Module 2

Restricting Access and Content

Advanced Modules on 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/

November 2022

Table of Contents

MODULE 2

Restricting Access and Content

The objectives of this module are:

- **To provide an overview of the current mechanisms through which access to the internet and access to content is restricted.**
- **To outline the fundamental international and regional legal principles relating to access.**
- **To unpack the different rights affected by such restrictions.**
- **To set out the limitations of implicated rights and explore the justifiability of the measures adopted by states.**
- **To identify practical ways to deal with restrictions.**

Introduction

The internet was created to facilitate the free flow of information;[1] it now allows people to instantaneously access information and services, to communicate, and to share knowledge and ideas. The internet offers an array of opportunities for the realisation of human rights and has, in many instances, been a catalyst for the empowerment of marginalised members of society. It is common cause that the internet is an enabling space for the advancement of the right to freedom of expression, the right of access to information, the right of freedom of assembly, the right to freedom of opinion, thought and belief, the right to be free from discrimination in all forms, the right to education, the right to culture and language, and the right of access to socio-economic services.

Access to the internet is a crucial component of social, economic and human development, particularly in the African context. The Declaration of Principles of Freedom of Expression and Access to Information in Africa, adopted by the African Commission on Human and Peoples' Rights (**ACHPR**) in 2019, calls for states to facilitate the rights to freedom of expression and access to information online and to provide the means to exercise these rights. It further highlights that universal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression, access to information and the exercise of other human rights.

However, a range of restrictions to internet access are eroding the right to freedom of expression and associated rights.[2] Suppressive tactics by governments and private actors

[1] Internet Society, 'Brief History of the Internet' (1997) (accessible at: https://www.internetsociety.org/internet/history-internet/brief-history-internet/).
[2] See Tim Berners-Lee, 'I Invented the web. Here are three things we need to change to save it' (2017) (accessible at: https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet).

cause significant challenges in accessing information online. As will become apparent, the unjustifiable restriction of access to the internet is a violation of human rights. This module outlines some of the prevalent harms to access and provides guidance on how to secure fundamental rights and freedoms in the digital age. In doing so, this module focuses on internet shutdowns, the ways in which access to content may be unjustifiably limited through blocking and filtering, the implications of social media taxes, and the harms of distributed denial of service (**DDoS**) attacks.

Internet Shutdowns

Overview of internet shutdowns

An internet shutdown typically involves the deliberate disruption of internet or electronic communications, to the extent that they become inaccessible or unusable. Internet shutdowns generally target a particular population or within a specific location with the objective of exerting control over the free flow of information. Internet shutdowns, which are sometimes referred to as a "blackout" or "kill switch", include full and localised shutdowns, bandwidth throttling, and service-based blocking of two-way communication platforms.[3]

Internet shutdowns on the rise

Internet shutdowns are unfortunately on the rise*:* in 2021 the #KeepItOn coalition reported at least 182 incidents of internet shutdowns around the world compared to 76 in 2016.[4] These figures highlight the rise of this new trend in which governments seek to silence dissenting voices, control information and curb freedom of expression. Of additional concern is the protracted duration of the shutdowns. At the time of this module's latest update, there was an ongoing shutdown in the Tigray region of Ethiopia approaching nearly two years; a shutdown in Pakistan's Federally Administered Tribal Area lasted nearly four years between 2016 and 2021, seriously compromising the education, healthcare, and business sectors.[5]

Internet shutdowns are used by states to limit opposition and disarm dissent and are often used during critical periods such as elections or times of mass protest. They pose severe threats to people's rights and are contrary to international human rights standards.

[3] See Access Now, 'What is an internet shutdown?' (2019) (accessible at: https://www.accessnow.org/keepiton/?ignorelocale) and Media Defence, 'Training Manual on Digital Rights and Freedom of Expression Online'. See further Access Now, 'Launching STOP: the #KeepItOn internet shutdown tracker' (2017) (accessible at https://www.accessnow.org/keepiton-shutdown-tracker/) and Indian Council for Research on International Economic Relations, 'The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India' (2018) (accessible at https://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf).

[4] #KeepItOn, '#KeepItOn STOP Data 2016-2021,' (accessible at: https://docs.google.com/spreadsheets/d/1DvPAuHNLp5BXGb0nnZDGNoiIwEeu2ogdXEIDvT4Hyfk/edit#gid=1399965468).

[5] Access Now, 'Internet shutdowns in 2021: the return of digital authoritarianism,' (2022) (accessible at: https://www.accessnow.org/internet-shutdowns-2021/).

International and regional responses

Over the last decade, the exponential growth in access to the internet has led to the corresponding development of international norms and standards regarding the use of the internet and the various rights it invokes. In the context of internet shutdowns, the rights to freedom of expression, access to information, and association and assembly rights contained in articles 19 and 21 of the International Covenant on Civil and Political Rights (**ICCPR**) are primarily implicated.

In a 2011 Report, the United Nations Special Rapporteur on Freedom of Expression (**UNSR FreeEx**) reported to the United Nations General Assembly that—

> "the Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression, as guaranteed by article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."

In 2012, the UN Human Rights Council (**UNHRC**) unanimously adopted a Resolution to protect the free speech of individuals on the internet. This resolution was the first of its kind and notably called upon states to "promote and facilitate access to the Internet". It affirmed that—

> "the 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".

In recent years there have been more explicit statements concerning internet shutdowns:

- In 2016, the UNHRC expressed deep concern regarding "measures aiming to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law."
- In 2017, the UNSR reported that: "Internet and telecommunications shutdowns involve measures to intentionally prevent or disrupt access to or dissemination of information online in violation of human rights law". The report explains further that shutdowns "ordered covertly or without an obvious legal basis violate the requirement of Article 19(3) of the [ICCPR] that restrictions be 'provided by law'".
- In 2018, the UNHRC expressed its deep concern "at measures in violation of international human rights law that aim to or that intentionally prevent or disrupt access to or dissemination of information online."
- In 2019, the UNHRC noted its deep concern with "the various forms of undue restriction of freedom of opinion and expression online, including where States have manipulated or suppressed online expression in violation of international law".
- In 2019, the UNSR reiterated that internet shutdowns are clearly inconsistent with article 19(3) of the ICCPR.
- In 2020, the UNHRC strongly condemned the use of internet shutdowns "to intentionally and arbitrarily prevent or disrupt access to or dissemination of information online."

- In June 2022, the UN High Commissioner for Human Rights presented a report to the UN General Assembly highlighting the severe human rights impacts of internet shutdowns, including the fact that they "very rarely meet the fundamental requirements of necessity and proportionality", and providing a set of recommendations for ending shutdowns, including calling on states to refrain from the full range of internet shutdowns.

