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).