35] Of relevance to the media, the Supreme Court of Chile, in 2019, made an order requiring several digital media outlets to update the information they had published about a person involved in a criminal case in order to achieve a balance between the right to information that was in the public interest and the right to honour.[36]

4.3. Non-consensual dissemination of intimate images (NCII)

[29] *Id* at para 80.
[30] *Id.*
[31] *Id* at para 81.
[32] *Id.*
[33] *Id* at para 94.
[34] *Id* at para 94.
[35] *De Queiroz v. Google Brasil Internet Ltd.* Case No. 0004144-77.2015.8.26.0297 (2016) (accessible here).
[36] *Surgeon v. Court of Appeals of Santiago*, Case No. RoI No. 1279-2019 (2019) (accessible here).

A growing body of case law is also beginning to recognise the right to be forgotten in cases of the non-consensual sharing of intimate images (NCII), such as *X v. Union of India* and *X v. YouTube*, both in the High Court of Delhi in India.

Litigating 'Non-Consensual Distribution of Images: Kenya

In 2016, the High Court of Kenya determined a case, *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* (2016), involving the non-consensual distribution of the petitioner's nude photographs by an ex-boyfriend, resulting in her dethronement as Miss World Kenya 2015.[37]

The Court held that Ebrahim had a legitimate expectation of privacy, that she did not waive her right to protection of privacy by taking nude photographs, and did not consent to their dissemination to third parties, and as such, her right to privacy under Article 31 of the Constitution of Kenya had been violated. It further ordered the ex-boyfriend to pay damages and directed the organisers of the Miss World Kenya not to publish the nude photographs in their possession.

The case provides valuable insights into the 'reasonable expectation of privacy,' whether images are obtained in an intrusive manner, and whether the presence of illegalities may invalidate a right to privacy claim.[38]

4.3. Limits on the right to be forgotten

As jurisprudence around the world has developed, lines have begun to be drawn identifying the limits of the right to be forgotten. In 2017, the CJEU declined to uphold a request to erase, anonymise, or block any data linking the plaintiff to the liquidation of his company contained in the companies register in the case of *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni.*[39] The CJEU held that in light of the range of possible legitimate uses for data in company 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.[40]

[37] *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* [2016] eKLR (accessible here).
[38] For further information on the use of the 'tort of invasion of privacy,' the public disclosure of embarrassing facts, breaches of the torts of breach of confidence and intentional infliction of mental distress, see: *Jane Doe 464533 v. D. (N.)* (accessible here); see also: Equality Project 'Technologically-Facilitated Violence: Non-Consensual Distribution of Intimate Images Case Law' (2019) (accessible here).
[39] Case No. C-385-15, (2017) (accessible here).
[40] *Ministra Nancy Andrighi v Google Brasil Internet Ltd and Others*, 2011/0307909-6, (2012) (accessible here).

- 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".[41]

According to the Global Principles of Freedom of Expression and Privacy (Global Principles),[42] 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[43] 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.[44] 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.[45]

5. ENCRYPTION AND ANONYMITY ON THE INTERNET[46]

5.1. Definition

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.[47] With "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.[48] It is also possible to encrypt data at rest that is stored on one's device, such as a laptop or hard drive.[49]

Anonymity can be defined either as acting or communicating without using or presenting one's name or identity, as acting or communicating in a way that protects the determination of one's name or identity or as using an invented or assumed name that may not necessarily be associated with one's legal or customary identity.[50] Anonymity may be distinguished from pseudo-anonymity: the former refers to taking no name at all, while the latter refers to taking an assumed name.[51]

---

[41] The Japan Times, 'Top court rejects 'right to be forgotten' demand' (2017) (accessible here).
[42] Article19 'The Global Principles' (accessible here). The Global Principles were developed by civil society, led by ARTICLE19, in cooperation with high-level experts from around the world.
[43] *Id* at Principle 18(1).
[44] *Id* at Principle 18(4).
[45] *Id* at Principle 18(2).
[46] 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 here).
[47] Report of the UNSR on Freedom of Expression, 'Report on anonymity, encryption and the human rights framework', A/HRC/29/32, (2015) (accessible here) at para 7. 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 here).
[48] *Id*.
[49] *Id.*
[50] Electronic Frontier Foundation, 'Anonymity and encryption' (2015) (accessible here) at p 3.
[51] *Id*.

5.2. Importance of freedom of expression

Encryption and anonymity are necessary tools for the full enjoyment of digital rights and deserve protection by virtue of the critical role that they play in securing the rights to freedom of expression and privacy. As described by the UNSR on FreeEX:[52]

> "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 a 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 a person fears 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, and are particularly important for journalists communicating online to be protected from surveillance and to maintain the confidentiality of journalistic sources. Accordingly, under international human rights law, restrictions on encryption and anonymity must meet the three-part test to justify the restriction.

5.4. Balancing security with freedom of expression

According to the UNSR on FreeEX, while encryption and anonymity may have the potential to frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public safety justifications to support any restrictions or to identify situations where the restriction has been necessary to achieve a legitimate goal.[53] Outright prohibitions on the individual use of encryption technology disproportionately restrict the right to freedom of expression as they deprive 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.[54] 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.[55]

The use of encryption and anonymity by journalists

[52] See above UNSR Report on Anonymity and Encryption n 47 at para 12.
[53] *Id* at para 36.
[54] *Id* at para 40.
[55] *Id* at para 41.

In the 2015 case of *Federal Prosecutor v Soleyana Shimeles Gebremariam and others (Zone 9 Bloggers)* in **Ethiopia**, in which nine bloggers were charged with planning, preparing, conspiring, and inciting to execute terrorism, it is notable that the prosecutor in the case cited the bloggers' use of encryption tools to protect the confidentiality of their data as evidence that they were undertaking covert acts against the government. Ultimately, all charges were either dropped or the defendants were acquitted due to a lack of evidence.[56]

Since 2015, awareness and understanding of the use of encryption tools has advanced, and it is, in most cases, no longer seen as an inherent indication of having something to hide. However, journalists continue to face many challenges in using fully secure and protected encryption and anonymity tools in practice, with constant threats from law enforcement agencies seeking 'back doors' into such tools.

Regardless, the principle of the confidentiality of journalistic sources is well established in case law, including in Africa. In the 2023 case of *Mazetti Management Services. amaBhungane Centre for Investigative Journalism* in **South Africa** the High Court set aside an interim injunction ordering a media organisation to return documents in its possession and confirmed that the confidentiality of sources is a key and important feature of investigative journalism.[57] An *amicus curiae* in the case made submissions on the importance of the confidentiality of journalistic sources as set out in international human rights law.

The UNSR on FreeEX has, therefore, called on states to promote strong encryption and anonymity, and noted that decryption orders should only be permissible when they result 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.[58]

The 2019 ACHPR Declaration of Principles on Freedom of Expression and Access to Information likewise provides that states should not adopt laws or other measures prohibiting or weakening encryption, including backdoors or key escrows unless such measures are justifiable and compatible with international human rights law and standards.[59]

Despite this clear mandate, many countries in sub-Saharan Africa continue to regulate or limit the use of encryption. For example, some require the registration and licensing of encryption service providers or have laws that compel service providers to hand over secret codes to state authorities.[60] According to the Global Partners Digital World Map of Encryption, at least

[56] *Federal Prosecutor v. Soleyana Shimeles Gebremariam and others (Zone 9 Bloggers)* (2015) (accessible here).
[57] *Mazetti Management Services v. amaBhungane Centre for Investigative Journalism* (2023) (accessible here).
[58] *Id* at paras 59-60.
[59] See above n 3 at Principle 40.
[60] CIPESA, 'How African Governments Undermine the Use of Encryption' (2021) (accessible here).

27 countries in Africa have laws and policies enabling widespread restrictions on the use of encryption tools.[61]

A new form of surveillance: SIM card registration[62]

In virtually all African countries, there is mandatory SIM card registration, during which a horde of identifying data is collected. While the surge in cybercrimes prompted SIM registration, the data requirements for registration are huge yet the data protection practices are poor with no specific data protection laws. Even in countries with data protection laws, implementation is often poor and many laws fall short of established human rights standards. Moreover, the trends in data collection seem to be changing with several countries increasingly pegging service delivery to data which is collected and stored in various databases. Of itself, SIM registration in effect eradicates the ability of mobile phone users to communicate anonymously and facilitates mass surveillance, making tracking and monitoring of all users easier for law enforcement and security agencies.

Another concern relates to the growing preference for African governments to implement data localisation regulations which mandate that personal data be stored within the country. While ostensibly this is to ensure the protection of personal information, it may also enable easier access to data for decryption and surveillance.[63]

6. GOVERNMENT AND COMMERCIAL SURVEILLANCE[64]

6.1. Definition

Communications surveillance encompasses the monitoring, intercepting, collecting, analysing, retention, or similar actions, of a person's communications in the past, present, or future.[65] This relates to both the content of communications and communication *metadata* – which is information *about* a communication, such as the identities of the parties, the time or duration or location of the communication, and technical services used. It has been noted that even communication metadata can give detailed insights 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.

In recent years, the use of sophisticated surveillance technology on mobile phones has gained increasing prominence amidst concerns about its extensive abuse to monitor political opponents and activists.

[61] Global Partners Digital, 'World Map of Encryption' (accessible here).
[62] See above n 60.
[63] *Id*.
[64] 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 here).
[65] Article19 et al, 'Necessary and proportionate: International principles on the application of human rights to communications surveillance' (2014) (accessible here) at p 4.

The Pegasus scandal

In 2021, news broke that at least 180 journalists as well as political leaders had been targeted for surveillance by Pegasus spyware, a system that can be remotely installed on a smartphone enabling complete control over the device.[66] The news attracted widespread condemnation, including, for example, the Supreme Court of India in 2021 ordered an independent inquiry into allegations that the government deployed the Pegasus spyware against various journalists, politicians, and dissidents because of the deeply chilling effects its use could have on freedom of expression.[67] Although the findings of the Court's investigation have not been made public, evidence has since come to light of the continued use of the Pegasus software to surveil journalists.[68]

In 2019, Meta launched litigation against the NSO Group, the maker of Pegasus software, claiming that it was responsible for a series of cyber-attacks which violated American law.[69] The litigation is as of 2024 still ongoing. In February 2024, NSO Group was ordered to hand over its code for Pegasus and other spyware products, as well as information concerning the full functionality of the relevant spyware.[70]

African activists and journalists were among some of the targets identified in the Pegasus scandal, as were powerful politicians and state officials revealed to be users of the tools. In 2024, Reporters without Borders found spyware traces on the phones of two **Togolese** journalists while they were on trial for defamation against a government minister.[71]

6.2. International law position

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."[72] Surveillance — both bulk (or mass) collection of data[73] or targeted collection of data — interferes directly with the privacy and security necessary for freedom of opinion and expression, and must be considered against

[66] Forbidden Stories, 'Journalists Under Surveillance' (2021) (accessible here).
[67] *Sharma v Union of India and Others*, Writ Petition (CRL.) No. 314 (2021) (accessible here).
[68] Amnesty International, 'India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists' (2023) (accessible here).
[69] Nick Hopkins and Stephanie Kirchgaessner, 'WhatsApp sues Israeli firm, accursing it of hacking activists' phones' *The Guardian* (2019) (accessible here).
[70] Stephanie Kirchgaessner, 'Court orders maker of Pegasus spyware to hand over code to Whatsapp' *The Guardian* (2024) (accessible here).
[71] RSF, 'In first for Togo, RSF identifies spyware on phones of two Togolese journalists' (2024) (accessible here).
[72] See above n 9 at para 8.
[73] 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 above n 47 at para 4.

the three-part test to assess the permissibility of the restriction.[74] 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 of conducting such surveillance is no longer limited by scale or duration.[75] In Africa, some countries have even passed legislation enabling digital surveillance of targeted groups; for example, the United Nations Special Rapporteur on Privacy has noted with concern the Anti-Cybercrime Law enacted in Egypt in 2018 which reportedly enables surveillance of the LGBTQI community.[76]

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.[77] 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.[78]

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 surveillance activities. According to the Necessary and Proportionate Principles, a civil society initiative to document the principles that apply to any limitation on freedom of expression, 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:[79]

- 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.

---

[74] *Id* at para 20.
[75] *Id* at para 2.
[76] UNSR on Privacy, 'Report prepared pursuant to Human Rights Council resolutions 28/16 and 37/2' (20190 (accessible here) at p 14.
[77] UNGA, 'Resolution on the right to privacy in the digital age' A/C.3/71/L.39/Rev.1, (2016) (accessible here).
[78] *Id.*
[79] See above n 65 at Principle 5.

- The surveillance activities requested, and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

The importance of independent oversight and subject notification

In addition to the principles discussed above, the groundbreaking case of *amaBhungane Centre for Investigative Journalism v Minister of Justice and Correctional Services* emphasised two additional principles that are critical to ensuring legitimate and rights-respecting targeted surveillance. First, the Constitutional Court of **South Africa** emphasised the need for a clear and independent process for appointing the designated judge to oversee requests for surveillance by law enforcement. Second, it highlighted that the law should accommodate the notification of subjects of surveillance that they have been surveilled after the fact and when such notification will no longer threaten the investigation.

In addition, it is notable that the Court reflected on the need for enhanced protections for lawyers and journalists as a result of the importance of confidentiality in these professions, and that legislation should therefore provide additional safeguards in such cases.

Surveillance constitutes an obvious interference with the right to privacy. Further, it also constitutes an interference with 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.[80]

As emphasised in the *amaBhungane* case, the interference with the right to freedom of expression is particularly apparent in the context of journalists who may be placed under surveillance as a result of their journalistic activities. The disclosure or surveillance of journalistic sources can have negative consequences for the right to freedom of expression due to a breach of an individual's confidentiality in their communications.[81] 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.[82] The court stated in this regard that:

[80] See above n 47 at para 21.
[81] For more, see *Big Brother Watch v United Kingdom* in the ECtHR (2018) (accessible here) and *amaBhungane Centre for Investigative Journalism v Minister of Justice* in South Africa (2019) (accessible here).
[82] [2012] ZAGPJHC 71, (2012) (accessible here).