In an African context, the 2019 Declaration of Principles on Freedom of Expression in Africa provides that:

> "States shall not interfere with the right of individuals to seek, receive and impart information through any means of communication and digital technologies, 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.
>
> States shall not engage in or condone any disruption of access to the internet and other digital technologies for segments of the public or an entire population."

The above standards make it clear that internet shutdowns result in rights violations, and these reports and resolutions are important for establishing the rights-based framework relating to internet shutdowns. The practicality of litigating against states requires a nuanced understanding of the international human rights standards of **legality**, **necessity**, and **proportionality** and when there can be reasonable and justifiable limitations on fundamental human rights, particularly the right to freedom of expression. This is addressed below.

Legality, necessity and proportionality

Central to litigating internet shutdowns is establishing that the measure violates the right to freedom of expression and access to information, among others, such as the right to health and education. As discussed above, internet shutdowns violate the full enjoyment of the right to freedom of expression. However, establishing this is not enough. The right to freedom of expression can only be limited when the limitation is provided by "law" and where "necessary" to ensure "respect of the rights or reputation of others" or for "the protection of national security or of public order (*ordre public*), or of public health or morals".[6]

States often rely on "national security" or "public order" to justify internet shutdowns. When litigating the issue of internet shutdowns, it is important to conduct a thorough limitations analysis in order to illustrate to a court that a right has been infringed, and that the limitation does not meet the threshold of Article 19(3) of the ICCPR.

[6] Article 19 of the International Covenant on Civil and Political Rights (accessible at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights).

Note on the limitation of freedom of expression

Article 19(3) of the ICCPR sets out the grounds upon which the right to seek, receive and impart information and ideas on the internet may be limited. The restriction must be:

1. **Provided by law.**
2. **Be necessary for**:
   - Respect for the rights of others.
   - The protection of national security or of public order (*ordre public*), or of public health or morals.
     - ➔ These are understood as the "legitimate grounds for restrictions".

The UNHRC, through General Comment 34, has given further scope to the understanding of Article 19(3):

The restrictions must be **provided by law**:[7]

- The law must be clear (be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly) and accessible, and apply equally to everyone.
- The law must also be consistent with international human rights law.
- It must provide sufficient guidance on remedies and procedures for challenging non-compliance with the law.
- It is for the state to demonstrate the legal basis for any restrictions imposed on freedom of expression.

Directions or instructions from state departments or actors are insufficient to meet this legality threshold.

The restriction must be **necessary**:

- It must respect the rights or reputations of others. The UNHRC explains that for example, it may be legitimate to restrict freedom of expression in order to protect the right to vote. The UNHRC cautions that restrictions must be constructed with care: while it may be permissible to protect voters from forms of expression that constitute intimidation or coercion, such restrictions must not impede political debate, including, for example, calls for the boycotting of a non-compulsory vote.
- It must be aimed at the protection of national security or of public order (*ordre public*), or of public health or morals. Here the UNHRC explains that restrictive laws used for the pursuit of national security cannot be used to suppress or withhold from the public information of legitimate public interest if it does not harm national security.

[7] The UNSR 2019 Report explains that "The restriction must be provided by laws that are precise, public and transparent; it must avoid providing authorities with unbounded discretion, and appropriate notice must be given to those whose speech is being regulated. Rules should be subject to public comment and regular legislative or administrative processes. Procedural safeguards, especially those guaranteed by independent courts or tribunals, should protect rights."

Journalists, researchers, environmental activists, human rights defenders, or others cannot be prosecuted for having disseminated such information if it does not harm national security. Relying on the justification of national security to stifle advocacy and activism is prohibited and merely alleging the justification of national security is insufficient.

The UNHRC explains further that the above grounds must conform to the strict tests of **necessity** and **proportionality:**[8]

- Restrictions must be "necessary" for a legitimate purpose.
- Restrictions must not be overbroad. The UNHRC emphasised that restrictive measures must conform to the principle of proportionality:
  - They must be appropriate to achieve their protective function.
  - They must be the least intrusive instrument amongst those which might achieve their protective function.
  - They must be proportionate to the interest to be protected.
  - The principle of proportionality must be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law.

Internet shutdowns are seldom proportionate, and are generally viewed as a "disproportionate restriction on the right to freedom of expression, and have serious repercussions for the protection of other human rights."

If a state cannot fulfil these requirements, then the restriction amounts to an unjustifiable and disproportionate limitation of the right. Echoing this and responding to the internet shutdown crisis in Kashmir in 2019, UN Special Rapporteurs have stated that "[t]he shutdown of the internet and telecommunication networks, without justification from the Government, are inconsistent with the fundamental norms of necessity and proportionality."

Recent examples of litigation relating to internet shutdowns

Despite these clear standards, states continue to claim that measures taken to restrict the internet are necessary and proportionate to ensure national security or public order, or both. Fortunately, there have been instances where courts have handed down decisions providing that these justifications do not warrant internet shutdowns and where the threat of litigation itself has proved successful.

Domestic Courts

Cameroon

[8] "Fundamentally, any restriction or limitation must not undermine or jeopardise the right to freedom of expression itself. Additionally, restrictions must be consistent with other rights found in the ICCPR and the fundamental principles found in the UDHR."

In 2017, a case was brought before the Constitutional Council in Cameroon which challenged the state's decision state to shut down the internet in the South West and North West of the country – the English-speaking regions – following language-related protests. Civil society actors filed a challenge demanding that the state restore access to the internet in these regions. After the filing of the challenge, access to the internet was restored without the need for a judicial determination.[9]

In 2018, Media Defence and Veritas Law filed a new challenge which sought to emphasise that the state's actions in shutting down the internet were an infringement on the right to freedom of expression and a violation of international and regional human rights law.[10] The internet was ultimately restored, illustrating, as stated by Access Now that "simply filing the lawsuit can get results, like increased transparency and responsiveness from telcos or the state."

Zimbabwe

In January 2019, an urgent chamber application was filed by Zimbabwe Lawyers for Human Rights (**ZLHR**) and the Media Institute of Southern Africa-Zimbabwe Chapter (**MISA-Zimbabwe**) challenging the ongoing internet shutdowns in Zimbabwe at that time. The High Court granted an interim order that the implicated mobile operator must immediately and unconditionally resume full services and thus ensure access to the internet. The Court's ruling was mainly based on the absence of a legal provision enabling the shutdown.

Comments from the litigants

MISA-Zimbabwe stated:

> "It is now important that civil society, as MISA did, lobby parliament and the executive on digital rights, by pointing out how archaic Internet shutdowns are in trying to stop sharing information and that shutdowns do more harm to the country's reputation than good."

