*Module 1*

# General Overview of Trends in Digital Rights Globally and Expected Developments

*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 1

## General Overview of Trends in Digital Rights Globally and Expected Developments

**This module aims to:**

- **Provide an overview of global trends in digital rights.**
- **Set out trends and expected developments relating to the right of access to information, including emerging threats and challenges.**
- **Outline trends and expected developments relating to privacy rights, including emerging threats and challenges.**
- **Explore trends and expected developments relating to freedom of expression online, and current efforts to address restrictions on freedom of expression.**

---

### Introduction

Over the last decade, the number of internet users worldwide has more than doubled. As of 2021, the digital population consists of nearly five billion people.[1] In Africa, the number of recorded internet users increased four-fold between 2011 and 2021, going from fewer than 140 million people to over 600 million in just ten years.[2] The internet has revolutionised the free flow of information by offering anyone with an internet connection the ability to gather and share information and ideas.[3] This had a profound effect on the exercise and the protection of the triad of information rights, namely the rights to privacy, freedom of expression and access to information.

The UN Human Rights Council's (**UNHRC**) 2016 Resolution on the promotion, protection and enjoyment of human rights on the internet confirmed that these rights, in turn, enable a full array of other fundamental rights. The Resolution also affirmed that these rights are advanced and exercised online, they deserve the same protections as when they are advanced offline.

Unfortunately, despite the internet's potential as a tool for democratic empowerment, the rights of internet users globally are subject to a wide range of challenges, threats, restrictions, and violations, at the hands of both state and non-state actors.

There is no shortage of obstacles to achieving the full capacity of the internet and digital technology to be platforms where human rights can be protected, respected, promoted, and

[1] Statista, 'Number of internet users worldwide from 2005 to 2021,' (accessible at https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/).
[2] Statista, 'Number of internet users worldwide from 2009 to 2021, by region,' (accessible at https://www.statista.com/statistics/265147/number-of-worldwide-internet-users-by-region/).
[3] ARTICLE 19, 'Digital Rights' (accessible at https://www.article19.org/issue/digital-rights/).

progressively realised. Fortunately, in many instances, digital rights advocates, activists and litigators have developed effective responses to oppressive regulations and restrictions on online rights, and there is a notable rise in innovative solutions challenging these problems. This module touches on recent developments relating to the triad of information rights, and highlights expected developments moving forward.

## The Right to Access Information

Access to the internet has increased significantly over the last decade. Regrettably, restrictions on the right to access information have also increased, including internet shutdowns, blocking and filtering of content, social media taxes, censorship, and distributed denial of service (**DDoS**) attacks.

*Internet shutdowns*

Dozens of countries have been affected by internet shutdowns in recent years. In 2021, Access Now and the #KeepItOn coalition documented at least 182 internet shutdowns in 34 countries around the world.[4] Myanmar, Zimbabwe, India, and the Tigray region of Ethiopia have seen some of the most prolonged internet shutdowns in history.

- In 2019, Myanmar experienced more than 100 days without internet services. In justifying the shutdowns, the chief engineer for the state-owned telecoms network insisted that the internet shutdowns were for the benefit of the people.[5] There continued to be a series of prolonged internet shutdowns in various regions of Myanmar in 2021 and 2022, with the longest nationwide outage reported as being nearly 2.5 months.[6] The start of 2020 saw another spate of internet shutdowns in two of Myanmar's conflict-ridden states.[7]
- At the beginning of 2019, the Zimbabwean government ordered a three-day internet shutdown across the country amid protest action. Following an interim court ruling, the internet was partially restored, but some social media platforms remained blocked.[8]
- India had nearly 100 internet shutdowns during 2019, including the most protracted recorded shutdown in history in Kashmir.[9] In 2020, the Supreme Court in India ruled that indefinite internet shutdowns violated freedom of speech and expression, ordering the

[4] Access Now, '#KeepItOn' (accessible at: https://www.accessnow.org/keepiton/).
[5] Access Now, 'As Myanmar marks 101 days of internet shutdowns, the #KeepItOn coalition urges full restoration of internet access' (2019) (accessible at: https://www.accessnow.org/as-myanmar-marks-101-days-of-internet-shutdowns-the-keepiton-coalition-urges-full-restoration-of-internet-access/).
[6] Access Now, Internet shutdowns in 2021' (2022) (accessible at: https://www.accessnow.org/internet-shutdowns-2021/)
[7] Al Jazeera, 'Myanmar reimposes internet shutdown in Rakhine, Chin states' (2020) (accessible https://www.aljazeera.com/news/2020/02/myanmar-reimposes-internet-shutdown-rakhine-chin-states-200204050805983.html).
[8] Access Now, 'Zimbabwe orders a three-day, country-wide internet shutdown' (2019) (accessible at: https://www.accessnow.org/zimbabwe-orders-a-three-day-country-wide-internet-shutdown/).
[9] BBC, 'Why India shuts down the internet more than any other democracy' (2019) (accessible at https://www.bbc.com/news/world-asia-india-50819905).