> "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."[83]

Surveillance activities carried out against journalists have the risk of fundamentally undermining the source protection to which journalists are otherwise entitled.[84]

6.3. Jurisprudence on journalism and the right to privacy

The linkages between journalistic freedoms and the right to privacy are a common theme in emerging litigation and jurisprudence against unlawful or abusive surveillance. For example:

- In two cases both dealing with the planned roll-out by the Communications Authority of **Kenya** of a system to provide it with access to mobile service subscribers' data, the High Court of Kenya held that the system was "a threat to subscribers' privacy," that there were fewer restriction measures to implement the Authority's goals of identifying illicit devices, and that the system was unlawful, unreasonable, and disproportionate.[85]

- In ordering the independent inquiry into allegations that the government deployed the Pegasus spyware against various journalists, politicians and dissidents, the Supreme Court of **India** found that the free press's democratic function was at stake, and that "such chilling effect on the freedom of speech is an assault on the vital public watchdog role of the press, which may undermine the ability of the press to provide accurate and reliable information."[86]

- The European Court of Human Rights (ECtHR) found some aspects of the **United Kingdom's** mass surveillance regime to be in violation of the right to privacy and

---

[83] *Id* at para 38.

[84] 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.

[85] *Kenya Human Rights Commission v. Communications Authority of Kenya* (2018) (accessible here) and *Okoiti v. Communications Authority of Kenya* (2018) (accessible here).

[86] Writ Petition (Crl.) No. 314 of 2021, (2021) (accessible here).

the right to freedom of expression under the European Convention on Human Rights, holding that although bulk interception regimes are not in themselves incompatible with those rights, the lack of independent oversight and the fact that the regime's use was not limited to combatting "serious crime" and did not sufficiently protect journalists' confidential communication resulted in it constituting a violation.[87]

7. PRIVACY AND ARTIFICIAL INTELLIGENCE

7.1. The privacy risks of AI

As the sophistication and usage of artificial intelligence (AI) has increased rapidly in recent years, concerns about both the use of personal information in the development of such tools as well as the ability of such tools to implement privacy violations have become more prominent. In particular, the launch of the public ChatGPT, alongside similar models, has raised alarm bells on several fronts.

- First, because such systems rely on **vast quantities of information** to train their algorithms and continuously improve performance, particularly information scraped from the internet, critics have highlighted that even publicly-available information, such as posts on social media, was never posted with the intent, and hence **consent**, of the data subjects for its usage by large-language models.

- Second, the **collection and storage** of such large quantities of information, including personal information, raise concerns about storage security and the implications if such data were to be accessed by unauthorised parties through hacking or other security breaches. Facial recognition technology, which also often relies on sophisticated algorithms to process large quantities of data, is increasingly in use across the continent by governments ostensibly for law enforcement and security purposes, but they also have the potential to be used for **real-time, intrusive tracking and surveillance** that risks several human rights including the rights to privacy, freedom of movement, and freedom of association.

- Third, AI tools such as these are able to **rapidly generate images and content** about a person based on its training data that may have little correlation to the truth, raising concerns about **mis- and disinformation** and the portrayal of personal information in the online ecosystem. AI's ability to rapidly analyse and make sense of large quantities of data can lead to the ability to infer personal information about a person that they never provided themselves, beyond the scope of consent requirements set out in data protection laws.

7.2. Developing international standards

As a result of these risks, AI has recently garnered increased attention from international and regional human rights bodies seeking to provide guidance and standards to protect the

[87] *Big Brother Watch v. The United Kingdom (Big Brother I)* App nos. 58170/13, 62322/14 and 24960/15 (2018) (accessible here).

affected rights and ensure the responsible development of these new technologies. For example:

- In 2021 the UN Special Rapporteur on the Right to Privacy published a report on AI and privacy and children's privacy that provides guidance on data protection standards for AI at the domestic level as well as calls on states and companies to develop AI solutions ethically and responsibly within a human rights framework.[88]

- Also in 2021, the UN High Commissioner for Human Rights released a report on the right to privacy in the digital age that analysed how the widespread use of AI affects the right to privacy and other fundamental rights, noting that issued a set of recommendations for states and businesses to design and implement rights safeguards.[89] The report notes that AI systems "[incentivise] widespread data collection, storage, and processing," contrary to the principle of data minimisation, and highlights concerns in the sectors of law enforcement, public services, employment, and online information management systems.

- Building on this, in 2023 the new Special Rapporteur submitted her report to the United Nations General Assembly (UNGA) that highlighted the need for transparency and explainability in the use of AI in order for data subjects to be able to exercise their rights over the use of their personal information in such systems.[90]

Notably, the African Union Commission on Human and Peoples' Rights (ACHPR) has also taken steps to interrogate the risks of AI by passing Resolution ACHPR/Res. 473 (EXT.OS/ XXXI) 2021: on the need to undertake a Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa in 2021.[91] In it, the ACHPR—

- acknowledges the myriad risks for human rights not limited to privacy;
- calls on states to put in place mechanisms to ensure the rights-respecting development and use of such technologies in Africa, including by working towards a comprehensive legal and ethical governance framework for AI; and
- commits to undertake a study to develop guidelines on AI.

The study officially began in June 2023.[92]

[88] UNSR on Privacy 'Artificial intelligence and privacy, and children's privacy' (2021) (accessible here).
[89] Report of the UN High Commissioner for Human Rights 'The right to privacy in the digital age '(2021) (accessible here).
[90] UNSR on Privacy 'Right to privacy,' (2023) (accessible here).
[91] ACHR, 'Resolution on the need to undertake a Study on huma and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa' ACHR/Res. 473 (EXT.OS/XXXI) (2021) (accessible here).
[92] ACHPR, 'PRESS RELEASE: Inception Workshop and Experts' Consultation on the Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa, 08 - 09 June 2023 Nairobi, Kenya' (2023) (accessible here).

8. CONCLUSION

As more of the world moves online and increasingly sophisticated new tools for processing personal information become more widely available, data protection is becoming ever more necessary. In the African context, some headway has been made in the passing of 36 data protection laws as well as the coming into force of the Malabo Convention in 2023.[93] However, with the growth and increasing sophistication of technologies and practices related to data harvesting and profiling, 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 people's rights to privacy.

[93] See https://dataprotection.africa/ for more information.

Module 5

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

ISBN 978-0-9935214-1-6
Published by Media Legal Defence Initiative: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in April 2024

TABLE OF CONTENTS

MODULE 5
DEFAMATION

- **Defamation claims are frequently used to 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. 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[1] suits by corporate actors using defamation laws to silence or intimidate critics is a concerning contemporary development that needs to be challenged.**

1. INTRODUCTION

Defamation proceedings, subject to the intention with which they are launched, can either be a tool or a weapon. As a tool, it can enable legal redress on the basis of the infringement of rights, such as the right to dignity. However, when defamation proceedings are launched in an effort to silence dissenting voices or intimidate critics, it becomes a weapon.

- Defamation claims are increasingly used to stifle 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 several 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

[1] Strategic Lawsuits Against Public Participation, see *SLAPP suits* below.

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.[2]

In the recent South African case of *Native Child Africa (Pty) Ltd v Akinwale*, the Court tackled issues concerning social media influencers in the context of a defamation claim.[3] The Court issued restraining orders against the influencer, barring defamatory content on various platforms, and preventing statements encouraging boycotts of the applicant's business. The influencer was also required to remove all defamatory material, issue apologies, and refrain from such behaviour. The Court explained that "without timely intervention, followers of such influencers could engage in damaging or even aggressive actions against brands, potentially leading to a disregard for law and order on social media platforms". This illustrates the contemporary and ever-evolving considerations relating to defamation online.

Dealing with online defamation cases is particularly challenging for many reasons,[4] including that "the internet is not an easily identifiable body that is administered or regulated within the confines of strict internationally recognised parameters or boundaries."[5] 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.[6] 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.

2. 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.[7] Penalties and costs attached to defamation proceedings can 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 refers to the rights and

[2] Iyer, 'An Analytical Look into the Concept of Online Defamation in South Africa.' Desan Iyer, (2018) (accessible here).
[3] *Native Child Africa (Pty) Ltd v Akinwale* [2023] ZAGPPHC 2007 (accessible here).
[4] Id at section 3.
[5] Id at p 127.
[6] For example, South African law, as seen in *National Media Ltd and Others v Bogoshi,* per note 22.
[7] Electronic Frontier Foundation, 'Online Defamation Law' (accessible here). 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.

reputation of others as a legitimate ground for limitation of the right to freedom of expression. Reputation is therefore the underlying basis in any claim of defamation, whether slander or libel.[8]

Defamation can be an important legal remedy for 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 growing trend in the online era that disproportionately affects women. In these cases, defamation may provide recourse to seek justice for the non-consensual sharing of images (NCII) or other personal attacks.

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

3. 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);
- the Africa Commission on Human and People's Rights (ACHPR) who have both urged states to reconsider such laws;
- 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";[9]
- Moreover, Principle 22 of the African Commission on Human and People's Rights (**ACHPR**) Declaration on Principles of Freedom of Expression and Access to Information in Africa calls on states to amend criminal defamation and libel laws in favour of civil sanctions that are necessary and proportionate. It further states that the imposition of custodial sentences for the offences of defamation and libel *is* a violation of the right to freedom of expression.

Court have also taken a strong stance:

- 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*,[10] it was held that

[8] 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 here). See also above no. 6 for a definition of libel and slander.
[9] UNHRC, 'General Comment No. 34' (2011) (accessible here).
[10] African Court, Application No. 004/2013 (2013) (accessible here).

imprisonment for defamation violates the right to freedom of expression and that criminal defamation laws should only be used in restricted circumstances.

- 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 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."[11]

- Most recently, the ECOWAS Court held that Nigeria's Broadcasting Code violated the right to freedom of expression protected by the ACHPR because the Code prohibited protected speech and the sanctions for committing hate speech were excessive. Nigeria was ordered to align the code with its international obligations and to protect the right to freedom of expression.[12]

African Commission's critique of Rwanda's criminal defamation laws

Agnes Uwimana-Nkusi v. Rwanda concerned the conviction of journalists Agnes Uwimana-Nkusi and Saidati Mukakibibi on the grounds of defamation and threatening national security following the publication of three articles criticizing the **Rwandan** government.[13] The journalist published articles detailing allegations of corruption among high-profile public officers, the human rights situation in Rwanda, and other government shortcomings. The government argued that the articles intended to incite violence and strife against the government by using defamatory statements devoid of evidence. Having exhausted all available domestic remedies, Media Dence (Media Legal Defence Initiative as it was then), filed a complaint to the Commission on behalf of the journalists arguing Rwanda violated their rights to freedom of expression and to a fair trial.

The Commission considered whether discussing the 1994 Rwanda Genocide amounted to genocide denial. Considering Rwanda's history, it assessed if implementing penal code articles was necessary and proportionate. The Commission emphasized democratic governance contexts in evaluating public order protection and incitement definitions. While acknowledging the sensitivity around the genocide, it found the journalists' articles did not incite violence or threaten security.

The Commission criticised criminal defamation laws, deeming them disproportionate restrictions on journalism. It stressed the vital role of freedom of expression in democracy, particularly in fostering political discourse and holding officials accountable. Consequently,

[11] 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 here).
[12] The Incorporated Trustees of Expression Now Human Rights Initiative v. Federal Republic of Nigeria ECOWAS ECW/CCJ/JUD/37/23 accessible here.
[13] *Agnes Uwimana-Nkusi v. Rwanda* (2021) (accessible here). See also Global Freedom of Expression at Columbia University, 'Case update: Agnes Uwimana-Nkusi v. Rwanda (accessible here).

the Commission ruled Rwanda's actions violated Article 9 of the Charter by unjustly restricting the journalists' freedom of expression

Promisingly domestic trends indicate – for several countries – a shift away from criminal defamation:

- In 2016, in *Misa-Zimbabwe et al v Minister of Justice et al*,[14] 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.
- 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*,[15] stating that they violated the right to freedom of expression as protected in the Lesotho Constitution.
- In 2020, Sierra Leone's Parliament has also repealed its 1965 Public Order Act in 2020 by approving the Independent Media Commission Act 2020.[16]
- In 2022, Zambia amended the Penal Code to abolish the offence of criminal defamation of the President.[17]
- In 2023, the South African legislature, repealed the common law crime of criminal defamation, this was done through the passing of the Judicial Matters Amendment Bill. In clause 35(2) the Bill notes that there are well-established civil remedies to respond to defamation as opposed to the chilling criminal defamation laws.

Despite these important legal decisions protecting freedom of expression, there have been instances in which journalists faced arrest for defamation.

- In 2019 in Ghana, National Security operatives raided an online news portal's office, arresting its deputy editor and a reporter over the publication of allegedly false news about the National Security Minister Albert Kan Dapaah.
- In October 2021, also in Ghana an editor of a digital newspaper, David Tamklie, was arrested by plain-clothed officers wielding guns for publishing false news.[18] The arrests were carried out under the Criminal and Offices Act of 1960 and the Electronic Communications Act 775 of 1960. According to the Criminal Offences Act, anyone who publishes or reproduces a false statement, rumour or report that could cause fear and alarm to the public commits a misdemeanour. The Electronic Communications Act similarly provides that any person who knowingly sends a false electronic communication is liable for conviction to a fine or imprisonment of no more than five years or both.[19]

[14] Constitutional Court of Zimbabwe, Case no. CCZ/07/15 (2015) (accessible here).
[15] Constitutional Court of Lesotho, Case no. CC 11/2016 (2018) (accessible here).
[16] Media Foundation for West Africa, 'Major Boost for Press Freedom as Sierra Leone Scraps Criminal Libel Law after 55 years' (24 July 2020) (accessible here).
[17] International Bar Association, 'Zambia: IBAHRI welcomes death penalty abolition' (2023) (accessible here).
[18] Section 208.
[19] Section 76.

- In Angola, a reporter was arrested and charged with criminal defamation insult and forgery, if convicted, the reporter faces up to 1.5 years in prison according to the Penal Code.[20] Criminal defamation investigations against Angolan journalists spike ahead of the elections and are reported as criminalising journalism in Angola.[21]

4. 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.[22]

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 purpose of restoring reputation or honour, there is still potential for them to be misused and cause a "chilling effect" on the full enjoyment and exercise of freedom of expression.

Overview of debates and decisions on defamation being used against survivors of gender-based violence

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 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. The Special Rapporteur on Violence Against Women, in a report on online violence, explains that the act of threatening survivors with legal proceedings in an attempt to prevent them from reporting their situation is another form of gender-based violence, cautioning that the use of defamation lawsuits against women who speak out about their experiences "may form part of a pattern of domestic violence and abuse.

[20] Committee to Protect Journalists "Angolan authorities charge journalist with criminal defamation over corruption report" 2023 (Accessible here).
[21] Committee to Protect Journalists "Angolan editors questioned in separate criminal defamation investigations" 2021 (Accessible here).
[22] Quartz Africa, Jonathen Rozen 'Colonial and Apartheid-era laws still govern press freedom in southern Africa' (2018) (accessible here).

- 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.[23] 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 that Patel had a pre-existing grudge against him. In 2019, a judge found against Patel and 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.