Papua and West Papua

In 2020, the Jakarta State Administrative Court (PTUN) ruled on an internet shutdown ordered by the Indonesian government in the areas of Papua and West Papua in 2019 in response to

[9] Media Defence along with Veritas Law were the applicants challenging the internet shutdown. Media Defence stated: "The case that has been brought highlights that open and accessible internet communications are essential to ensuring the right to freedom of expression. Disruption of online services, whether through website blocking or internet shutdowns, amounts to a serious violation of that fundamental right. The government of Cameroon is obliged under domestic and international legal obligations to protect freedom of expression, including ensuring that it remains accessible and that people are able to use it freely and without interference."

[10] CIPESA, 'Litigating Against Internet Shutdowns in Cameroon' (2018) (accessible at https://cipesa.org/2018/03/litigating-against-internet-shutdowns-in-cameroon/)

widespread protests in the region sparked by incidents of racial abuse and state violence.[11] The Indonesian government argued that the shutdown was necessary to prevent the spread of fake news during the protests. However, in the case filed by a group of Indonesian CSOs, the Court found that the shutdown violated the law and that the government had failed to prove that Indonesia was in a state of emergency that required authorities to shut down the internet. It further held that initiatives to address fake news should be dealt with under provisions in the Criminal Code or through the blocking of specific accounts, rather than shutting down internet access.[12][13]

Kashmir

A comprehensive case dealing with internet shutdowns is that of *Bhasin v Union of India; Azad v Union of India*. It stems from a 2019 disconnection of internet services in parts of Kashmir.

The petitioners approached the Supreme Court seeking, among other things:

- An order setting aside all orders, notifications, directions and/or circulars issued by the respondents under which any / all modes of communication including internet, mobile and fixed-line telecommunication services have been shut down or suspended or in any way made inaccessible or unavailable in any locality.
- An order directing the respondents to immediately restore all modes of communication including mobile, internet and landline services throughout Jammu and Kashmir in order to provide an enabling environment for the media to practise its profession.

The questions of law that arose for the Supreme Court to consider were:

- Whether the government could claim an exemption from producing all orders pertaining to the suspension of telecommunications services.
- Whether freedom of expression and freedom to practise any profession or to carry on any occupation, trade or business over the internet constituted part of the fundamental rights under the Constitution.
- Whether the government's action of prohibiting internet access was lawful and valid.
- Whether the imposition of the relevant restrictions by the government was valid.
- Whether the freedom of the press of the petitioners was violated due to the restrictions.

In its ruling, the Supreme Court made some profound statements regarding freedom of expression and the intersection between law and technology:

[11] Moch. Fiqih Prawira Adjie, 'Jokowi 'violates the law' for banning internet in Papua, court declares,' (2020) (accessible at: https://www.thejakartapost.com/news/2020/06/03/jokowi-violates-the-law-for-banning-internet-in-papua-court-declares.html).
[12] Id.
[13] Access Now, which intervened as a friend of the court in this matter, argued that "shutdowns not only interfere with the right to information and freedom of expression, but also the right to assembly, as well as the rights to work, health, education, scientific progress, and cultural rights in the internet age, and that shutdowns are incompatible with human rights law, especially during the COVID-19 pandemic." Access Now also highlighted the significance of the Court's finding that "any decision that limited people's right to information should be made in accordance with the law and not merely based on the government's discretion."

> "We need to distinguish between the internet as a tool and the freedom of expression through the internet. There is no dispute that freedom of speech and expression includes the right to disseminate information to as wide a section of the population as is possible. The wider range of circulation of information or its greater impact cannot restrict the content of the right, nor can it justify its denial."

In addition, the Supreme Court conducted a thorough limitations analysis, noting that:

> "It goes without saying that the Government is entitled to restrict the freedom of speech and expression guaranteed under Article 19(1)(a) if the need be so, in compliance with the requirements under Article 19(2). It is in this context, while the nation is facing such adversity, an abrasive statement with imminent threat may be restricted, if the same impinges upon the sovereignty and integrity of India. The question is one of extent rather than the existence of the power to restrict."

The Supreme Court found that freedom of speech and expression and the freedom to practice any profession or carry on any trade, business, or occupation over the medium of the internet enjoys constitutional protection and any restriction upon such fundamental rights should be in consonance with the restrictions provided for in the Constitution, inclusive of the test of proportionality.

Ultimately, the Court issued a list of directions including a declaration that suspending internet services indefinitely is impermissible, and can be for a temporary duration only; suspending the internet in terms of the "Suspension Rules" must adhere to the principle of proportionality and must not extend beyond the necessary duration; any order suspending or restricting access to the internet is subject to judicial review; and the state was directed to review all orders suspending internet services.

Commentary – did the judgment go far enough?

The Software Freedom Law Centre, India (SFLC.In) welcomed the judgment but noted some concerns:

1. The direction to review the suspension orders could be a futile exercise as the review committee is composed of members exclusively from the executive.
2. The judgment did not give any immediate relief to the people in Kashmir.

Former Chief Justice, Justice Shah of the Delhi High Court stated, during the Fourth LC Jain Memorial Lecture, that the judgment is laudable in many respects, but went on further to state:

> "After ruling that the suspension of communication services must adhere to the principles of necessity and proportionality, the Court failed to apply these principles to actually decide the legality of the communication shutdown in Kashmir.

> Instead, it directed the fresh publication of all orders, with the Review Committee reviewing all these orders. The reliance on Lord Diplock's aphorism "you must not use a steam hammer to crack a nut, if a nutcracker would do", was, at least for the people of Kashmir, meaningless."

Overall, this judgment has been widely welcomed. It provides a comprehensive discussion on the topic of internet shutdowns, and it is useful to future litigants who are faced with these issues. Although often facing the challenges of poorly capacitated court systems lacking independence, these and other cases – including in Sudan and Uganda – provide lessons on how to meaningfully effect change through litigation in domestic courts.

Regional courts

Togo

In 2017, the Togolese government enacted an internet shutdown in response to protests over President Faure Gnassingbé's efforts to pursue a fourth term in power.

- Seven local CSOs, including Amnesty International Togo, and an individual blogger activist applied to the Community Court of Justice of the Economic Community of West African States (ECOWAS) arguing a violation of Article 9 of the African Charter on Human and Peoples' Rights (African Charter) which protects freedom of expression, as well as that the shutdown prevented their ability to carry out their work and damaged their reputation and finances.[14]
- The government justified the shutdown in terms of national security, claiming that there was a spread of hate speech and incitement online which risked a civil war.