government to publish reasons, including the duration of the shutdown, each time it wishes to implement this action in future.[10]

- In Tigray, a northern region of Ethiopia in which fighting between rebels and government forces has been ongoing since November 2020, the internet and phone service have been shut down for nearly two years, with the government arguing the measures are necessary to curb violence and critics accusing authorities of using the internet as a weapon of war.[11]

In a positive legal development, the Community Court of Justice of the Economic Community of West African States (ECOWAS) held in 2020 that the Togolese government had violated the right to freedom of expression by shutting down the internet during protests in that country in September 2017, finding that access to the internet is a derivative right that enhances the exercise of freedom of expression.[12] Because the country did not have a national law that specified the grounds on which an interference in the right to freedom of expression could be justified, the Court concluded that the internet was not shut down in accordance with the law and that the government had violated Article 9 of the African Charter on Human and Peoples' Rights **(the African Charter).**

It appears that internet shutdowns are increasingly a tool that governments are willing to use to control criticism and protest, especially at times of civil unrest or around election periods. However, recent jurisprudential developments have indicated strong legal support for the position that such shutdowns are an unjustifiable violation of the right to freedom of expression and access to information, and it is hoped that such developments will continue and will spark the necessary civic awareness – particularly among mobile operators and civil society – to generate actions that will ensure the protection of people's rights in the digital age.

**#KeepItOn**

Access Now's #KeepItOn coalition monitors and reports on internet shutdowns across the globe. The #KeepItOn coalition has been fighting internet shutdowns with various creative approaches, including grassroots advocacy, direct policymaker engagement, technical support and legal interventions.

Important initiatives such as these are likely to continue as lawyers and civil society organisations (**CSOs**) find new ways to push back against attempts to restrict access. These initiatives fulfil an essential role in keeping users informed about state actions that are contrary to international human rights norms.

[10] *Bhasin v Union of India*, Writ Petition No. 1031 of 2019, Supreme Court of India (accessible at: https://main.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf).
[11] Zecharias Zelalem, 'FEATURE-Six million silenced: A two-year internet outage in Ethiopia,' Reuters (accessible at: https://www.reuters.com/article/ethiopia-internet-shutdown-idAFL8N2ZM09X).
[12] 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/.)

*Blocking and filtering of content*

Censorship has been on the rise over the past decade. A new and increasingly prevalent form is social media censorship, which is characterised by the blocking and filtering of certain content on social media. Blocking refers to the prevention of access to a website, domain or IP address. In contrast, filtering is the use of technology that sieves through content, blocking individual pages that display specific characteristics.[13] Although considered less extreme than internet shutdowns or other measures that fully limit access, such mechanisms are deeply concerning also for the potential they have to distort the information that is available to a population, potentially enabling propaganda and limiting diverse viewpoints in more subtle ways that total restrictions on access. Blocking and filtering may, in some instances, constitute a violation of article 19 of the Universal Declaration of Human Rights (**UDHR**), which grants everyone the right "to seek, receive and impart information and ideas through any media and regardless of frontiers."

In the last decade, China has developed the largest and the most sophisticated online censorship regime in the world. As a result, many controversial events are prohibited from news coverage, preventing Chinese citizens from becoming aware of their government's actions.[14] However, China is not alone in this regard. Several governments have taken to censoring in order to control the flow of information, especially around critical times like election periods. In a 2011 Report, the UN Special Rapporteur (**UNSR**) on the promotion and protection of the right to freedom of opinion and expression (**FreeEx**) noted with particular concern the—

> "emerging trend of timed (or "just-in-time") blocking to prevent users from accessing or disseminating information at key political moments, such as elections, times of social unrest, or anniversaries of politically or historically significant events. During such times, websites of opposition parties, independent media, and social networking platforms such as Twitter and Facebook are blocked, as witnessed in the context of recent protests across the Middle East and North African region."

- Freedom House noted that in Egypt in 2018, internet blocking increased to unprecedented levels during the presidential elections. In 2019, NetBlocks reported that an estimated 34 000 internet domains supporting an opposition campaign were blocked in Egypt.
- In early 2019, Chad reached over 365 days of censored access to the internet following a recommendation to amend the Constitution to allow the President to remain in power until 2033.[15]

[13] ARTICLE 19, 'Freedom of Expression Unfiltered: How blocking and filtering affect free speech' (2016) (accessible at https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf).
[14] Human Rights Watch, 'China's Global Threat to Human Rights' (2019) (accessible at https://www.hrw.org/world-report/2020/china-global-threat-to-human-rights).
[15] CNN, 'Chadians feel 'anger, revolt' as they struggle without internet for one year' (2019) (accessible at https://edition.cnn.com/2019/04/24/africa/chad-internet-shutdown-intl/index.html).