- In 2022, a South African High Court overturned a previous order that restricted an individual from discussing her experiences of gender-based violence (GBV).[24] The appellant was initially prohibited by a Magistrate's Court order from claiming she was raped by her ex-boyfriend. The alleged rape occurred after their breakup in July 2015, and in September 2019, the appellant shared her experience in a private Instagram group. The posts were meant to remain private, but someone in the group made them public without her consent. In response, her ex-boyfriend obtained a protection order preventing her from repeating the rape allegation. The High Court emphasized that the appellant's GBV allegations were not publicly posted and affirmed her right to speak out about her experiences. The court criticized the original protection order, stating it perpetuated the idea that GBV victims should remain silent.

- In another positive development in South Africa, the High Court in July 2022 defended the right of victims/survivors to speak about their experiences of violence. In the case of *Segerman v Peterson*, the victim/survivor had spoken about her rape with friends and family and had posted about it in a closed, private, and anonymous social media platform group in which she named her rapist as a way to warn others, and to seek healing, community, and support from others in the group. Although the posts were intended to remain private, someone in the group made them public on various social media platforms. The alleged perpetrator applied to the Magistrate's Court for a protection order against the victim/survivor, arguing she was harassing him by speaking about him to others and identifying him as her rapist. The Magistrates Court granted the protection order, which stated that she was "not allowed to tell anyone, in any manner, that he had raped her." On appeal at the High Court, the Court affirmed the right of women to freely speak about violence affecting them.[25]

- The case of *Akbar v. Ramani* in India found similarly, with the Court stating that victims of sexual harassment "cannot be punished for raising their voices against abuse on the pretext of a criminal complaint of defamation, as the right to reputation cannot be

[23] 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 here).
[24] *D.S v A.P and Others* [2022] ZAWCHC 42 (accessible here).
[25] Women's Legal Centre, 'High Court vindicates women's rights to speak about their rape experience as a critical way to combat the scourge of violence against women,' (2022) (accessible here). The judgment is (accessible here). For more on defamation in the online sphere, see section 1.1. in Media Defence's Report, Mapping Digital Rights and Online Freedom of Expression Litigation in East, West and Southern Africa (2021), (accessible here).

protected at the cost of the right of life and dignity of woman as guaranteed in the Indian Constitution."

5. 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."[26]

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 a particular way and at the particular time."[27]

In 2022 the High Court of Namibia ruled that a member of an opposition political party had defamed the wife of the President, Hage Geingob, and was ordered to pay damages to First Lady, Monica Geingos.[28] The Court determined that Hishoono had actually intended to target Geingob with defamatory claims on social media. Hishoono's argument that he was merely repeating existing rumours already circulating about Geingos was not considered a valid defence. The Court emphasised that there is no moral distinction between the originator and the conveyer of a rumour. Both actions are discouraged, emphasising that spreading rumours or making damaging statements to one's reputation without a valid legal defence carries the same level of responsibility.

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.[29] 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."[30]

---

[26] African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression in Africa', (2019) (accessible here).
[27] Supreme Court of Appeal of South Africa, Case No. 579/96 (1998) (accessible here).
[28] *Geingos v Hishoono* (2022) (accessible here).
[29] Carver above at n 8 at p 52.
[30] *National Media Ltd and Others v Bogoshi* (2010) (accessible here).

Similarly, General Comment No. 34 states that "a public interest in the subject matter of the criticism should be recognised as a defence"[31] against defamation.

6. 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." 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.

7. 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.[32] Likewise, heavy fines, whether in criminal or civil cases, are aimed at punishing the defamer rather than redressing the wrong to the defamed.[33]

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, as seen in various cases in South Africa:

- The 2019 High Court judgment in *Manuel v Economic Freedom Fighters* sheds light on applying defamation laws to online statements.[34] Key points include the court

[31] UNHRC above at n 9 at p 12.
[32] UNHRC above at n 9.
[33] African Court, above at n 10.
[34] *Manuel v Economic Freedom Fighters* (accessible here).

considering Twitter users as the hypothetical audience, the 'repetition rule' holding those who share defamatory statements accountable, and the extension of the reasonable publication defence to the public. The court ordered the removal of the statement within 24 hours, but challenges arose in fully erasing content from social media. The Supreme Court of Appeal upheld the defamation ruling but referred damages for reconsideration due to their high amount, emphasizing the need to balance defamation claims with freedom of expression.

- In *Daily Maverick (Pty) Ltd and Another v Modiba*, the High Court dealt with a defamation case arising from a series of defamatory tweets.[35] The Daily Maverick, an online news service, along with others, filed a case against Modibe Modadiba. Starting from January 17, 2019, and spanning ten months, Modadiba submitted unsolicited columns to the Daily Maverick, four of which were published. No compensation, whether in cash or kind, was offered to Modadiba, which was the usual practice for guest columnists. In June 2019, an article by Modadiba titled “Why Zindzi Mandela should be protected” was deemed unfit for publication due to poor writing and incoherence. Subsequent columns submitted by Modadiba were also rejected. One, discussing the establishment of a national women's football league, lacked depth, and another on Pan-Africanism was too short, incoherent, and lacked a proper conclusion. Modadiba eventually stopped submitting articles to the Daily Maverick. On January 3, 2020, Modadiba took to Twitter, claiming that he decided to stop writing for the Daily Maverick because they only published articles critical of black leaders, ANC, or EFF. He alleged that when writing anything deemed "anti-white," the Daily Maverick had an issue. Modadiba continued to post a series of similar tweets, asserting that the applicants were involved in a coordinated effort to mobilize students and social media influencers to spread fake news about certain individuals and organizations for payment. The court additionally explained that the Economic Freedom Fighters, IOL, and the Information Communication & Technology Union regarded the allegations in the tweets as credible and significant. Since the applicants successfully demonstrated the aspects of defamation, the statements made by the respondent were considered false. Consequently, the court instructed the respondent to issue an unqualified retraction and pay damages amounting to R100,000.

- Once again, in a 2020 case the High Court in Johannesburg, South Africa, ruled that a political party's statements accusing specific journalists of being apartheid agents were defamatory.[36] In *Gqubule-Mbeki and Another v Economic Freedom Fighters*, two journalists filed the application after the party shared a statement on Twitter, repeating allegations from Winnie Madikizela-Mandela that the journalists were involved in an apartheid government-backed disinformation and propaganda campaign. The court emphasized the lack of evidence supporting the truth of these allegations and stated that the political party couldn't use the defences of reasonable publication and fair comment.[37]

[35] *Daily Maverick (Pty) Ltd and Another v Modiba* [2022] ZAGPJHC 555 (accessible here).
[36] *Gqubule-Mbeki and Another v Economic Freedom Fighters and Another* [2020] ZAGPJHC 2 (accessible here).
[37] Andisiwe Makinana, ‘Trevor Manuel loses Constitutional Court bid to appeal dismissal in damages from EFF,’ Business Day (2021) (accessible here).

8. TYPES OF DEFAMATORY MATERIAL

8.1. Opinion versus fact

We have dealt above with 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,"[38] 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."

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 an opinion or as a statement of fact. There are, for example, ways in which a statement of fact may be made to appear as an opinion.[39] 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.'"[40]

8.2. 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."[41]

In an amusing recent example, American satirical news publication The Onion submitted an *amicus curiae* brief to the United States Supreme Court in a case brought by a man who was arrested for mocking local police using satire. The brief blends legal arguments with humour

[38] UNHRC above at n 9 at p 12.
[39] Electronic Frontier Foundation above at n 6.
[40] US District Court, Southern District of New York, Case No. 1:2019cv11161 - Document 39' (2020) (accessible here).
[41] Verashni Pillay, 'Zapiro cartoon: Zuma surrenders, drops lawsuit,' (2012) (accessible here).

and satire to argue for protecting the publication of parody and satire as an ancient and valuable art form and to prevent the imprisonment of humourists.[42]

8.3. 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,"[43] 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*[44] raises some questions about the extent to which this principle holds up in African courts, particularly in the online domain.

8.4. 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.

8.5. 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.

8.6. 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,

[42] Novak v City of Parma and Others, 'Brief of the Onion as amicus curiae in support of petitioner,' Supreme Court of the United States No. 220293, (accessible here).
[43] European Court of Human Rights, Application No. 1131/05 (2007).
[44] High Court of South Africa above at n 32.

> 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."[45]

It is important that civil defamation laws contain sufficient checks and balances to prevent them from 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."[46]

9. ALTERNATIVE CLAIMS

9.1. 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 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.

In the ground-breaking case of *Mineral Sands Resources v Reddell*, the High Court of South Africa recognised a SLAPP defence for the first time. The case involved a mining company that had been seeking to develop a project in an environmentally protected region of South Africa, and which had sued environmental activists who criticised the project publicly for defamation for an amount of approximately R14 million (equivalent to roughly $1 million). The court ruled that the mining company was seeking "exorbitant amounts for damages" which the defendants could not afford; that it was "evident that the strategy adopted" by the company was that "the more vocal and critical the activist is … the higher the damages amount claimed." The court also stated that because the company "would be satisfied to dispose of the matter on the basis of a public apology," it was clear that the action was not aimed at obtaining monetary or financial damages but rather at "vindicating a right" or for some other purpose.[47] In a subsequent appeal to the Constitutional Court of South Africa, it was held that the SLAPP defence constitutes a form of the existing abuse of process doctrine under common law and did not require a development of the common law to be recognised as a defence under South African law.[48]

Following this landmark Constitutional Court ruling on SLAPP suits, South Africa's courts have been seeing an increase in cases raising SLAPP as a defence. One such case *is Maughan v Zuma*, where the South African High Court rejected a legal action initiated by the former

[45] African Court above at n 10.
[46] PEN South Africa, 'Stifling Dissent, Impeding Accountability: Criminal Defamation Laws in Africa,' p 4 (2017) (accessible here).
[47] *Mineral Sands Resources (Pty) Ltd and Another v Reddell and Others; Mineral Commodities Limited and Another v Dlamini and Another; Mineral Commodities Limited and Another v Clarke*, Western Cape High Court of South Africa (2021) (accessible here).
[48] *Mineral Sands Resources Pty Ltd v Christine Reddell*, Constitutional Court of South Africa CCT 66/21 (2022) (accessible here).

president, Jacob Zuma, against a journalist, deeming it an abuse of the legal process. The journalist had written an article containing information about the president's medical condition, gathered from publicly available court documents. When Zuma filed a lawsuit against the journalist, claiming the unauthorized disclosure of confidential information, the journalist sought to dismiss the summons. The Court determined that the notion of abuse of process, akin to a SLAPP suit, could be applicable in criminal proceedings. It concluded that the private prosecution lacked substance and was filed with the sole intent of intimidating and harassing the journalist.[49] Most recently, in the case of *Mazetti Management Services v AmaBhungane Centre for Investigative Journalism*, the South African High Court revoked a temporary injunction that had instructed a media organization to return documents it possessed and prevented further publication.[50] A group of companies, displeased with critical articles, secured an *ex parte* order from the High Court, demanding the return of documents they thought were stolen and prohibiting additional articles based on those documents. Upon review, the Court determined that the initial order was an abuse of the legal process and amounted to a SLAPP suit. The Court affirmed that South African law safeguards source confidentiality and permits pre-publication restrictions only in exceptional cases.

A growing number of states, such as Canada,[51] 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, such laws must also be carefully constructed so as not to impede the right of access to justice. Towards the end of 2023, South African civil society organisations collaborated to create an anti-SLAPP model law for South Africa.[52] The model law aims to discourage legal proceedings that hinder public participation and those that repress activists and journalists who act in the public interest. The model law sets out the test for SLAPP suits and outlines the remedies.

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. In the 2023 *Maughan v Zuma* judgment outlined above, Maughan argued that the private prosecution was a severe misuse of legal proceedings, contending that the summons in the private prosecution was obtained with the ulterior motive of intimidating, harassing, and impeding her ability to carry out her journalistic duties freely, especially reporting on Zuma's criminal trial. The Court acknowledged Maughan as one of the few remaining journalists consistently covering all of Zuma's legal matters despite facing media comments and harassment. The Court recognized that she had been subjected to harassment and restrictions, hindering her ability to report accurately and that she operated under the constant threat of potential private prosecution in criminal court or civil litigation.

[49] *Maughan v Zuma and Others* [2023] ZAKZPHC 59 (accessible here).
[50] *Mazetti Management Services (Pty) Ltd and Another v Amabhungane Centre for Investigative Journalism NPC and Others* (Accessible here).
[51] Osler, O'Brien and Tsilivis, 'Ontario Court of Appeal clarifies test under "anti-SLAPP" legislation' (2018) (accessible here).
[52] CALS "The case for anti-SLAPP legislation in South Africa" 2023 (accessible here).

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 (**EFF**) 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.[53]

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, or threats 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".[54]

9.2. 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 the government. For example, under the Lesotho Penal Code, the crime of *scandalum magnatum* (offences against the royal family) is created as a separate crime from defamation and thus remains on the statute books despite criminal defamation recently being declared unconstitutional. *Scandalum magnatum* has still been used in recent years by the government of Lesotho against its detractors.[55]

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."[56] 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.[57]

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.[58] 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

[53] Daily Maverick, Rebecca Davis. 'EFF court losses mount as Karima Brown wins battle, but faces criticism of her own' (2019) (accessible here).
[54] *Brown v Economic Freedom Fighters and Others* [2019] ZAGPJHC 166 (accessible here).
[55] Hoolo 'Nyane, 'Abolition of criminal defamation and retention of *scandalum magnatum* in Lesotho', African Human Rights Law Journal (2019) (accessible here).
[56] Merriam Webster Dictionary, 'Sedition', (accessible here).
[57] Federal Court of Appeal of Nigeria, Chief Arthur Nwankwo v. The State, 6 NCLR 228 (1983), par. 237.
[58] African Court on Human and Peoples' Rights, Application No. 004/2013, at par. 155 (2014) (accessible here).

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 tolerance, especially when he himself makes public statements that are susceptible of criticism."[59]

The 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa also states, in Principle 21, that public figures should be required to tolerate a greater degree of criticism.

The Office of the High Commissioner for Human Rights (OHCHR) has called for the abolition of the offence of 'defamation of the State,'[60] and some jurisdictions have refused to allow elected and other public authorities to sue for defamation.[61] The ECtHR has limited such suits to situations which threaten public order, implying that governments cannot sue in defamation simply to protect their honour.[62]

9.3. 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.[63]

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

[59] European Court of Human Rights, Application No. 11662/85 (1991), par. 59 (accessible here).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 here).
[60] OHCHR, Concluding Observations of the Human Rights Committee: Serbia and Montenegro, (12/08/2004), par. 22 (accessible here).
[61] OHCHR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,' (2000) (accessible here).
[62] *Ibid*.
[63] See Power & Associates, 'Protecting and promoting freedom of expression in Marikana,' (accessible here).

images (e.g. that reflects 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.
  - Most social media companies have defamation reporting processes,[64] 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 bono* (free of charge) or rely on legal defence funds for their fees.