Judgment

As described by the Global Freedom of Expression Database at Columbia University:

> "The Court found that access to the internet is a "derivative right" as it "enhances the exercise of freedom of expression." As such, internet access is "a right that requires protection of the law" and any interference with it "must be provided for by the law specifying the grounds for such interference." [p. 11] As there was no national law upon which the right to internet access could be derogated from, the Court concluded that the internet was not shut down in accordance with the law and the Togolese government had violated Article 9 of the African Charter on Human and Peoples' Rights. The Court subsequently ordered the Respondent State of Togo to take

[14] Global Freedom of Expression: Columbia University, 'Amnesty International Togo and Ors v. The Togolese Republic,' (2020) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/amnesty-international-togo-and-ors-v-the-togolese-republic/).

measures to guarantee the "non-occurrence" of a future similar situation, implement laws to meet their obligations with the right to freedom of expression and compensate each applicant to the sum of 2,000,000 CFA (approx. 3,500 USD)."

The Court also established that non-natural persons, including CSOs, can bring claims to protect their right to freedom of expression in the ECOWAS Court.[15][16]

In conjunction with litigation considerations, there are some other practical tips which may be of use, particularly in relation to capturing and preserving evidence during internet shutdowns. These tips can be useful for establishing a rights violation and pursuing litigation.

Tips to consider when litigating this issue

The Southern African Litigation Centre has published a guide on litigating internet shutdowns in Southern Africa which highlights the legal considerations for legal action on internet shutdowns in various courts in the region.

- **The parties**: consider the impact of the shutdown and if it is necessary to identify specific categories of applicants and respondents. Identify who is responsible for ordering the shutdown and who implemented it.
- **The procedure and the relief**: consider if the case requires urgent litigation and interdicts, injunctions or judicial reviews. Consider the type of precedent the case will set.
- **The law**: consider whether there are existing laws that prescribe blockage orders. If there are, consider whether the government has complied with them and consider if the laws themselves are in accordance with human rights standards.
- **The rights**: consider which rights were violated and consider responses to government justifications.

[15] Id.

[16] Access Now, which intervened in the case as a friend of the court along with a group of other CSOs, stated: "The ECOWAS Togo decision is generally consistent with existing international law, such as Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and the UN Human Rights Committee (UNHRC)'s General Comment No. 34 on Article 19 ICCPR, which state that no internet restrictions are permissible unless they are provided by law. However, the court did not address the necessity and proportionality requirements outlined in General Comment No. 34, including that any restrictions on the freedom of expression, such as internet shutdowns, "must be the least intrusive instrument amongst those which might achieve their protective function." This is the key question that should be asked whenever a government is contemplating shutting down an entire internet network or service: would a less harmful step be effective? Nevertheless, the court did order the government of Togo to enact the law protecting freedom of expression that would be consistent with international human rights instruments in the future. This means that the Togolese government should enact legislation protecting its citizens' rights from any disproportionate restrictions on their expression."

Conclusion

The growing number of shutdowns internationally and in Africa is of grave concern. Fortunately, there is a simultaneous growth of activism and litigation that is working towards curbing these continued rights violations. Until states refrain from blanket bans over access to the internet through shutdowns, there will be a continued need for strategic litigation, activism, and advocacy.

Access to Content: Censorship, Blocking and Filtering

Overview of censoring, blocking and filtering of content

Access to information is a central tenet of the internet. However, efforts to restrict access have developed in step with improved infrastructure and technology that should enable access. Technical measures are being implemented in many jurisdictions by state and non-state actors to limit, influence, monitor, and control people's access to the internet. These measures include censoring, blocking, filtering, and monitoring content. While these measures may not be as extreme as complete internet shutdowns, they equally hinder the full enjoyment of the right to freedom of expression and have the potential to severely distort and disrupt people's access to information online.

Censorship and blocking	**Filtering**
Typically refers to the prevention of access to specific websites, domains, IP addresses, protocols or services included on a blacklist.[17] Justifications for blocking often include the need to prevent access to illegal content, or content that is a threat to public order or is objectionable for a particular audience.[18]	Generally, refers to restricting or limiting access to information (or related services) that is either illegal in a particular jurisdiction, is considered a threat to public order, or is objectionable for a particular audience. Filtering can relate to the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols, or keywords, or based on their perceived connection to content deemed inappropriate or unlawful.
Note: The distinction between these concepts may appear to be semantic, but there is arguably a difference in scale and perspective. However, the key commonality is that they both limit access to the internet.[19]	

ARTICLE 19 outlines several different ways in which access to content can be restricted:[20]

[17] ARTICLE 19, 'Freedom of Expression Unfiltered: How blocking and filtering affect free speech' (2016) at 7 (accessible at https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf).
[18] Internet Society, 'Internet Society Perspectives on Internet Content Blocking: An Overview' (2017) (accessible at https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/).
[19] Id. See further Barnes, 'Technical Considerations for Internet Service Blocking and Filtering' (2013) (accessible at https://tools.ietf.org/id/draft-iab-filtering-considerations-03.html).
[20] ARTICLE 19 above n 7 at 9.

- URL blocking, which blocks a specific web page.
- IP address blocking, which prevents connection to a host.
- Entire domain names can be blocked through DNS tampering.
- Blacklisting, which compiles a list of URLs to be filtered, while whitelisted URLs are not subject to blocking or filtering.
- Keyword blocking, which is generally used to enable the blocking of specific categories of content.

The rise of disinformation has also contributed to an increase in blocking and filtering with states trying to mitigate the spread of false information, and, in some instances, legally permitting blocking and filtering in order to prohibit and punish the dissemination of false or inaccurate statements.

Applicable international human rights standards

The same general considerations relating to access, online rights and freedom of expression discussed above are applicable here, save for specific considerations relating to filtering and blocking. In 2011, in a Joint Statement on Freedom of Expression and the Internet, a collective of Special Rapporteurs and experts stated the following in relation to filtering and blocking:

- Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – can only be justified in accordance with international standards, for example, where necessary to protect children against sexual abuse.
- 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.
- Products designed to facilitate end-user filtering should be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering.

In a 2016 Report, the UNSR on FreeEx explained that:

> "States often block and filter content with the assistance of the private sector. Internet service providers may block access to specific keywords, web pages or entire websites. On platforms that host content, the type of filtering technique depends on the nature of the platform and the content in question. Domain name registrars may refuse to register those that match a government blacklist; social media companies may remove postings or suspend accounts; search engines may take down search results that link to illegal content. The method of restriction required by Governments or employed by companies can raise both necessity and proportionality concerns, depending on the validity of the rationale cited for the removal and the risk of removal of legal or protected expression.

> Ambiguities in State regulation coupled with onerous intermediary liability obligations could result in excessive filtering. Even if content regulations were validly enacted and enforced, users may still experience unnecessary access restrictions. For example, content filtering in one jurisdiction may affect the digital expression of users in other jurisdictions. While companies may configure filters to apply only to a particular jurisdiction or region, there have been instances where they were nevertheless passed on to other networks or areas of the platform."