- **If you live in a country that has defamation laws that infringe on 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.

10. 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. In a new trend, it is also being used to silence victims of gender-based violence and to institute SLAPP suits against critics of powerful private interests. Despite the recent trend towards the decriminalisation of defamation, there remains a need to ensure the implementation of judgments, remove criminal punishments for other insult laws, and institute legal protections against alternative methods of silencing activists such as SLAPP suits.

[64] For Facebook, see here. For Twitter, see here.

Module 6

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

ISBN 978-0-9935214-1-6
Published by Media Legal Defence Initiative: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in April 2024

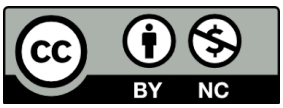

TABLE OF CONTENTS

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.**

1. 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. This is necessary, given the importance of contextual and cultural adaptation to a particular context.

Hate speech must, however, be clearly and narrowly defined and objective criteria must be applied. In the 2023 case of *The Incorporated Trustees of Expression Now Human Rights Initiative v. Federal Republic of Nigeria*, the ECOWAS Court held that provisions of Nigeria's Broadcasting Code violated the right to freedom of expression in the African Charter because its provisions on offensive and hate speech prohibited speech that was protected, were too vague, ambiguous and overbroad, and the sanctions imposed were excessive. The Court ordered Nigeria to bring the provisions into alignment with international standards.

Over-regulation of hate speech can also 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.[1] 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,[2] 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

[1] Media Defence, 'Training manual on digital rights and freedom of expression online, at p 57 (2020) (accessible here).
[2] Media Defence, 'Training Manual on Digital Rights and Freedom of Expression Online' (2010) at p 57 (accessible here)

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.[3]

Judges in Kenya have observed that the landscape of politics often blurs the boundaries between hate speech, political discourse, and criticism of elected officials.[4] A notable case illustrating this complexity is *Ian Karani Wamboma v Republic* which involved the distribution of leaflets containing the message "watu wa Jubilee wahame Busia County mara moja or else watakiona" (Jubilee supporters should move out of Busia County at once, or they'll see {the consequences}).[5] The Court clarified that Kenyan politics are frequently organised along ethnic lines, yet cautioned against applying the National Cohesion and Integration Act (NCI Act) to political offences unless the speech unequivocally targets specific ethnic groups.

South Africa has also recently grappled with these issues as the legislature has considered a newly proposed bill, the Prevention and Combatting of Hate Crimes and Hate Speech Bill, 2018. Intended to address the rising prevalence of hate crimes and hate speech in the country, particularly online, and to give effect to the rights against discrimination in the Constitution, the Bill has nevertheless been criticised for creating the potential to silence criticism and end difficult discussions about race, gender, religion, and sexuality.[6] The Bill would extend the protected characteristics defined in South Africa's Constitution from four to fifteen, introduce a new, broad definition of "harm" that critics say would be open to subjective interpretation, and by regulating private communications would also intrude in the right to privacy. In December 2023, the Bill passed both houses of parliament and is awaiting Presidential signature before becoming law. However, there have been calls from civil society organisations for the President not to sign the Bill into law because it criminalises hate speech and opens itself up to being used to undermine freedom of expression.[7] There were reported to be over 10,000 submissions to the National Council of Provinces opposing the Hate Speech Bill.[8]

2. 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 action that is violent.

[3] Article 19 Eastern Africa, 'Kenya: Use of "hate speech" laws and monitoring of politicians on social media platforms' (2020) (accessible at here).
[4] Yale Law School Lowenstein Clinic & ALT Advisory 'A human rights response to online ethnic hate speech in Kenya' (2023) (accessible here).
[5] *Ian Karani Wamboma v. Republic* (2018) eKLR, at para 2 (accessible here).
[6] See, for example, Tyla Dallas, 'Hate speech bill will have chilling effect on free speech and could be used to silence political opponents,' (2022) (accessible here).and Power & Associates, 'Submission on the Prevention and Combating of Hate Crimes and Hate Speech Bill,' (2022) (accessible here).
[7] Free Speech Union South Africa 'For Freedom's sake, Ramaphosa must reject hate crimes, hate speech Bill' (accessible here).
[8] Masilela 'Over 10,000 submissions opposing the Hate Speech Bill' *IOL News* (accessible here).

The Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence,[9] 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, as does the 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa.[10] 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 the discussion of matters of public interest and should not be envisaged unless there are particularly strong reasons for doing so."[11]

The seminal **South African** case of *Qwelane v South African Human Rights Commission in South Africa* also dealt with the issue of intent, with the Constitutional Court holding that speech must have a clear intention both to "be harmful or to incite harm" **and** to "promote or propagate hatred" before it amounts to hate speech:

> "A disjunctive reading would render the impugned section unconstitutional, since merely hurtful speech, with no element of hatred or incitement, could for example constitute prohibited hate speech. This would be an impermissible infringement of freedom of expression as it would bar speech that disturbs, offends and shocks."

In another significant **South African** case heard by the Supreme Court of Appeal, *Afriforum NPC v Nelson Mandela Foundation Trust*, a non-governmental organisation brought a case after a protest in 2017 which included the display of the old apartheid South African national flag.[12] The Nelson Mandela Foundation argued that displaying the flag brought back painful memories of the unjust apartheid system. Afriforum opposed the case, claiming that South African laws against hate speech only applied to spoken words and not to physically displaying a flag.

---

[9] 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 here).
[10] Principle 23.
[11] European Court of Human Rights, Application No. 15890/89, (1994) para 33-35 (accessible here).
[12] *Afriforum NPC v Nelson Mandela Foundation Trust* [2023] ZASCA 58 (accessible here).

The Court, however, ruled that to uphold the spirit of the Constitution and international legal commitments, hate speech should be understood to encompass displaying a flag. Consequently, the Court decided that the showing of the old flag constituted hate speech and was not protected under the South African constitutional system. The Court emphasised that such displays are intentionally harmful, incite harm, and significantly impact an individual's self-work and acceptance.

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 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."[13]

3. MUST VIOLENCE OR HATRED ACTUALLY RESULT?

Another tenet of the Rabat Plan of Action threshold test is the likelihood and imminence of violence.[14] 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*,[15] 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 actual harm having been committed as a result of his statements, though they did clearly incite and advocate for violence.[16]

Online hate speech laws are 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

[13] UNESCO, Iginio Gagliardone et al, 'Countering online hate speech' at p 58 (accessible here).
[14] OHCHR above n 9.
[15] High Court of South Africa, Gauteng Division, Case No. EQ6/2016 (2018) (accessible here).
[16] South African Human Rights Commission, 'Media Statement: SAHRC Welcomes the Equality Court's Finding Against Velaphi Khumalo' (2018) (accessible here).

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.[17]

Often this is because of:

- Overly broad definitions of hate speech and disinformation.
- Vague provisions that allow discretionary interpretation by law enforcement, prosecutors, and courts and that enable the laws to abuse fundamental rights.
- Holding internet intermediaries liable for content policing.
- Providing for overly harsh and punitive penalties for violations.

Kenya has passed a similar law,[18] and more are under consideration in Nigeria[19] and South Africa.[20] Critics argue that these laws constitute nothing less than online censorship.

4. 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 proposed Prohibition of Hate Speech Bill in Nigeria is an example. The Bill established a national agency to regulate hate speech in Nigeria, and it proposed that:

> "Any person who uses, publishes, presents, produces, plays, provides, distributes and/or directs the performance of any material, written and or visual which is threatening, abusive or insulting or involves the use of threatening, abusive or insulting words or behaviour commits an offence if such person intends thereby to stir up ethnic hatred, or having regard to all the circumstances, ethnic hatred is likely to be stirred up against any person or person from such an ethnic group in Nigeria."

It further proposed the punishment of persons guilty of this offence with life in prison or, if the act results in the loss of life, the death sentence. Since 2019, the Bill has been reported as being an "epic fail" and received opposition from ordinary citizens and civil society organisations. In 2023, Nigeria then introduced the National Broadcasting Commission Bill which regulates digital platforms.

Civil society has argued that such a broad definition is open to subjective interpretation by law enforcement and would pose a threat to critical opinion, satire, public dialogue, and political

[17] CIPESA, Edrine Wanyama, 'Ethiopia's New Hate Speech and Disinformation Law Weighs Heavily on Social Media Users and Internet Intermediaries' (2020) (accessible here).
[18] Mail & Guardian, 'Kenya signs bill criminalizing fake news' (2019) (accessible here).
[19] Amnesty International, 'Nigeria: bills on hate speech and social media are dangerous attacks on freedom of expression' (2019) (accessible here).
[20] Daily Maverick, Pierre de Vos, 'Hate speech bill could be used to silence free speech' (2019) (accessible here).

commentary, and is particularly concerning in light of the exceptionally harsh penalties imposed.[21]

5. 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,[22] following the role of the media in perpetuating hatred against Jewish people in Germany and advocating for their extermination. In the landmark ICJ case of *South Africa v Israel*, **South Africa** argued that the language used by Israeli soldiers and entertainers about Palestinians in Gaza sparked war and is proof of Israel's intent to commit genocide. One of the provisional orders made by the ICJ in its judgment is for Israel to take measures within its power to prevent and punish the direct and public incitement of genocide. The ICJ referred to comments made by senior Israeli politicians that contained inciting and dehumanising rhetoric.[23]

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.[24] Two of the respondents were the founders of a radio station that broadcast anti-Tutsi propaganda before the **Rwandan** genocide and the names and licence plate numbers of intended victims during the genocide.[25]

The Rome Statute establishing the International Criminal Court also establishes the crime of incitement to genocide.[26]

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

[21] Amnesty International, 'Nigeria: Bills on hate speech and social media are dangerous attacks on freedom of expression,' (2019) (accessible here),
See also Sandra Eke, 'Nigeria: A Review Of The Hate Speech Bill,' (2020) Mondaq (accessible here).
[22] United Nations General Assembly, Convention on the Prevention and Punishment of the Crime of Genocide, Resolution 260 (III) (1948), Art. 3.(accessible here).
[23] Article 19 'Israel: The ICJ orders measures to prevent incitement to genocide and preserve evidence' 2023 (accessible here).
[24] International Criminal Tribunal for Rwanda, Case No. ICTR-99-52-T, (2003) (accessible here).
[25] Media Defence above at n 2.
[26] International Criminal Court, 'Rome Statue of the International Criminal Court' at Articles 6, 25 and 33 (2002) (accessible here)..

European Court of Human Rights jurisprudence, even when compared to similar cases of historical revisionism.[27]

Rwanda and the ideology of genocide, sectarianism, and divisionism

In 2017, the African Court on Human and Peoples' Rights dealt with a case concerning speech that allegedly spread "the ideology of genocide, sectarianism, and divisionism" in *Ingabire Victoire Umuhoza v Rwanda*.[28] The case related to the arrest of a leader of a **Rwandan** political party who had made statements relating to the Rwanda Genocide and, more specifically, highlighting that crimes against humanity were committed against the Hutu people and not only the Tutsi people. The Court found that Rwanda had violated the right to freedom of expression and that the restriction was not necessary and proportional, because the speech did not deny or minimise the crimes committed against the Tutsis and were statements "of the kind that is expected in a democratic society and should thus be tolerated, especially when they originate from a public figure as the Applicant is."

In 2021 the Africa Commission received a case, *Agnes Uwimana-Nkusi v Rwanda*, that concerned the conviction of journalists Agnes Uwimana-Nkusi and Saidati Mukakibibi on the grounds of defamation and threatening national security following the publication of three articles criticising the government.[29] The journalist published articles detailing allegations of corruption among high-profile public officers, the human rights situation in Rwanda, and other government shortcomings. The government argued that the articles intended to incite violence and strife against the government by using defamatory statements devoid of evidence.

Having exhausted all available domestic remedies, Media Dence (Media Legal Defence Initiative as it was then), filed a complaint to the Commission on behalf of the journalists arguing Rwanda violated their rights to freedom of expression and to a fair trial. The Commission considered whether discussing the 1994 Rwanda Genocide amounted to genocide denial. Considering Rwanda's history, it assessed if implementing penal code articles was necessary and proportionate. The Commission emphasised democratic governance contexts in evaluating public order protection and incitement definitions. While acknowledging the sensitivity around the genocide, it found the journalists' articles did not incite violence or threaten security. The Commission criticised criminal defamation laws, deeming them disproportionate restrictions on journalism. It stressed the vital role of freedom of expression in democracy, particularly in fostering political discourse and holding officials accountable. Consequently, the Commission ruled Rwanda's actions violated Article 9 of the Charter by unjustly restricting the journalists' freedom of expression.

6. RELIGIOUS DEFAMATION

[27] 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.
[28] *Ingabire Victoire Umuhoza v. Rwanda* (2018) (accessible here).
[29] *Agnes Uwimana-Nkusi v. Rwanda* (2021) (accessible here). See also Global Freedom of Expression at Columbia University, 'Case update: Agnes Uwimana-Nkusi v. Rwanda (accessible here).

Many African states have laws prohibiting the 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:[30]

> "…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.[31]
- Six other African countries, including **Somalia** and **Egypt**, have scored 'higher than average' on the harshness of their religious defamation laws.[32]
- In 2022 the **Nigerian** High Court, in the case of *State v Muhhammad Mubarak Bala*, convicted the respondent in the case of blasphemy and causing a public disturbance because of messages he posted on his personal Facebook page in March 2020, which were seen as disrespectful to religious beliefs and potentially causing trouble to the community.[33] The respondent spent a year in police custody without formal charges being laid. The Court held that the Applicant did not provide sufficient evidence to avoid conviction which then led to his 24-year prison sentence for these offences. This highlights the concerns about stifling freedom of expression through religion and expresses a lack of tolerance for dissenting views.

General Comment 34 states that:[34]

> "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."

In 2017, the UN Special Rapporteur on freedom of religion or belief called on States, in his first report to the UN General Assembly, to repeal blasphemy laws because of their stifling

[30] End Blasphemy Laws, 'Ethiopia,' (2020) (accessible here).
[31] 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 here).
[32] *Ibid* at page 15.
[33] *State v Muhhammad Mubarak Bala* K/89C/2021 (accessible here).
[34] UN Human Rights Council, 'General Comment No. 34 at p 12 (2011) (accessible here).

effect on the right to freedom of religion or belief and on the ability to engage in a healthy dialogue about religion.[35]

Many other countries have abolished the offence of blasphemy in recent years, for example, the United Kingdom in 2008,[36] Canada in 2018,[37] and Denmark in 2017.[38]

The Constitutional Court of **South Africa** grappled with religious hate speech in the case of *South African Human Rights Commission v Masuku*,[39] which concerns whether statements made by the respondent constitute hate speech against Jewish people in terms of the Equality Act. Ultimately, the Court applied the new definition of 'hate speech' as decided in the *Qwelane* matter (discussed above) and found that while one of the statements made did constitute hate speech, the others did not as they did not specifically target members of the Jewish faith or ethnicity.