In a case in the European Court of Human Rights in which access to a lawful website was obstructed as a result of blocking measures applied to an illegal website, the Court stated that "when exceptional circumstances justify the blocking of illegal content, a State agency making the blocking order must ensure that the measure strictly targets the illegal content and has no arbitrary or excessive effects, irrespective of the manner of its implementation. Any indiscriminate blocking measure which interferes with lawful content or websites as a collateral effect of a measure aimed at illegal content or websites amounts to arbitrary interference with the rights of owners of such websites."[21]

Blocking and filtering in Ethiopia

Ethiopia has repeatedly made use of blocking and filtering mechanisms in the recent past. Between 2012 and 2018, hundreds of websites were blocked, including the websites of LGBTQI+ organisations, media outlets and CSOs like the Electronic Frontier Foundation.[22] In 2017, during a spate of anti-government protests, Facebook, Twitter, WhatsApp, and Dropbox were frequently blocked.

In 2018 Freedom House noted that with the change of regime, over 250 websites were unblocked. Despite this, politically motivated blocking and filtering has continued in Ethiopia (and the full internet shutdown in the Tigray region remains ongoing). As of 2021, Freedom House confirmed that there were still no procedures for determining which websites are blocked or for appealing blocking decisions.

[21] European Court of Human Rights, *Vladimir Kharitonov v. Russia* (application No. 10795/14), (2020), para. 46 (accessible at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-203177%22]}).
[22] Access Now, 'Ethiopia: Verifying the unblocking of websites,' (2018) (accessible at: https://www.accessnow.org/ethiopia-verifying-the-unblocking-of-websites/).

Blocking and filtering in Turkey

Turkey's government has recently received sustained criticism for the "systematic actions the Turkish government has taken to restrict Turkey's media environment, including closing media outlets, jailing media professionals, and blocking critical online content."[23] In 2018, Freedom House found that over 3300 URLs containing news items were blocked.

In 2019, the Wikimedia Foundation, which owns and operates Wikipedia, petitioned the European Court of Human Rights (**ECtHR**) in relation to the blocking of Wikipedia in Turkey. With the petition to the ECtHR still outstanding in January 2020, in response to a ruling from the Turkish Constitutional Court, the Turkish government restored access to Wikipedia. The Constitutional Court ultimately found that blocking Wikipedia was unconstitutional.

Blocking of Twitter in Nigeria

In a prominent recent example of content blocking, the federal government of Nigeria in 2021 suspended social media site Twitter after it removed content posted by President Muhammadu Buhari which threatened to punish regional secessionists. The ban was in place for seven months before Twitter agreed to a number of the government's demands, including opening a local office in Nigeria.

The ban was subsequently declared unlawful by the ECOWAS Community Court of Justice in a case brought by the Socio-Economic Rights and Accountability Project (SERAP) and joined with other similar cases. The Court held that the ban violated the right to freedom of expression, access to information and the media and ordered the government to prevent such a repetition. Media Defence and Mojirayo Ogunlana-Nkanga represented the applicants.

Blocking and filtering remain a contemporary concern. While in limited instances there may be justifiable limitations, generally such measures constitute an unjustifiable infringement and are often carried out with limited guidance to the public and limited to no regulation or oversight over the state.[24]

Unjustifiable limitations

[23] U.S. Mission to the United Nations 'Remarks at a UN Third Committee Dialogue with the Special Rapporteur on the Freedom of Expression' (2019) (accessible at https://usun.usmission.gov/remarks-at-a-un-third-committee-dialogue-with-the-special-rapporteur-on-the-freedom-of-expression/)

[24] UNICEF 'Children's Rights and Business in a Digital World: Freedom of Expression, Association, Access to Information and Participation (2017) at 11 (accessible at https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_EXPRESSION.pdf).

As discussed above, and as with all limitations of the right to freedom of expression, restrictions are only permissible if they are provided by **law**, pursuant to a legitimate aim and conform to the strict tests of **necessity** and **proportionality**. In terms of "blanket" or "generic" bans, the 2011 UNHRC General Comment found that "generic bans on the operation of certain sites and systems are not compatible" with article 19 of the ICCPR. Where restrictions constitute "generic" bans, they will generally amount to an infringement of the right to freedom of expression.

Justifiable limitations

There may be circumstances where measures such as blocking and filtering of content are justifiable. The protection of children's rights may be one such justification. Blocking and filtering techniques can be developed and utilised to prevent the proliferation of and exposure to damaging material and to protect children from harmful and illegal content. However, despite this important purpose, UNICEF's 2017 Report on 'Children's Rights and Business in a Digital World: Freedom of Expression, Association, Access to Information and Participation' has recognised the inherent concerns around blocking and filtering, including a lack of transparency; the unscrupulous nature of filters; the lack of evidence to show where and when they have been deployed; and the threat of legitimate content being limited.[25] The children's rights example illustrates that even when there might appear to be a legitimate purpose, rights can be unduly limited if the elements of legality, necessity and proportionality are not thoroughly and independently tested.

In digital rights litigation, practitioners will do well to test all tenets of the limitations analysis before determining the appropriateness or otherwise of an imposed restriction. The ECtHR, in its 2012 decision of *Ahmet Yıldırım v Turkey*, provides guidance on the limitations analysis in relation to blocking and filtering.

Case note: *Ahmet Yıldırım v Turkey*

The applicant owned and ran a website on which he published his academic work and his views on various topics. In 2009, the Denzili Criminal Court in Turkey ordered the blocking of the website as a preventative measure in the context of criminal proceedings against the site's owner, who was accused of insulting the memory of Atatürk. The Court subsequently ordered the blocking of all access to *Google Sites*, a website hosting platform, as this was the only means of blocking the offending website. The applicant unsuccessfully tried to have the blocking order removed and applied to the ECtHR submitting that the blocking of *Google Sites* amounted to indirect censorship.

The ECtHR held that the impugned measure amounted to a restriction stemming from a preventive order blocking access to a website. The ECtHR found that the impugned measure produced arbitrary effects and could not be said to have been aimed solely at

[25] Id at 12.

blocking access to the offending website, since it consisted in the wholesale blocking of all websites hosted by *Google Sites*.

The ECtHR reasoned that specific legal provisions are necessary, as general provisions and clauses governing civil and criminal responsibility do not constitute a valid basis for ordering internet blocking. Relying on General Comment 34, the Joint Declaration on Freedom of Expression and the Internet and the 2011 UNSR FreeEx Report, the ECtHR went further, stating:

> "In any case, blocking access to the Internet, or parts of the Internet, for whole populations or segments of the public can never be justified, including in the interests of justice, public order or national security. Thus, any indiscriminate blocking measure which interferes with lawful content, sites or platforms as a collateral effect of a measure aimed at illegal content or an illegal site or platform fails *per se* the "adequacy" test, in so far as it lacks a "rational connection", that is, a plausible instrumental relationship between the interference and the social need pursued. By the same token, blocking orders imposed on sites and platforms which remain valid indefinitely or for long periods are tantamount to inadmissible forms of prior restraint, in other words, to pure censorship."

Furthermore, the ECtHR held that the judicial review procedures concerning the blocking of websites in Turkey are insufficient to meet the criteria for avoiding abuse, as Turkish domestic law does not provide for any safeguards to ensure that a blocking order in respect of a specific website is not used as a means of blocking access in general. Accordingly, the ECtHR found there had been a violation of the right to freedom of expression.

In another case in the Turkish Constitutional Court in 2021, it was found that blocking access to news articles on account of a violation of reputation and personal rights unjustifiably infringed the right to freedom of expression and, again, that the domestic law which permitted the blocking provided no opportunity to realistically challenge the decision and no procedural safeguards against excessive and arbitrary internet-blocking measures.[26]

Similar considerations relating to ligation in respect of internet shutdowns are applicable in the context of blocking and filtering. However, there are further practical considerations that might be of use to potential litigators and activists.

[26] Global Freedom of Expression: Columbia University, 'The Case of Keskin Kalem Yayıncılık v. Ticaret A.Ş.,' (2021) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/the-case-of-keskin-kalem-yayincilik-v-ticaret-a-s/).

Tips for measuring restrictions

The Open Observatory of Network Interference is a useful, free resource that detects censorship and traffic manipulation on the internet. Their software can help measure:

- Blocking of websites.
- Blocking of instant messaging apps (WhatsApp, Facebook Messenger and Telegram).
- Blocking of censorship circumvention tools (such as Tor).
- Presence of systems (middleboxes) in your network that might be responsible for censorship and/or surveillance.
- Speed and performance of your network.

This tool can be a helpful way to collect data that can be used as evidence of restrictions to access.

Conclusion

Activists and litigators should remain vigilant in relation to blocking and filtering and, where necessary, apply the principles of legality, proportionality, and necessity to establish when the restriction of content amounts to a rights violation. As international pressure against full-scale internet shutdowns mounts, litigators should be cognisant that blocking and filtering may increase as a popular measure to restrict the free flow of information.

Social Media Taxes

Overview of social media taxes

Social media taxes, as the name indicates, refers to the fairly recent concept of an additional tax that is placed on social media users. This has been a growing trend in Africa, with Uganda leading the way with the introduction of the Excise Duty (Amendment) Act 2018. This Act envisages that "a telecommunication service operator providing data used for accessing over-the-top services is liable to account and pay excise duty on the access to over-the-top services." Taxing over-the-top services (**OTTs**) is supposedly set to create a level playing field among telecommunications service providers and to favour local content over international content.

Impacts of social media taxes

Such taxes "disproportionately and negatively impact the ability of users in Uganda to gain affordable access to the internet, and thus unduly restrict their right to freedom of expression."[27]
The Ugandan Tax Authority reported that within a year of the tax being introduced, it had only received 17% of the anticipated revenue. Reportedly, many social media users relied on virtual private networks (**VPNs**) to avoid the financial implications of the tax, and research has found that the tax "actually lowered domestic tax revenue and reduced Internet use."[28]

Further, "since mobile money is disproportionately used by lower-income households and individuals (informal sector, women, youth, etc), mobile money taxes have implications on the attainment of financial inclusion and wider socio-economic development goals".[29] Uganda subsequently abandoned the OTT tax, but later introduced a new 12% tax on internet data, which is likely to have similar effects.

Tanzania, Mozambique and Benin have also attempted to initiate such taxes, along with a host of other African countries.[30] This trend has sparked concern among digital rights activists and individual users alike.

Human rights implications of social media taxes

There are clear rights-based implications for the use of social media. The additional financial burden will curb people's access and enjoyment of online content, and it may also diminish their ability to access information and exchange ideas. Human Rights Watch has expressed concern that the proposed tax is "just another way for authorities to stifle free speech", explaining that "[t]axing anyone to use social media is an affront to their basic human rights."[31] Research ICT Africa has pointed out that "in some countries these taxes are… a tactic for repressive governments to control freedom of speech where dissent coincides with the largest band of Internet users, who are often between 18 to 35 years of age."[32]

The international human rights framework on access to the internet and the promotion of the right to freedom of expression has been discussed, in detail, above. The same principles apply here, save for the addition of a brief review of the African human rights system.

---

[27] ARTICLE 19 'Eastern Africa new tax and licensing rules for social media threaten freedom of expression' (2018) (accessible at https://www.article19.org/resources/eastern-africa-new-tax-and-licensing-rules-for-social-media-threaten-freedom-of-expression/).
[28] Research ICT Africa, 'COVID-19 exposes the contradictions of social media taxes in Africa,' (2021) (accessible at: https://www.africaportal.org%2Fdocuments%2F21197%2FCOVID-19-social_media_taxes_in_Africa.pdf&usg=AOvVaw2IBpeOS-hjI-78IXJedOta&cshid=1665150125432582).
[29] Id.
[30] Id.
[31] Human Rights Watch 'Uganda's Troubling Social Media Tax
New Law Restricts Right to Free Speech and Information on Social Media' (2018) (accessible at https://www.hrw.org/news/2018/07/02/ugandas-troubling-social-media-tax).
[32] Research ICT Africa above n. 30.

In 2016, the ACHPR adopted a Resolution on the Right of Freedom of Information and Expression on the Internet in Africa. The Resolution recalls the 2012 United Nations Human Rights Council Resolution, discussed above, and affirms that "the 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." The Resolution recognises the importance of the internet in advancing human and people's rights in Africa, particularly the right to freedom of information and expression.

In 2018, the ACHPR expressed concern regarding the growing trend of states in East Africa adopting stringent regulations on the internet and internet platforms. The ACHPR noted particular concern over the following developments:

- The Electronic and Postal Communications (Online Content) Regulations 2018 in Tanzania, which introduced licensing requirements for bloggers that required them to pay up to 2,100,000 Tanzanian Shillings (around USD900) for licences.
- The Excise Duty (Amendment) Bill 2018 in Uganda, which requires users of OTTs, such as social media platforms, to pay UGX200 (USD0.05), per user, per day of access.
- The directive issued by the Kenya Film and Classification Board on 14 May 2018 requiring licences for anyone posting videos for public exhibition or distribution online on their social media accounts.
- The 5% levy on telecommunications proposed by the Nigerian government in 2022, which was halted after Communications and Digital Economy Minister Isa Pantami argued that the sector was already over-taxed in the face of rising costs.