7. 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 about whether this is justified. Related crimes such as blasphemy are beginning to be removed in progressive jurisdictions, and African states that have not yet removed these crimes should be encouraged to follow suit.

[35] UN Special Rapporteur on the right to freedom of religion or belief, 'Elimination of all forms of religious intolerance,' (2017) (accessible here).
[36] Media Defence, 'Training Manual on International and Comparative Media and Freedom of Expression Law', Richard Carver, (2020) (accessible here).
[37] Global News Wire, 'Repeal of Canada's Blasphemy Law Applauded by National Secularist Organization' (2018) (accessible here).
[38] The Guardian, 'Denmark scraps 334-year old blasphemy law' (2017) (accessible here).
[39] *South African Human Rights Commission v Masuku* (2019) (accessible here).

Module 7

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

ISBN 978-0-9935214-1-6
Published by Media Legal Defence Initiative: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in April 2024

TABLE OF CONTENTS

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 States to suppress dissent and the media.**
- **The African Union (AU) has encouraged a harmonised, continent-wide approach to tackling cybercrimes in Africa, as seen in long-awaited African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) which came into force in 2023.**
- **Data privacy is starting to attract more widespread attention across the continent, with many countries recently passing new data protection legislation.**
- **Concerningly, many cybercrimes have a particularly gendered nature, such as cyberstalking and the non-consensual sharing of intimate images (NCII).**
- **There are, however, various practical steps that can be taken to address cybercrimes and ensure that fundamental rights are equally protected both off- and online.**

1. INTRODUCTION

The increase in internet access in the recent past has created a number of new legal challenges. The internet is transnational, amorphous, and difficult to define, and as such 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.

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 are losing $4 billion annually due to cybercrimes,[1] roughly 10% of the continent's GDP,[2] and Africa now has the third highest number of cybercrime victims in the world.[3] in 2023, Africa continued to be one of the world's regions targeted most by cybercrime due to the increased digitisation

[1] World Economic Forum, 'Africa must act now to address cybersecurity threats. Here's why' (2022) (accessible here).
[2] Interpol, 'African Cyberthreat Assessment Report,' (2021) at p 9 (accessible here).
[3] Caryn Dolley, 'Cyberattacks: South Africa, you've been hacked,' Daily Maverick (2021) (accessible here).

of organisations without the necessary corresponding cybersecurity practices.[4] Without adequate regulatory frameworks and protections, the growth of internet access, e-commerce, and economic development is likely to 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.

Africa Cyber Surge II

INTERPOL and AFRIPOL collaborated on a joint operation spanning 25 African nations, resulting in the arrest of 14 suspected cybercriminals and the identification of 20,674 suspicious cyber networks, shedding light on the escalating digital insecurity and cyber threats prevalent in the region. These networks were found to be associated with financial losses exceeding USD 40 million.[5]

Dubbed Africa Cyber Surge II, the four-month operation commenced in April 2023 with a focus on uncovering cybercriminals and compromised infrastructure. Led by INTERPOL's Cybercrime Directorate, in conjunction with the INTERPOL Africa Cybercrime Operations desk and the INTERPOL Support Programme for the African Union regarding AFRIPOL (ISPA), the initiative aimed to enhance communication, analysis, and intelligence sharing among participating countries. By fostering collaboration among African law enforcement agencies, the operation aimed to prevent, investigate, and disrupt cyber extortion, phishing, business email compromise, and online scams.

This operation underscored the efficacy of cybersecurity initiatives when international law enforcement, national authorities, and private sector partners join forces to exchange insights and proactively combat cybercrime. With support from private sector entities such as Group-IB and Uppsala Security, the operation leveraged actionable intelligence to drive its efforts forward, emphasizing the importance of cooperation in safeguarding digital landscapes.

As far back as 2011, the 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

[4] Interpol, 'African Cyberthreat Assessment Report Cyberthreat Trends' (2023) (accessible here).
5 Interpol, 'Cybercrime: 14 arrests, thousands of illicit cyber networks disrupted in Africa operation' (2023) (accessible here).

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."[6]

2. WHAT IS A CYBERCRIME?

2.1. 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.[7] 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.[8]

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.[9]

2.2. 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).[10] 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."[11] However, even the AU itself was the target of a major cyberattack between 2013 and 2017,[12] 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.[13]

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:

---

[6] United Nations General Assembly, Human Rights Council, 17th Session, 'Report of the Special Rapporteur on freedom of expression' at p 10 (2011) (accessible here).
[7] Article 19, 'Freedom of Expression and ICTs: overview of international standards' at p 25 (2018) (accessible here).
[8] *Id.*
[9] ITU Definition of Cybersecurity, (accessible here).
[10] Institute for Security Studies, Karen Allen 'Is Africa cybercrime savvy?' (2019) (accessible here).
[11] African Union, 'A global approach on Cybersecurity and Cybercrime in Africa' (accessible here).
[12] Le Monde, 'A Addis-Abeba, le siège de l'Union africaine espionné par Pékin' (2018) (accessible here).
[13] African Union 'Convention on Cyber Security and Personal Data Protection' (2014) Article 3(g) (accessible here).

> "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."[14]

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."[15]

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 cybercrime legislation.[16]

2.3. Cybercrimes in domestic law

The UN Conference on Trade and Development (UNCTAD) reports that 39 out of the 54 countries in Africa analysed (72%) have cybercrime legislation in place.[17]

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.[18]

[14] *Id*.
[15] UN General Assembly, Fifty-seventh session, 'Resolution on the Creation of a global culture of cyber security, at p 3 (accessible here).
[16] Council of Europe, 'Budapest Convention and Related Standards', (accessible here).
[17] UNCTAD, 'Cybercrime Legislation Worldwide' (accessible here).
[18] Media Defence, 'Training manual on digital rights and freedom of expression online, at p 62 (2020) (accessible here).

3. TYPES OF CYBERCRIMES

3.1. Data privacy violations

The use of data, including the volume of cross-border data flows, is increasing exponentially every year, particularly in relation to personal data. However, there is a lack of adequate regulations over the collection and processing of personal information in Africa. 33 African countries currently have data protection or cybercrime laws in place,[19] but their comprehensiveness and effectiveness vary significantly. The progression of legislation and regulation in this area has been rapid in Africa in recent years. At present, 36 African countries have passed data protection laws, with three further being in the process of considering drafts. Most recently, **Tanzania**, **Uganda** and **Eswatini** passed new data protection laws in 2022 and **Nigeria** and **Somalia** in 2023. **Kenya** also passed new regulations to their data protection law in 2021, in an effort to strengthen their existing law.

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.[20] 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.[21]

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.

In **Kenya**, the High Court in Nairobi ruled in 2020 in *Nubian Rights Forum and Others v The Hon. Attorney General and Others*[22] that the government could not implement a new comprehensive digital identity system without an adequate data protection law being in place. On surveillance, the Constitutional Court of **South Africa** found in the case of *amaBhungane and Another v Minister of Justice and Correctional Services and Others*[23] in 2021 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

[19] United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation Worldwide' (2021) (accessible here).
[20] Forbes, 'California Begins Enforcing Broad Data Privacy Law – Here's What You Should Know' (2020) (accessible here).
[21] The Guardian, 'California's groundbreaking privacy law takes effect in January. What does it do?' (2019) (accessible here).
[22] High Court of Kenya in Nairobi, Consolidated petitions no. 56, 58 & 59 of 2019, (2020) (accessible here).
[23] Constitutional Court of South Africa, Case No. CCT 278/19, (2021) (accessible here).

Communications and Provision of Communication Related Information Act (RICA) unconstitutional.

3.2. Criminalisation of online speech

Cybercrime 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 sexual abuse material (CSAM), blasphemous content, content critical of states and their institutions, and content unauthorised by intellectual property rights holders.[24]

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:

- child pornography;[25]
- direct and public incitement to commit genocide;
- hate speech;
- defamation; and
- incitement to discrimination, hostility or violence.[26]

Even legislation that does criminalise these forms of expression needs to be precise, have adequate and effective safeguards against abuse or misuse and include oversight and review by an independent and impartial tribunal or regulatory body.[27] 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."[28]

In **Zimbabwe**, for example, the Cyber Security and Data Protection Act passed in 2021,[29] 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."[30] However, the Act has been widely criticised as being a tool for the Zimbabwean government to stifle freedom of expression and access to information, promote interference of private communications and data and use search and seizure powers to access the

[24] Article 19, 'Freedom of Expression and ICTs' (2018) (accessible here).
[25] Although this term is used the report, the preferred terminology is "Child sexual assault material" (CSAM).
[26] United Nationals Special Rapporteur on the Right to Freedom of Opinion and Expression, Frank La Rue, (2011) at para 25 (accessible here).
[27] *Id* at para 71.
[28] United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression, (2018) at para 13 (accessible here).
[29] Zvamaida Murwira, 'Zimbabwe: Milestone Cyber Security Bill Sails Through Parly,' AllAfrica (2021) (accessible here).
[30] ALT Advisory Africa, 'Zimbabwe gazettes Cyber Security and Data Protection Bill' (2020) (accessible here).

information of activists in order to quell protests.[31] Before it was passed, MISA-Zimbabwe 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."[32]

Prominent journalists and activists have seen been arrested under these provisions, leading to criticism that the Act criminalises digital activism.[33]

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.

3.3. 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.[34] Furthermore, women encounter sexualised forms of online harassment at much higher rates than men.[35] Journalists are also particularly at risk due to their public-facing roles and efforts to stifle independent media: research by UNESCO has found that almost three-quarters of women journalists have experienced online violence.[36]

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 affecting 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 the non-consensual dissemination of intimate images (NCII), often leaving victims with little recourse against perpetrators.[37]

[31] Paradigm Initiative, 'On Zimbabwe's Approval of a Cybercrime and Cybersecurity Bill' (2019) (accessible here).
[32] MISA-Zimbabwe, 'Commentary on Cybersecurity and Data Protection Bill HB 18 of 2019' (2019) (accessible here).
[33] MISA-Zimbabwe, 'Analysis of the Data Protection Act,' Kubatana (2021) (accessible here).
[34] Pew Research Center, 'Online harassment 2017' (2017) (accessible here).
[35] *Id*.
[36] UNESCO, 'Top 26 Preliminary Findings' (accessible here).
[37] 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

South Africa is an exception, having passed the Film and Publications Board Amendment Act[38] 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."[39]

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.)[40]
- 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.[41]

The importance of a name:

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:[42]

- 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.

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 here).

[38] South Africa Film and Publications Board Amendment Act, 2019 (accessible here).

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

[40] See Case No. A3032-2016 in the High Court of South Africa for reference (2017) (accessible here).

[41] News24, Oberholzer, 'What to do if you're a victim of revenge porn & image-based abuse' (2020) (accessible here).

[42] GenderIT, '"Revenge Porn": 5 important reasons why we should not call it by that name' (2019) (accessible here).

- 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.[43]

- Lastly, the term oversimplifies the offence by ignoring a range of aggressors and motivations and invoking a moralist reaction against the victim.[44]

Many stalking crimes begin online before moving offline,[45] 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."[46]

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."[47]

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

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*,[48] the High Court of **South Africa** granted an interdict in favour of the

[43] Id.
[44] 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 here).
[45] South Africa Law Reform Commission, 'Report on Stalking' (2006) (accessible here).
[46] Id at p 182.
[47] Id at p 183.
[48] High Court of South Africa in Johannesburg, Case No 23897/17, (2017) (accessible here).

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."[49]

3.2. 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 adults.[50] 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."[51]

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.[52]

[49] *Ibid* at para. 29.
[50] 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 here).
[51] UNICEF, 'Cyberbullying: What is it and how to stop it' (accessible here).
[52] UNICEF, 'UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying' (2019) (accessible here).

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 was pitted against one of the largest technology companies in the world, Facebook, the former owner of Instagram.[53] The girl, believing the threats were from someone attending her school, feared for her physical safety and therefore attempted 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 example of the 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.

3.2. 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.[54] 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.[55] It is also open for any state willing to implement its provisions to join and can be ratified by African countries.[56]

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.[57]

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

[53] Daily Maverick, 'Anonymously threatened with gang rape and murder, SA teenager takes Facebook Inc to court to disclose perpetrator' (2020) (accessible here).
[54] Council of Europe, 'The State of Cybercrime Legislation in Africa – an Overview' at p 2 (2015) (accessible here)
[55] Council of Europe, 'The global state of cybercrime legislation 2013 – 2020: A cursory overview,' at p 5 (2020) (accessible here).
[56] Council of Europe, 'Chart of signatures and ratifications of Treaty 185' (2020) (accessible here).
[57] Council of Europe above n 54 at p 8.

4. TRENDS IN AFRICA

Malabo Convention enters into force after nine years

Adopted by the African Union in 2014, the AU Convention on Cybersecurity and Personal Data Protection, known as the Malabo Convention, finally took effect in June 2023 following Mauritania's ratification, becoming a vital regional treaty for safeguarding personal data in Africa. Despite its significance, the Convention's lengthy nine-year journey to ratification highlights the need for updates to address evolving digital technologies' impact on personal information usage.58

The Convention's implementation marks a crucial stride in Africa's cybersecurity and data protection efforts. Envisioned to establish a comprehensive legal framework for electronic commerce, data protection, and cybercrime and cybersecurity, the Convention necessitates all 55 AU member states to align their domestic laws with its standards and principles once operational. However, concerns over the Convention's lack of detail and enforcement mechanisms have been raised alongside its positive reception.

Moving forward, effective implementation and gap addressing become paramount. The AU Commission can spearhead this by formulating implementation guidelines and action plans, enhancing human rights protection in artificial intelligence use, ensuring adequate resourcing for domestic data protection frameworks, and instituting regional oversight bodies. Supporting data protection authorities and fostering alignment across the continent will be crucial in actualizing the Convention's objectives.