The ACHPR further stated:

> "These regulations may negatively impact the ability of users to gain affordable access to the Internet, which goes against States' commitment to protect the right of every individual to receive information, as well as the right to express and disseminate one's opinion within the law which is provided under Article 9 of the African Charter on Human and Peoples' Rights."

The ACHPR's 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa also addresses the issue of social media taxes under Principle 38 on Non-interference, which states that:

> "States shall only adopt economic measures, including taxes, levies and duties, on internet and information and communication technology service end-users that do not undermine universal, equitable, affordable and meaningful access to the internet and that are justifiable and compatible with international human rights law and standards."

Recent examples in Africa

Kenya

The Kenyan Film and Classification Board requires citizens to obtain a license to be able to post videos for public consumption. The Board has explained that it seeks to protect national security from illegal filming activities, as well as provide an additional stream of revenue. The additional cost raises concerns about the ability of video producers to operate, including concerns that this could have far-reaching consequences for freedom of expression online, although it is unclear if the regulations apply to all video producers posting on social media.

Potential developments to monitor in Kenya

The Kenya Information and Communication (Amendment) Bill was presented to Parliament in 2019. The Bill seeks to introduce regulations relating to the licensing of social media platforms and sharing of information by licensed persons. The Bill aims to create obligations on social media users, requires the registration of bloggers, and allows the Communications Authority to develop a bloggers code of conduct. The Board appears to be calling for the adoption of this legislation. The Board's CEO has indicated that "social media is a threat to the country's moral fabric as it negatively influences the youth." Although the Bill appears to have languished since its introduction in 2019, such legislative efforts raise serious concerns for freedom of expression on the internet.

Tanzania

Tanzania has also introduced licensing requirements which attach additional fees to social media. The Electronic and Postal Communications (Online Content) Regulations, 2020 introduced new online content regulations. Bloggers, in particular, are required to pay unreasonably high fees in order to obtain a license. Among other concerns with the regulations, the licensing requirement has been heavily criticised for being incompatible with the right to freedom of expression. The Association for Progressive Communications (**APC**) argues that:

> "Tanzania's new excise duty in the form of online content licence fees fundamentally threatens universal access to and affordability of the internet. Consequently, it clearly constitutes a limitation on the right to freedom of expression. Further, it is unjustifiable when measured against the arguments that could be made by the Tanzanian government in support of the increase, such as the need to ensure appropriate excise duty levels in order to ensure the fiscal sustainability of the state in meeting the developmental and other socioeconomic rights of its inhabitants."[33]

[33] APC above n 17 at 12.

Attempts to oppose the Regulations

- In 2018, ARTICLE 19 reviewed the Tanzania Regulations. The report ultimately found that they were defective and wholly at odds with international standards on freedom of expression. ARTICLE 19 recommended that the Regulations should be withdrawn entirely and called on the Tanzanian government to do so. ARTICLE 19 also reviewed subsequent amendments to the Regulations in 2020 and found that several issues with the 2018 Regulations had not been addressed at all, and others had been made worse, including failure to limit the sweeping power of the Authority and a failure to provide appropriate due process safeguards in the licensing process.
- In April 2018, Reuters reported that civil society activists obtained a temporary court injunction against the regulations from Tanzania's High Court that would require bloggers to, among other things, pay a tax, obtain a clearance certificate and obtain an operating license.
- In May 2018, Reuters reported that the Tanzanian government overturned the injunction. As a result, owners of social media platforms are required to register and comply with the regulations.

Conclusion

The trend of introducing social media taxes in Africa warrants concern. There appears to be a misnomer that states can wilfully ignore their obligation to respect, protect and promote the right to freedom of expression in pursuit of economic gain. The ACHPR, civil society actors, and affected individuals should continue to speak out against these trends. Litigation, policy reform and advocacy strategies need to be urgently adopted to re-route the current trajectory away from increased reliance by states on social media taxes.

Distributed Denial-of-Service Attacks

Overview of DDoS attacks

The UNSR on FreeEx defines a DDoS attack as a cyber-attack that seeks to undermine or compromise the functioning of a computer-based system.[34] The UNSR notes further that a DDoS attack can have the same effect as an internet shutdown. This increasingly common online phenomenon uses a large number of computers to target websites and online services and overwhelms them with more traffic than they can handle, rendering them temporarily inoperable.[35]

[34] Access Now, 'Defending users at risk from DDoS attacks: An evolving challenge' (2015) (accessible at https://www.accessnow.org/defending-users-at-risk-from-ddos-attacks-an-evolving-challenge/).
[35] See further Media Defence above n 3 at 23.

DDoS Attacks and critical moments

The 2019 UNSR Research Paper on Freedom of Expression and Elections in the Digital Age found:

> "During elections, State actors have historically denied access to unfavourable views and information concerning incumbent officeholders … One common practice involves the use of Distributed Denial of Service ("DDoS") attacks, [which] have targeted the websites of political parties, journalists and media outlets, and human rights defenders and civil society organizations. Perpetrators have also targeted the websites of States' election commissions, which publicize critical information such as changes to ballot locations. DDoS attacks are also potentially a cover for coordinated hacks on voter registration and other electoral databases and other attempts to steal the data of voters, candidates and public officials. Given that online media have become the primary resource of news and information for many voters, and the integration of electronic systems into electoral processes, DDoS attacks are likely to increase in magnitude and frequency. Furthermore, in the Internet of Things era, the growing number of connected devices makes them attractive targets for DDoS attacks."

Given their similarity to internet shutdowns, DDoS attacks, whether committed by a state or non-state actor, infringe the right to freedom of expression. They are usually well hidden, covert, and illicit in nature, and, accordingly, fall foul of the "provided by law" requirement of Article 19(3) of the ICCPR. They completely disable access to online content, usually during a critical time – such as an election – and they are distinctly disproportionate. The UNSR Research Paper further found that DDoS attacks "whether committed by State actors or their agents, are incompatible with Article 19 of the ICCPR" and are "almost always unnecessary and disproportionate measures under Article 19(3)."

The Inter-American Commission on Human Rights reported in 2013 that DDoS attacks can be extremely disruptive to the exercise of the right to freedom of expression, and, as a result, states are obligated to investigate and properly redress such attacks. The principles mentioned above and sentiments relating to access and freedom of expression are implicated by DDoS attacks. The UN Guiding Principles on Business and Human Rights can also be relied on when trying to prevent and mitigate DDoS attacks by non-state actors, including the safeguarding of systems infrastructure.