According to Data Protection Africa and the AU's latest status list on the Malabo Convention, dated 12 May 2023, lists the following 15 states as having submitted ratification:

- Angola (11 May 2020)
- Cape Verde (5 February 2022)
- Côte d'Ivoire (3 April 2023)
- Congo (23 October 2020)
- Ghana (3 June 2019)
- Guinea (16 October 2018)
- Mozambique (21 January 2020)
- Mauritania (9 May 2023)
- Mauritius (14 March 2018)
- Namibia (1 February 2019)
- Niger (16 March 2022)
- Rwanda (21 November 2019)
- Senegal (16 August 2016)
- Togo (19 October 2021)
- Zambia (24 March 2021)

58 ALT Advisory, 'AU's Malabo Convention set to enter force after nine years' (2023) (accessible here).

In addition, the following states are listed as having signed the Malabo Convention without yet ratifying it:

- Benin
- Cameroon
- Chad
- Comoros
- Djibouti
- Gambia
- Guinea-Bissau
- South Africa
- Sierra Leone
- Sao Tome and Principe
- Sudan
- Tunisia

As the AU has previously noted that:

> "[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."[59]

As a result, many African governments have been keenly adopting new cybercrime legislation in an attempt to keep pace and to continue to protect against crimes committed online. Currently, at least 39 African states have basic cybercrime legislation either fully or partially in place, though many are missing implementing regulations.[60]

However, cybercrime 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.[61] This is a growing concern among human rights defenders regarding a wave of arrests and convictions of activists and journalists 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.[62] The Committee to Protect Journalists states that in

[59] African Union above n 11 at p 3.
[60] UNCTAD above n 19.
[61] Access Now, 'When "cybercrime" laws gag free expression: stopping the dangerous trend across MENA' (2018) (accessible here).
[62] Committee to Protect Journalists, Peter Nkanga 'How Nigeria's cybercrime law is being used to try to muzzle the press' (2016) (accessible here).

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."[63] 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.[64] In 2020, the ECOWAS Community Court of Justice (ECOWAS Court**)** ruled that section 24 of the Act — which criminalises the sending of grossly offensive, indecent, or false messages — did not align with Nigeria's obligations under the African Charter and the ICCPR, and ordered Nigeria to repeal or amend the law.[65]

Other common problematic clauses in cybercrime legislation include those that criminalise the "creation of sites with a view to disseminating ideas and programmes contrary to public order or morality", "broadcasting information to mislead security forces", "publication of false information," and more.[66] Recently, **Zimbabwe**, **Eswatini**, **Tanzania**, **Zambia**, **Uganda**, **Rwanda**, and **Malawi** have recently passed cybercrimes legislation.[67] Zambia's Cyber Security and Cyber Crimes Act is currently being challenged at the Constitutional Court by a group of civil society organisations alleging that it contains provisions that threaten the right to protection of the law and the right to freedom of expression.[68]

In the case of *Andare v Attorney General of Kenya*,[69] 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.[70]

5. STEPS TO TAKE IN RESPONSE TO ONLINE HARMS

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

5.1. 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, 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.

[63] *Id.*
[64] OrderPaper, 'Tomiwa Ilori, The Nigerian Cybercrimes Act 2015: Is It Uhuru Yet?' (accessible here).
[65] The Incorporated Trustees of Laws and Rights Awareness Initiatives v Nigeria, ECOWAS Court Suit No. ECW/CCJ/APP/53/2018 (2020) (accessible here).
[66] *Id* at p 8.
[67] Media Defence, 'Mapping Digital Rights and Online Freedom of Expression Litigation in East, West and Southern Africa,' (2020) (accessible here).
[68] MISA-Zimbabwe, 'Zambia's newly enacted cybercrime law challenged in court' (2021) (accessible here).
[69] High Court of Kenya at Nairobi, Petition No. 149 of 2015 (2015) (accessible here).
[70] See also, *Shreyal Singh v India*, Writ 167 of 2012 (accessible here).

- **Consider domestic legal challenges.** Many cybercrime 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 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 or domestic avenues have been exhausted, there may be recourse in regional human rights courts such as the ECOWAS Court, 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.[71]

5.2. 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 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.[72]

- **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 review the relevant platforms' terms of use prior to reporting to identify the most salient term that has been violated.[73]

6. 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.

[71] International Justice Resource Center, 'Courts and Tribunals of Regional Economic Communities' (accessible here).
[72] Department of Justice and Constitutional Development, Protection from Harassment Act, 2011 (accessible here).
[73] Complaints platforms are available here: Facebook; Instagram; X; YouTube; and TikTok.

Module 8

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

ISBN 978-0-9935214-1-6
Published by Media Legal Defence Initiative: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in April 2024

TABLE OF CONTENTS

MODULE 8

DISINFORMATION, MISINFORMATION AND PROPAGANDA

- **Disinformation refers to content purporting to be news that is intentionally and verifiably false and that seeks to mislead readers.**
- **While acknowledging the social ills occasioned by disinformation 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 considered for 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.**

1. INTRODUCTION

The phenomenon of dis- and misinformation has increased exponentially in recent times with the advent of the internet and social media platforms. While manipulating and distorting information has been squarely part of the historical record for many years, the weaponisation of information in the 21st century is occurring on an unprecedented scale and requires urgent and effective responses.[1] In July 2021, the Special Rapporteur on the promotion of the right to freedom of opinion and expression published a report on disinformation and freedom of opinion and expression. This Report defines disinformation in this digital age as a "pathway for false or manipulated information to be created, disseminated, and amplified by various

[1] UNESCO, 'Journalism, 'Fake News' and Disinformation: Handbook for Journalism Education and Training (2018) (UNESCO Handbook) (accessible here).

actors for political, ideological or commercial motives at a scale, speed and reach never known before".[2]

This module focuses on disinformation, misinformation, and propaganda and provides guidance on media and information literacy (MIL) strategies and campaigns which may assist with mitigating misinformation while ensuring that the right to freedom of expression is not violated. [3]

'Fake news' – a common but unhelpful term

South African civil society organisation Media Monitoring Africa explains that—

> "while a common term, "fake news" is not commonly understood and is often misused to sow division and mistrust. In recent years the term has been misappropriated by powerful actors who weaponize the term "fake news" to confuse, polarise, mislead, and create distrust of genuine news.8 Politicians, for example, have been known to call information "fake news" when the information does not align with their views. Its imprecise nature also means that it encompasses a spectrum of information types, ranging from relatively low-risk forms – such as honest mistakes made by reporters, political discourse, and the use of clickbait headlines – to high-risk forms – malicious fabrications or content that such as content that undermines political processes."[4]

For these reasons, this module uses misinformation and disinformation rather than fake or false news.

Increasingly, strategies to combat mis- and disinformation should be more social and educational in their character in order to ensure that the right to freedom of expression is not violated by overly-broad legislative provisions which criminalise or chill expression. Combatting misinformation should fall more within the realm of advocacy and education than that of 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.

2. WHAT IS MIS- AND DISINFORMATION

Although definitions of misinformation and disinformation are not universally agreed upon, especially in the online realm, we can glean insights from emerging interpretations of these concepts for comparative purposes.[5]

[2] United Nations General Assembly 'Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (2021) (accessible here).
[3] *Id* at p 70 (accessible here.
[4] Media Monitoring Africa, 'Disinformation through a children's rights lens' (2022) (accessible here).
[5] UNESCO Handbook above 1 at p 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".[6]
Misinformation	Misinformation is information that is false, but the person who is disseminating it believes that it is true.[7]
Mal-information	Mal-information is information that is based on reality but is used to inflict harm on a person, organisation or country.[8]

Disinformation refers to content purporting to be news that is intentionally and verifiably false and that seeks to mislead readers. In June 2023, the United Nations Secretary-General published a policy brief on information integrity on digital platforms. This policy brief recognises fake news sites that are made to look legitimate as one tactic of dis-information and attributes the difficulty in tracking the true scale of false news to the cloned versions of news sites and articles that are made to look legitimate. In the public address accompanying the launch of the policy brief, the Secretary-General noted with concern the impact that the rapid growth of generative artificial intelligence and digital platforms has on spreading mis- and dis-information globally.[9] The Secretary-General notes further that digital platforms have done little to reduce the spread of hate speech and mis- and misinformation on their platforms. Some of the proposals made by the policy brief are for:

- Governments, technology companies, and other involved parties should avoid using, endorsing, or promoting disinformation and hate speech for any reason.
- Governments ought to ensure a free, sustainable, independent, and diverse media environment, providing robust safeguards for journalists.
- Digital platforms need to prioritize safety and privacy in the design of all products. They should consistently apply policies and allocate resources across different countries and languages.
- All those involved should swiftly implement measures to ensure that all applications of artificial intelligence are safe, secure, responsible, and ethical, complying with human rights obligations.

For the purposes of this module, the term "misinformation" is used broadly and, unless otherwise specified, includes reference to disinformation and mal-information. The term 'false news' is not preferred unless referring to legal provisions regulating such, for the reason that the concept of 'news' should not be conflated with false information. Misinformation should not be confused with quality journalism and the circulation of trustworthy information which complies with professional standards and ethics.[10] Misinformation and its ilk are not new but rather have become increasingly more powerful as they are fuelled by new technologies and

[6] *Id* at p 44-5.
[7] *Id.*
[8] *Id.*
[9] United Nations 'Global Threat of Online Mis- and Disinformation and Hate Speech, says UN Secretary-General' (2023) (accessible here).
[10] UNESCO Handbook above n 1 at p 18.

rapid online dissemination. The consequence is that digitally-driven misinformation, in contexts of polarisation, risks eclipsing quality journalism, and the truth.[11]

Prevalence of mis- and disinformation

The 2017 Joint Declaration on Freedom of Expression and 'Fake News,' Disinformation and Propaganda (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.

More recently, in October 2023, at the African Commission on Human and Peoples Rights held its 77th Ordinary Session the LEXOTA disinformation tracker was launched to explore and track the role of the government and law in curbing disinformation and its impact on freedom of expression.[12] The tracker operates in real time and monitors 44 out of the 55 African countries making it a highly effective tool to curb disinformation.

2.1. The human rights implications of mis- and disinformation

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). The 2023 Joint Declaration on Media Freedom and Democracy, stressed that mandate holders should:[13]

- Adhere to high standards of information provision that meets recognised professional and ethical standards;
- Refrain and distance themselves from disinformation, discrimination, hate speech and propaganda. Media should never serve as a vehicle for propaganda for war. In case of incidental errors in their reporting, the media should promptly correct the information.
- Media should proactively work towards identifying and changing harmful stereotypes and should counteract disinformation, hate speech, discriminatory norms and attitudes as well as negative prejudice in their coverage and reporting.

Principle 22 of the 2019 ACHPR principles calls on states to repeal laws in their respective countries that criminalise the publication of false news.[14] This recommendation likely stems

[11] *Id.*
[12] CIPESA 'Effects of Disinformation on the Digital Civic Space Spotlighted at the African Commission' (2023) (accessible here).
[13] United Nations Human Rights Special Procedures, 'Joint declaration on media freedom and democracy' (accessible here).
[14] ACHPR, 'Declaration of Principles on Freedom of Expression and Access to information in Africa (2019) (accessible here).

from concerns about the potential misuse of calls to curb mis- and dis-information and attempts to establish a balance between combating misinformation and protecting individuals right to free expression.

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 for 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."

2.2. Causes of misinformation

To understand how to combat misinformation, it is useful to first understand its causes and 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.[15] Equally, the speed at which information is transmitted and the instant access to information that the internet provides has caused a rush to publish and be the first to transmit information. This, alongside more insidious practices such as the intentional distribution of disinformation for economic or political gain, has created what the United Nations (UN) Educational, Scientific and Cultural Organisation (UNESCO) refers to as a "perfect storm".[16]

[15] Id at p 55.
[16] Id.

In the UN Secretary-General's report titled "Our Common Agenda", it was noted that while the UN vehemently upholds the universal right to freedom of expression, it is crucial to foster a collective, evidence-based agreement within societies regarding the public value of facts, science, and knowledge.[17] Efforts to enable this include:

- Reestablishing the moral imperative against lying. Institutions can serve as a "reality check" for communities, mitigating disinformation, countering hate speech, and addressing online harassment, particularly against women and girls.
- Expediting efforts in generating and disseminating trustworthy, verified information.

The UN, with its pivotal role, can enhance these efforts, drawing inspiration from successful models such as the Intergovernmental Panel on Climate Change, the World Meteorological Organization Scientific Advisory Panel, or the Verified Initiative for COVID-19.

Additional measures involve:

- supporting independent media in the public interest
- regulating social media, fortifying freedom of information laws, and
- ensuring significant representation of science and expertise in decision-making through entities like science commissions.

A collaborative exploration of a global code of conduct promoting integrity in public information is proposed, involving states, media outlets, and regulatory bodies, facilitated by the United Nations. Given contemporary concerns about trust and distrust related to technology and the digital realm, there's a recognised need to better understand, regulate, and manage our digital commons as a global public good.

These causes continue to pose difficulties for newsrooms, journalists, and social media users as 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.

2.3. Content moderation by private actors

As private technology platforms have grown their audiences around the world and become increasingly powerful, the decisions they make internally as to how to moderate the content appearing on their platforms have become increasingly consequential for the protection of freedom of expression and access to information in the digital age. How these platforms make decisions about removing or downgrading content they classify as mis- or disinformation requires transparency and accountability in order to ensure the protection of rights and the creation of an enabling information ecosystem. Even decisions about which content is shown to users and how (for example, ranking and curating of feeds) have the potential to affect freedom of expression and access to information.

[17] United Nations, 'Our Common Agenda: Report of Secretary-General' (2021) (accessible here).

Rarely do the community standards enforced by these companies accord with domestic legal provisions that regulate, for example, hate speech or propaganda. Research has also found that untargeted or disproportionate content moderation disproportionately impacts marginalised persons, mainly through disregarding their experiences on social media.[18]

While it is important to ensure that states do not approach intermediaries such as social media platforms to attempt to remove online content outside the bounds of the law, it is increasingly apparent that there is a need for greater oversight over the decisions these companies make that affect fundamental rights.

In this regard, the case of *UEJF v. Twitter* in France is instructive. As described by the Columbia Global Freedom of Expression Case Law Database:

> "The Paris Court of Appeal confirmed an order from the Paris Tribunal ordering Twitter to provide information on their measures to fight online hate speech. Six French organizations had approached the Court after their research indicated that Twitter only removed under 12% of tweets that were reported to them and sought information on the resources Twitter dedicated to the fight against online racist, anti-Semitic, homophobic speech and incitement to gender-based violence and commission of crimes against humanity. The Paris Tribunal had ruled that Twitter provide this information, and despite Twitter's argument in the Court of Appeal that they had no statutory obligation to disclose this information, the Court held that the organizations were entitled to the information to enable them to determine whether to file an application under French law that Twitter was not promptly and systematically removing hate speech from their platform."[19]

2.4. Legal responses to mis- and disinformation

False news provisions are laws which prohibit and punish the dissemination of false or inaccurate statements. The criminalisation of false news has been struck down in various countries.[20] For example, in the matter of *Chavunduka and Another v Minister of Home Affairs and Another*,[21] 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:

---

[18] Eugenia Sipaer, 'AI Content Moderation, Racism and (de)Coloniality', International Journal of Bullying Prevention' (2021) at p 61 (accessible here).
[19] Columbia Global Freedom of Expression Database, 'UEJF v. Twitter,' (2022) (accessible here).
[20] Unfortunately, examples also exist of such legislation being held, such as in The Gambia (*Gambia Press Union v. Attorney General* 2018) (accessible here).
[21] Supreme Court of Zimbabwe, 2000 (1) ZLR 552 (S) (accessible here).