Examples of DDoS attacks

In 2017, Freedom House reported:

> "Independent blogs and news websites are increasingly being taken down through distributed denial-of-service (DDoS) attacks, activists' social media accounts are being disabled or hijacked, and opposition politicians and human rights defenders

> are being subjected to surveillance through the illegal hacking of their phones and computers. In many cases, such as in Bahrain, Azerbaijan, Mexico, and China, independent forensic analysts have concluded that the government was behind these attacks."

DDoS attacks are affecting states across the world, regardless of their social policies or economic status:

- In 2018, it was reported that a website of a Mexican political opposition party was rendered inoperable by a DDoS attack. The attack occurred during a debate between presidential candidates in the lead up to the elections.
- In 2019, the South African financial sector fell victim to a string of DDoS attacks.
- DDoS attacks were ranked among the top five security threats in Kenya in 2019.
- British political parties were also subject to back-to-back DDoS attacks in the lead up to the general election in 2019.

Conclusion

Be it politically, socially, or economically motivated, DDoS attacks are a legitimate threat to freedom of expression. Nefarious state and non-state actors are becoming increasingly skilled and sophisticated, posing new challenges for states to overcome in order to ensure they fulfil their positive obligations to protect and promote freedom of expression. Mitigating DDoS attacks in future will take multidisciplinary teams of litigators and technologists working jointly to protect and promote freedom of expression.

Accountability of Private Platforms for Content Moderation

Overview of Content Moderation

As internet and social media companies have become increasingly influential in the digital age, questions have arisen about the accountability mechanisms in place for these actors who hold extraordinary power over the ability of the general public to exercise their rights to freedom of expression and access to information. The content moderation policies of these tech giants effectively block and filter the content not only that individuals can post, but also that other users can access. As a result, attention is now mounting on how these companies make their decisions about removing or deprioritising content, and the transparency and accountability mechanisms in place to ensure that they comply with human rights law and standards.

Critics argue that users in African countries, in particular, lack the influence over and access to these big multinational companies to be able to understand how content moderation may be affecting their freedom of expression and to take action where content is removed (or where illegal content remains up).

Various cases have recently reached the courts in this regard:

- In Germany, the Federal Court of Justice ruled that Facebook's terms of service on deleting user posts and blocking accounts for violations of its Community Standards were invalid because they did not make provision for informing users about decisions to remove their content and to grant them an opportunity to respond, followed by a new decision.

- In France, the Paris Court of Appeal ordered Twitter to provide information on the measures the company was taking to fight online hate speech in a case brought by organisations who had found, in their research, that Twitter only removed under 12% of tweets that were reported to them.

- In another case involving Facebook, the Republic of The Gambia initiated proceedings in the United States requesting Facebook to release public and private communications and documents about content that Facebook had deleted following the genocide in Myanmar. The Gambia had previously initiated proceedings in the International Court of Justice against Myanmar claiming a breach of its obligations under international law for its alleged crime of genocide against the Rohingyas. The Gambia thus sought information from Facebook on content that it had removed which may have contributed to or exacerbated the violence against the Rohingyas, given Facebook's dominant position as an almost sole news provider in that country at the time. The US District Court held that Facebook must disclose the requested materials.

These cases show the various ways in which private platforms are being held accountable for the content moderation decisions they make that have very real impacts on users' rights to freedom of expression, as well as other rights.

Non-Consensual Dissemination of Intimate Images

In recent years, the issue of the Non-Consensual Sharing of Intimate Images (NCII) has become increasingly prominent as a result of the unfortunate proliferation of this form of online gender-based violence. In many cases content is shared in order to blackmail, threaten, or harass internet users, predominantly women and gender minorities. It is vital that the rights of the victims/survivors to privacy and reputation are protected by enabling such content to be rapidly and permanently removed. While this is one of the narrow circumstances in which the removal of content is not only justified but absolutely critical to protecting human rights, it is still important to maintain appropriate checks and balances over the tech companies that make decisions regarding the removal or blocking of content.

Case law on NCII

A body of case law is gradually building up that provides guidance on how courts are interpreting this issue around the world:

- In a case in India in 2021, the High Court of Delhi upheld an actor's right to privacy under the Indian Constitution and directed internet intermediaries as well as YouTube, the host of the content, to take down the explicit videos of the actor which had been uploaded on to multiple video-sharing platforms without her consent.

- In another case in India, the High Court of Delhi ordered the police to remove content that was unlawfully published on a pornographic website and went further to order search engines to de-index that content from their search results. In its judgment, the Court stressed the need for "immediate and efficacious" remedies for victims of cases of NCII and set out the type of directions that a court can issue in such cases.

- The Constitutional Court of Ecuador dealt with a case in 2021 in which pictures of the victim/survivor had been sent to their parents without the victim's consent. The Court also found in favour of the right to privacy and held, in the words of the Columbia Global Freedom of Expression database, that "the storage and sharing of sexual photos without the consent of the victim were a violation of her constitutional rights to personal data protection, reputation, and intimacy" and that "intimate images were personal data sent exclusively to the defendant's partner and required previous consent to be processed by anyone else."

Some countries are also incorporating provisions criminalising NCII in domestic law. For example, South Africa's Cybercrimes Act, passed into law in 2020 criminalises the disclosure of data messages that contain intimate images of a person without the latter's consent. While such provisions are welcomed for the recourse they provide to victims of online gender-based violence, concerns have also been raised about the potential for infringements on the right to freedom of expression if such provisions are vague, broad, or open to abuse. It is, therefore, crucial, that protections for privacy are carefully balanced against potential intrusions into freedom of expression in the online space. Litigation by civil society can play an important role in appropriately defining this balance and ensuring the advancement of digital rights for all.

Conclusion

The power and opacity of the tech giants raise real questions about the legitimacy of content moderation decisions that are made on a daily basis and how they affect the information environment around the world. Litigation has been shown to be a powerful way to seek greater transparency and accountability from these actors and to achieve a more rights-respecting balance between the various rights implicated by different types of content online.

Conclusion

The internet is a site of struggle for the advancement of human rights. Restricting access to the internet, either through internet shutdowns, blocking and filtering, imposing regulatory restrictions, or facilitating DDoS attacks limits people's fundamental human rights. The promotion, protection, and enjoyment of human rights on the internet is well established as a norm under international human rights law, and restricting access to the internet, by states or non-state actors, violates human rights and can only be justified under very narrow circumstances.

It is comforting to observe that despite the rise of restrictive conduct, the international community, civil society actors and individuals are fighting to advance freedom of expression and digital rights. Fortunately, there are strong legal foundations that allow for progressive and dynamic solutions to these contemporary challenges.