> "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" of 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. Unfortunately, false news provisions have since found their way into other legislation in Zimbabwe and have been used to justify the arrest and silencing of critics and journalists.[22] Zimbabwe's Data Protection Act, which, as of January 2024 has been enacted but is not yet in force, criminalises the spreading of false information online. The Act states that any person who unlawfully and intentionally makes available, broadcasts, or distributes data to any other person concerning an identified or identifiable person knowing it to be false, with intent to cause psychological or economic harm, will be guilty of an offence. Civil society has raised concerns that this provision promotes self-censorship, and unjustifiably infringes on freedom of expression.[23]

Courts in other countries have also grappled with these issues:

- In **Botswana**, a journalist was criminally charged for alarming publications in 2022.[24] This charge is contained in Botswana's Penal Code and can result in the journalist facing up to two years of imprisonment or a fine.

- In the case of *Media Council of Tanzania v Attorney General*, the East African Court of Justice unanimously ruled that several sections of **Tanzania's** Media Services Act were

[22] Including section 31 of the Criminal Law (Codification and Reform Act) and the Cybersecurity and Data Protection Act. Media Defence, 'Mapping Digital Rights and Online Freedom of Expression Litigation in East, West and Southern Africa,' (2020) p 35 (accessible here).
[23] MISA-Zimbabwe, 'Analysis of the Data Protection Act,' (2021) (accessible here).
[24] Committee to Protect Journalists, 'Botswana journalist Tshepo Sethibe criminally charged over 'alarming publications' (accessible here). See SALC, 'False news or free speech: Protecting freedom of expression in Botswana' (2023) (accessible here).

in violation of the Treaty for the Establishment of the East African Community.[25] The court found that these provisions encroached upon the right to freedom of expression. The legal challenge was initiated by three non-governmental organizations in Tanzania that were troubled by the legislation's use of criminal offences for defamation, false news, and other media-related conduct. They also raised concerns about restrictions on the publication of certain content and mandatory media accreditation. The Court determined that the Tanzanian government had not successfully demonstrated the legitimacy of the restrictions imposed by the law on the right to freedom of expression. It concluded that the contested provisions of the Act breached the treaty by infringing on the right to freedom of expression safeguarded by the African Charter on Human and Peoples' Rights. As a remedy, the Court instructed Tanzania to bring the Media Services Act into alignment with the provisions of the Treaty.

- In 2014, the High Court of **Zambia** in *Chipenzi v. The People* likewise struck down a provision in the country's Penal Code that prohibited the publication of false information likely to cause public fear, holding that it did not amount to a reasonable justification for limiting freedom of expression.[26]

- More recently, the ECOWAS Community Court of Justice delivered a landmark judgment in the case of *Federation of African Journalists and Others v The Gambia*,[27] 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.

    - In a related case, in 2018 the Court of Cassation of Tunis in **Tunisia** in *Attorney General v. N.F* upheld the acquittal of a woman who had been charged with 'publication of false news threatening public order' for publishing statements alleging electoral fraud.[28] The Court held that because the woman had subsequently deleted the post, she could not be found to have criminal intent.

2.5. 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*

[25] *Media Council of Tanzania v Attorney General* (accessible here).
[26] *Chipenzi v. The People*, High Court of Zambia HPR/03/2014 (2014) (accessible here).
[27] ECOWAS Community Court of Justice, Application No. ECW/CCJ/APP/36/15, (2018) (accessible here).
[28] *Attorney General v. N.F.,* Court of Cassation of Tunis 52620-18 (2018) (accessible here)

States v Alvarez[29] 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."[30] MIL strategies and campaigns proposed by organisations such as 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.

2.5.1. Media and Information Literacy (MIL) strategies and campaigns

As a point of departure, MIL strategies and campaigns are a process which enables the detection of misinformation and a means to combat its spread, particularly online.[31] 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.[32]
- **News literacy** which refers to literacy about the news media, including journalistic standards and ethics.[33] 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."[34]
- **Advertising literacy** which relates to understanding how online advertising works and how profits are driven in the online economy.[35]
- **Computer literacy** which refers to basic IT usage and understanding the easy manner in which headlines, images, and, increasingly, videos can be manipulated to promote a particular narrative.[36]
- **Understanding the "attention economy"** which relates to one of the causes of misinformation and the 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.[37]
- **Privacy and intercultural literacy** which relates to developing standards on the right to privacy and a broader understanding of how communications interact with individual identity and social developments.[38]

MIL strategies and campaigns should underscore the importance of media and information literacy in general but should also include a degree of philosophical reflection. According to UNESCO, MIL strategies and campaigns should assist users to "grasp that authentic news

[29] *United States v Alvarez*, 567 U.S. 709 (2012) (accessible here).
[30] *Id* at p 15-6.
[31] UNESCO Handbook above n 1 at .70.
[32] *Id* at p70.
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id* at p 47.
[38] *Id* at p 70.

does not constitute the full 'truth' (which is something only approximated in human interactions with each other and with reality over time)."[39]

2.5.2. Litigation where justifiable limitations exist[40]

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, as well as false statements, can violate the right to freedom of expression, while under-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, including the right to equality and dignity.[41] However, such litigation should consider the potential for unintended consequences and the possibility of jurisprudence which may negatively impact freedom of expression. Depending 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 of Advanced Modules on Digital Rights and Freedom of Expression Online in sub-Saharan Africa.

2.5.3. 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 2022 there were nearly 400 fact-

[39] *Id* at p 72.
[40] See Module 6 of this series for more information on hate speech and justifiable limitations to freedom of expression.
[41] 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 here).

checking projects debunking misinformation in 105 countries around the world, up from about 186 organisations in 2016.[42]

In general, fact-checking and verification processes, which were first introduced by US weekly magazines such as *Time* in the 1920s,[43] 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 newsrooms and publications that employ dedicated fact-checkers.[44]
- **Ex-post fact-checking, verification, and "debunking"**. This method of fact-checking is increasingly popular and focuses on information published after the fact. It focuses on enabling accountability for the veracity of information after publication. 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 misinformation, and the need to debunk viral hoaxes.[45] Alongside MIL strategies and campaigns, fact-checking and social media verification are becoming increasingly important in the fight against misinformation, alongside efforts to build the independence, credibility, and scale of the work of fact-checkers.

The REAL411[46] and PADRE[47]

The Real 411 is an initiative launched in South Africa as 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 and the 2021 local elections, allows users to report disinformation to the Digital Complaints Committee (DCC), which assists a complainant with referrals to one of the multiple statutory bodies in South Africa that 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. The Real411 has since expanded to address online hate speech, incitement, and harassment as well.

The South African Independent Electoral Commission (IEC) partnered with social media platforms to combat disinformation ahead of South Africa's 2024 National and Provincial elections. The IEC together with Google, Meta, TikTok and non-governmental organisations

[42] Duke Reporters' Lab, 'Fact-checkers extend their global reach with 391 outlets, but growth has slowed,' (2022) (accessible here).
[43] UNESCO above n 1 at p 81.
[44] *Id.*
[45] For more resources on the legal defence of factcheckers, see the Fact-Checkers Legal Support Initiative (accessible here).
[46] Accessible here.
[47] Accessible here.

signed a Framework of Cooperation to work together to combat disinformation and other digital harms.[48] The Framework sets out to:

- Establish cooperation during the election period in good faith;
- Foster collaboration that respects existing laws and does not require sharing confidential user data;
- Support the establishment of a Working Group between partners which promotes access to accurate information, conducts awareness campaigns on elections, and provides training to political parties, election candidates and other key election stakeholders on addressing disinformation;
- Allow online platforms to implement policies and processes such as content removal, advisory warnings, and delisting to address disinformation.
- Enable signatories to cooperate with the IEC and Media Monitoring Africa's initiatives including Real 411 and the Political Party Advert Repository (PADRE).

3. 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 war or advocacy of hatred that constitutes incitement.[49] 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, can be effective remedies.[50]

4. CONCLUSION

The advent of the internet and the proliferation of 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 fact-checking and the publication of counter-narratives, remain the preferred vanguard in the fight for the truth while maintaining protections for freedom of expression.

[48] Electoral Commission of South Africa 'Electoral Commission partners with social media giants to combat disinformation in 2024 National and Provincial Elections' (accessible here).
[49] Article 20 of the ICCPR, read with article 4(a) of CERD.
[50] See, for example, the UK Government Communications Services, 'RESIST: Counter-disinformation toolkit' (accessible here).

Module 9

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

ISBN 978-0-9935214-1-6
Published by Media Legal Defence Initiative: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in April 2024

TABLE OF CONTENTS

MODULE 9
NATIONAL SECURITY

- **"National security" is a common justification offered by states for limiting freedom of expression. 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 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.**

1. INTRODUCTION[1]

"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)[2] and the African Charter on Human and Peoples' Rights (ACHPR),[3] 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."[4]

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.

[1] This module should be read in conjunction with Richard Carver 'Training Manual on International and Comparative Media and Freedom of Expression Law at p 76-86 (accessible here)
[2] International Covenant on Civil and Political Rights (1966) at articles 19, 21 and 22 (accessible here).
[3] African Charter on Human and Peoples' Rights (ACHPR), at articles 3, 11, 12, 27 (1981) (accessible here).
[4] *Id.*

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

2. THE DEROGATION PROCESS UNDER INTERNATIONAL AND REGIONAL HUMAN RIGHTS TREATIES

Most 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."[5]

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 right 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. General Comment No. 29, can be taken as an authoritative interpretation of derogation during states of emergency. There are several 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 be 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.[6]
- The situation leading to derogation must be "a public emergency which threatens the life of the nation."[7] 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 derogations that have taken place in situations that appear to fall short of the article 4 requirements.[8]
- The UNHRCtte emphasises the importance of the principle that derogations should be limited "to the extent strictly required by the exigencies of the situation."[9] 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.

---

[5] ICCPR above n 2 at article 4.
[6] United Nations Human Rights Council, 'General Comment No. 29, states of emergency (article 4)' at para 2 (2001) (accessible here).
[7] *Id*.
[8] *Id* at para. 3.
[9] *Id* at para. 4.

The ACHPR, on the other hand, does not contain a clause explicitly permitting derogation during a public emergency. However, many states that are party to the ACHPR have adopted constitutional or legislative measures that do contain derogation clauses, contrary to the position of the ACHPR and the African Commission.[10] 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."[11]

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,[12] while others claim its omission has enabled the positive development of human rights norms in Africa.[13]

The 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa adopted by the African Commission on Human and Peoples' Rights (ACHPR) provides that national security is one of two legitimate objectives for limiting access to information or freedom of expression.[14] However, it further provides in Principle 22 that "freedom of expression shall 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."

This provides a cogent summary of the position in international law of the appropriate line between protecting national security and defending the right to freedom of expression. It is also in line with UN General Comment No. 34 on how States should give effect to article 19(3), which provides that when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself and must comply with the general principles of derogations from the right – that is, be provided in law, be necessary, and be proportional.[15] It also emphasises that extreme care must be taken to ensure that provisions relating to national security do not "suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information."[16] Restrictions must also not be overbroad and must demonstrate in a specific and individualised fashion the precise nature of the threat, and the

[10] Abdi Jibril Ali, 'Derogation from Constitutional Rights and Its Implication Under the African Charter on Human and Peoples' Rights' *Law, Democracy & Development* (2013) (accessible here).
[11] Kenya Court of Appeal, Petition 628 of 2014 (2015) (accessible here).
[12] Melkamu Aboma Tolera, 'Absence of a derogation clause under the African Charter and the position of the African Commission' (2013) (accessible here).
[13] Jibril Ali above at n 10.
[14] Principle 9(3)(b).
[15] UNHRC, 'General Comment No. 34. Article 19: Freedoms of opinion and expression', CCPR/C/GC/34 (2011) (accessible here).
[16] Para 30.

necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.

3. 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 the 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.

Defamation and threatening national security

Agnes Uwimana-Nkusi v. Rwanda concerned the conviction of **Rwandan** journalists Agnes Uwimana-Nkusi and Saidati Mukakibibi on the grounds of defamation and threatening national security following the publication of three articles criticising the government.[17] The journalist published articles detailing allegations of corruption among high-profile public officers, the human rights situation in Rwanda, and other government shortcomings. The government argued that the articles intended to incite violence and strife against the government by using defamatory statements devoid of evidence. Having exhausted all available domestic remedies, Media Dence (Media Legal Defence Initiative as it was then), filed a complaint to the Commission on behalf of the journalists arguing Rwanda violated their rights to freedom of expression and to a fair trial.

The Commission considered whether discussing the 1994 Rwanda Genocide amounted to genocide denial. Considering Rwanda's history, it assessed if implementing penal code articles was necessary and proportionate. The Commission emphasised democratic governance contexts in evaluating public order protection and incitement definitions. While acknowledging the sensitivity around the genocide, it found the journalists' articles did not incite violence or threaten security. The Commission criticised criminal defamation laws, deeming them disproportionate restrictions on journalism. It stressed the vital role of freedom of expression in democracy, particularly in fostering political discourse and holding officials accountable. Consequently, the Commission ruled Rwanda's actions violated Article 9 of the Charter by unjustly restricting the journalists' freedom of expression.

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. **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.[18]

[17] *Agnes Uwimana-Nkusi v. Rwanda* (2021) (accessible here). See also Global Freedom of Expression at Columbia University, 'Case update: Agnes Uwimana-Nkusi v. Rwanda (accessible here).
[18] Freedom House, 'Kenya's Antiterrorism Strategy Should Prioritize Human Rights, Rule of Law' (2018) (accessible here).

Recently, a flurry of laws passed by African states attempting to regulate the rising risk of cybercrimes and to tackle the proliferation of misinformation online have also referenced the need to protect national security as justification for often repressive and broad provisions. For example, **Zimbabwe's** Cybersecurity and Data Protection Act, of 2021, exempts entities from provisions aimed at protecting the processing of personal information for national security purposes.[19] **Nigeria's** Cybercrimes Act of 2015 provides harsh penalties for anyone who accesses computer systems or data that are vital to national security.[20]

The Johannesburg Principles

In 1995, a group of international experts drew up the Johannesburg Principles on Freedom of Expression and National Security.[21] 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.'[22] The Tshwane Principles state that:[23]

- 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

[19] Article 11(5)(d) (accessible here).
[20] Article 6 (accessible here)
[21] 'The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information,' (1996) (accessible here).
[22]Open Society Justice Initiative, 'Understanding the Global Principles on National Security and the Right to Information' (2013) (accessible here).
[23] Open Society Justice Initiative, 'The Tshwane Principles on National Security and the Right to Information: An Overview in 15 Points' (accessible here).

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.[24]

4. 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 scarcely be 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 reforms that arguably make for improved national security.[25]

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."[26] 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:

> "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."[27]

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."[28]

5. TERRORISM

[24] Open Society Justice Initiative above n 18.
[25] Katie Trippe, 'Pandemic policing: South Africa's most vulnerable face a sharp increase in police-related brutality' *Atlantic Council* (2020) (accessible here).
[26] 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 here).
[27] 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 here).
[28] Johannesburg Principles above n 17 at Principle 2(a).

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 as 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.”[29]

5.1. Defining terrorism

One serious problem with legal restrictions on the 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,[30] 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 a definition of terrorism, based upon best practices worldwide, which focuses on the act of terror rather than the perpetrator:[31]

> “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:

[29] UN Security Council, Resolution 1624 of 2005, (2005) (accessible here).
[30] International Convention for the Suppression of Financing of Terrorism, article 2(1) (1999)
[31] 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 here).

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."

The issue has been relevant in South Africa which, in 2022, tabled the draft Protection of Constitutional Democracy against Terrorist and Related Activities Amendment Bill, which has been criticised for its broad definitions of terrorism.[32]

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.

5.2. 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.[33] 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.[34]

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.

Two judgments by the Economic Community of West African States (ECOWAS) Community Court of Justice have taken a strong stand against the abuse of national security justifications for limiting freedom of expression. In addition to the June 2020 ruling addressing the internet shutdowns implemented by the Togolese government in 2017, discussed below,[35] in a similar case in 2022, the Court held that the government of Nigeria's banning of social media platform Twitter, on the grounds of preventing secessionist violence, was also illegal.[36]

6. 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.

[32] Terrance Booysen, 'This article – and good governance – could soon become outlawed,' MoneyWeb (2022) (accessible here).
[33] UNHRC, 'General Comment no. 34 at para 46 (2011) (accessible here).
[34] UNHRC, '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 here).
[35] ECOWAS Community Court of Justice, Suit No. ECW/CCJ/APP/61/18 (2020) (accessible here).
[36] *SERAP v. Federal Republic of Nigeria* (2022) (accessible here).

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."[37]

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."[38]

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.

7. NECESSARY IN A DEMOCRATIC SOCIETY

Most cases involving national security restrictions tend to be decided based on necessity. One area where restrictions may fall is if they are overbroad. This was the issue 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**.[39] 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.[40]

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 **Nigerian** presidential elections, including journalists, were arrested and publications were seized and banned.[41] 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

[37] Supreme Court of Zimbabwe, Civil Application No. 156/99 (2000) (accessible here).
[38] *Id*.
[39] United Nations Human Rights Commission, Communication No. 458/1991 (1994) (accessible here).
[40] *Id* at para 9.7.
[41] African Commission on Human and Peoples' Rights, Communication No. 102/93 (1998) (accessible here).

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."[42]

8. 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."[43] 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 in *Amnesty International Togo and Others v The Togolese Republic* 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 applicant's right to freedom of expression.[44]

This was also the question that the United States Supreme Court confronted in *New York Times Co. v United States*[45] — better known as the "Pentagon Papers" case. The government sought prior restraint on the publication of a large stash of documents — 47 volumes of them — labelled "top secret" and leaked from the Department of Defense.

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:

---

[42] High Court of Kenya, Petition no.628 of 2014 (2015) (accessible here).
[43] Johannesburg Principles, above at n 17.
[44] Economic Community of West African States Community Court of Justice, Suit no. ECW/CCJ/APP/61/18 (2020) (accessible here).
[45] United States Supreme Court, Case 403 US 713 (1971) (accessible here).

> "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."[46]

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 ... ."[47]

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.

9. 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 the 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.

[46] *Id.*
[47] *Id*.

Module 10

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

ISBN 978-0-9935214-1-6
Published by Media Legal Defence Initiative: www.mediadefence.org
This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in November 2022
Revised in April 2024

TABLE OF CONTENTS

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 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.**

1. 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 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.[1] 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:

[1] Digital Freedom Fund, Strategic Litigation Toolkit' (2022) (accessible here).

- Advanced 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.

2. FOUNDING JURISDICTION AND STANDING

2.1. 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 to 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 a major multinational technology platform or telecommunications company 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*[2] 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.[3]

2.2. Establishing standing

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 involves 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.

[2] Business & Human Rights Resource Center, 'Shell lawsuit (re oil pollution in Nigeria)' (2010) (accessible here).
[3] The Guardian 'Shell must face Friends of the Earth Nigeria claim in Netherlands' (2009) (accessible here).

3. GENERAL PRINCIPLES AND INTRODUCTION TO DIGITAL RIGHTS LITIGATION

3.1 What are digital rights?

It is now firmly entrenched by both the ACHPR[4] and the United Nations[5] (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.

The impact of strategic litigation in SSA

Strategic or impact litigation has played an important role in advancing freedom of expression in sub-Saharan Africa for many years. Some of the most foundational cases relating to journalists operating in both the offline and online realm include:

- *Konaté v Burkina Faso* (2013): the African Court on Human and Peoples' Rights held that criminal defamation laws that imposed sanctions of imprisonment were incompatible with Article 9 of the African Charter on Human and Peoples' Rights and other international human rights provisions.

- *Media Council of Tanzania v Attorney-General of the United Republic of Tanzania* (2019): the EACJ held that certain provisions of Tanzania's Media Services Act relating to fake news and rumours violated the right to freedom of expression by their broad and vague wording.

[4] ACHPR, 'Resolution on the right to freedom of information and expression on the internet in Africa', ACHPR/Res.362(LIX), (2016) (accessible here).
[5] 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 here).

- *SERAP v Federal Republic of Nigeria* (2022): the ECOWAS Court held that the government's suspension of Twitter in the country in 2021 violated the rights to freedom of expression, access to information and the media.

- *Amnesty International Togo v the Togolese Republic* (2020): The ECOWAS Court held that the Togolese government violated the right to freedom of expression by shutting down the internet during protests in September 2017.

- *Isaac Olamikan & Anor v. Federal Republic of Nigeria* (2023). The journalists faced deregistration due to their online journalistic activities. . The Court agreed, finding flaws in provisions regarding journalist registration and editor appointment qualifications by the Nigerian Press Council, failing to recognize the public interest served by online and citizen journalists. Emphasizing the evolving media landscape, the Court highlighted the influential role of influencers and content creators in shaping public opinion, noting that social media offers an unrestricted platform for information dissemination and expression.

3.2. 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.

3.2.1. 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 in regional fora usually requires that all domestic 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.

3.2.2. 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.

3.2.3. 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 affect 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.

4. OVERVIEW OF REGIONAL AND CONTINENTAL COURTS

4.1. 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.

4.1.1. Standing

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.[6]

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.[7] 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.

[6] For more on standing see Pedersen, 'Standing and the African Commission on Human and Peoples' Rights' African Human Rights Law Journal (2006) (accessible here) and Mayer, 'NGO Standing and Influence in Regional Human Rights Courts and Commissions' Notre Dame Law School (2011) (accessible here).
[7] For more on *actio popularis*, see *Article 19 v Eritrea* at the ACtHPR (2007) (accessible here).

4.1.2. Admissibility

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.[8]

4.1.3. Parties' submissions and the ACHPR's decision

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 Assembly of Heads of State and Government. The Secretariat of the 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.

Challenges at the Commission

Human Rights Watch shared various reflections on the work of the Commission, commemorating its 35th anniversary:

- "The Commission's establishment 35 years ago is an important reminder that political independence and the liberation of Africa are best achieved when underpinned by human rights and democratic governance".
- "Despite serious challenges, the Commission has stood its ground and sided with countless victims of rights violations by using resolutions and rulings against abusive governments and introducing complaints before the African Court".
- "The Commission is probably the most important institution that Africans created to realize the objectives and foundational values of the AU."

4.2. Litigating at the African Court on Human and Peoples' Rights

The African Court has the 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.[9] It complements and reinforces the functions of the

[8] For more on the criteria for exhausting local remedies, see *Sir Dawda K. Jawara v The Gambia* (2000) (accessible here) and *SERAC v Nigeria* (2002) (accessible here).
[9] 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 here).

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 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."[10]

4.2.1. Standing

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 recent years, The Gambia, Niger and Guinea-Bissau have made the declarations necessary to allow NGOs and individuals to access the African Court directly.[11] However, since 2016, four states have withdrawn their declarations (Tanzania, Rwanda, Cote d'Ivoire, and Benin), leaving only seven states who allow it.[12]

4.2.2. Legal representation

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 sections 42-47 of the Practice Directions of the African Court.

4.2.3. Jurisdiction and composition of the 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.[13]

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.

---

[10] African Court on Human and People's Rights, 'Frequently Asked Questions' (accessible here).
[11] African Court on Human and Peoples' Rights 'Declarations,' (accessible here).
[12] Id.
[13] For more on jurisdiction, see *Konaté v. Burkina Faso* in the African Court (accessible here).

4.2.4. Remedies

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.[14]

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 the African Court Protocol. However, persistent non-compliance by states with the Court's orders has become a serious issue, with research finding that 75% of states do not comply with its decisions.[15]

Commentary on the African Court

Amnesty International echoed these concerns noting that limits on individual and NGO access is a major challenge, and that implementation is equally challenging.[16] Of further concern Amnesty noted that—

> "Some States unfortunately went as far as withdrawing their 34(6) declarations in reaction to Court's decisions that displeased them. Rwanda withdrew its 34(6) declaration in 2016, Tanzania in 2019, and Benin and Cote d'Ivoire in 2020. These attacks to the Court itself were real steps backwards for the protection of human rights on the continent and for the concerned people who were deprived of a justice avenue that they had already been granted. Hopefully the future trend will on the contrary show more and more States valuing the building of a strong African human rights system."

The Court itself has also noted some challenges. In her 2023 speech Lady justice Aboud, President Court noted that while the Court has delivered several landmark judgments on a wide range of issues, "a quick look at the African legal and legislative landscape reveals that most African countries still adopt, maintain and implement laws contrary to the spirit and letter of the judgments already delivered by the Court."[17] That she, she went further to share positive examples of the Courts reach:

> "The Court is pleased to note that the impact of its case law has found some form of expression in the recent adjudication in some domestic fora. For example, the High Court of Lesotho and the High Court of Kenya have referred to the case of Konaté v Burkina Faso in dealing with freedom of expression. As none of these two countries was a party to

[14] For more on the African Court's deliberations on reparations, see the judgment from *Norbert Zongo and Others v Burkina Faso* (2015) (accessible here).
[15] Lilian Chenwi, 'Successes of African Human Rights Court undermined by resistance from states,' The Conversation (2021) (accessible here).
[16] Amnesty International, 'Why the African Court should matter to you' (2023) (accessible here).
[17] Speech By Hon. Lady Justice Aboud, President of the African Court on Human and Peoples' Rights on the Occasion of the opening of the 2023 Judicial Year Of The African Court (2023) (accessible here).

the freedom of expression cases adjudicated by the Court, the practice portrays a trend to preventive and pre-emptive implementation, that is, to avoid being condemned by the Court in a potential similar case."

4.3. 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.[18] The East African Court of Justice Rules of Procedure (EACJ Rules) govern its functioning. The EACJ serves the East African Community (EAC), namely Burundi; the Democratic Republic of the Congo; Kenya; Rwanda; South Sudan; the 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 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.[19]

4.3.1 Standing and jurisdiction

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.[20] In terms of rule 36 of the EACJ Rules, *amici curiae* are allowed to apply to be involved in a matter.

4.3.2. Admissibility

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, an unusually short period.[21] There is also no provision in the EAC Treaty that recognises the concept of continuing violations. However, there is no requirement that all domestic remedies must be exhausted first before approaching the EACJ.[22]

---

[18] For more see International Justice Resource Center 'East African Court of Justice' (accessible here).
[19] See the EACJ User Guide for more information (accessible here).
[20] 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 here).
[21] 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 here).
[22] 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

4.3.3. Legal representation and procedure

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 other things, 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.

4.4. 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 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.

4.4.1. Standing

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.[23] 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.

---

an applicant can show an alleged violation of the EAC Treaty, the EACJ must exercise jurisdiction (accessible here).

[23] See *Ocean King v Senegal* for more on how strictly adherence to the standing provision is applied by the ECOWAS Court (accessible here).

4.4.2. Amicus curiae

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*,[24] 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. It seems that this has opened the door to *amici* applications at the Court going forward, and *amici* have been successfully admitted in later cases including *Amnesty International Togo v The Togolese Republic* and *SERAP v Federal Republic of Nigeria*.

4.4.3. Admissibility

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.

4.4.4. Remedies

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 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.[25]

The ECOWAS Court has recently demonstrated its willingness to progressively address digital rights issues placed before it. In two prominent cases, it recently ruled against states who had shut down access to the internet and/or social media in violation of the right to freedom of expression. In June 2020, the Court 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.[26] In a similar case in 2022, the Court held that the government of Nigeria's banning of social media platform Twitter was also illegal.[27]

For more information, see Media Defence's Training Manual on Litigation of Freedom of Expression in West Africa.

[24] ECOWAS Court Suit No. ECW/CCJ/APP/36/15 (2018) (accessible here).
[25] For more, see Olisa Agbakoba Legal 'Enforcement of the Judgments of the ECOWAS Court' (2018) (accessible here).
[26] Economic Community of West African States Community Court of Justice, Suit no. ECW/CCJ/APP/61/18 (2020) (accessible here).
[27] SERAP v. Federal Republic of Nigeria (2022) (accessible here).

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 providing 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.[28] 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.[29]
3. **Advocacy strategies**. Litigation alone is not enough to effect substantive change or effectively disrupt the status quo — advocacy is an essential component.[30] 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.

For more information on the practicalities of litigating digital rights, see the recently published *Strategic Litigation Toolkit* by the Digital Freedom Fund.

5. 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.

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.

[28] Human Rights Center UC Berkley School of Law 'Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court' (2014) (accessible here).
[29] For more see UNODC E4J University Module Series: Cybercrime, 'Module 4: Introduction to Digital Forensics' (2019) (accessible here).
[30] See APC, 'Advocacy Strategies and Approaches' (accessible here); Call Hub, 'Advocacy Strategies' (accessible here) and Call Hub, 'Grassroots Advocacy' (accessible here).