- In 2021, the Nigerian government banned Twitter in what was widely seen as retaliation by President Muhammadu Buhari for Twitter's moderation of a tweet that it says violated its policies on incitement.[16]In a foundational case for social media blocking decided in July 2022, the ECOWAS Community Court of Justice held that the seven-month ban was unlawful and violated the freedom of expression of the people of Nigeria.[17]

This phenomenon is a threat not only to the public's right to access information but also to the very core of democracy. It is expected that with increases in the number of people with access to the internet and the potential for citizen organisation and uprisings on social media, resultant increases in censorship may be likely.

**Jurisprudence in the ECtHR on blocking**

In the 2021 case of *OOO Flavus v Russia* (2020), the European Court of Human Rights (ECtHR) held that the indiscriminate blocking of entire online news websites without giving notice of the specific offending material was a breach of the right to freedom of expression.

Likewise, the case of *Vladimir Kharitonov v Russia* (2020) also involved the wholesale blocking of a website, this time seemingly in error because it shared an IP address with another website sharing illegal content. The ECtHR held that the blocking orders effect on co-hosted websites was far beyond the illegal content actually targeted and was, therefore, a violation of the right to freedom of expression.

*Social media taxes*

A number of African states have introduced or considered introducing, taxes specifically for the use of social media, ostensibly to raise public revenues or protect the local telecommunications sector from competition. This has resulted in more people being pushed offline, increases barriers to getting online, and limits on freedom of expression and access to information — as well as to goods and services.[18]

The Web Foundation has noted that Africa is the continent with the highest financial barriers to internet access. Social media taxes add yet another barrier to accessing a resource that is already inaccessible to many people, which serves to deepen the digital divide and hinder people's rights.

In Uganda, the government imposed a new tax scheme for the daily use of mobile communications apps such as Facebook, Twitter, Instagram, LinkedIn, WhatsApp, Snapchat

[16] Emmanuel Akinwotu, 'Nigeria lifts Twitter ban seven months after site deleted president's post,' (2022) The Guardian (accessible at: https://www.theguardian.com/world/2022/jan/13/nigeria-lifts-twitter-ban-seven-months-after-site-deleted-presidents-post).
[17] *SERAP v. Federal Republic of Nigeria*, ECW/CCJ/JUD/40/22, 2022 (accessible at: https://globalfreedomofexpression.columbia.edu/cases/serap-v-federal-republic-of-nigeria/).
[18] Mozilla Foundation, 'Internet Health Report, 2019,' (2019) (accessible at: https://internethealthreport.org/2019/taxing-social-media-in-africa/).

and Skype. The Collaboration on International ICT Policy in East and Southern Africa (**CIPESA**) recorded that the internet penetration rate in Uganda dropped by 5 million users within three months of the social media tax scheme's rollout, severely limiting freedom of expression and access to information. Research also found that the tax lowered domestic tax revenue.[19]

Although Uganda subsequently abandoned the OTT tax (but later introduced a new 12% tax on internet data) it is only one of many African countries that are considering imposing taxes on the use of social media. Tanzania, Mozambique and Benin have also attempted to initiate such initiatives, along with a host of other African countries.[20] However, despite these growing concerns, there have been notable successes in challenging this emergent threat.

**Don't Tax My Megabytes**

In 2018, the citizens of Benin took to social media following the introduction of a tax that specifically targeted the use of social media networks.

Thousands of social media accounts on Facebook and Twitter used the Hashtag "TaxePasMesMo" (Don't Tax My MegaBytes). After a few weeks of concerted digital protest, the government repealed the tax.

Internet Without Borders welcomed the victory and noted:

> "The mobilisation online, around the Hashtag #TaxePasMesMo (Don't Tax My MegaBytes), showed to the world the anger of netizens in the country. This anger and resentment enabled them to denounce the tax and to enter into a dialogue with the authorities, which fortunately led to the tax's cancellation. This case also shows the strength of the young Beninese democracy. The annulment of the social media tax is an important precedent for digital rights and freedoms in West Africa."

The introduction of social media taxes is a violation of the right to access information. Unfortunately, it is a growing trend, and it is possible that more countries, particularly in Africa, will resort to social media taxes, either due to genuine economic need, or to restrict access and limit freedom of expression to disarm dissent. However, it is expected that lawyers, CSOs and citizens will continue to push back against this threat. The success of #TaxePasMesMo is indicative of innovative forms of digital protest aimed at challenging the introduction of restrictions on freedom of expression.

[19] 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).
[20] Id.

*Registration of bloggers*

Bloggers – a largely undefined group of people who write online entries, self-publish, might remain anonymous and might write informally, semi-professionally or professionally – fulfil an essential role in our contemporary society by disseminating information through the exercise of their right to freedom of expression. Despite being an open-ended group, bloggers play a similar role to journalists in enabling informed discussion and access to information, and many international standards and guidelines on freedom of expression online provide legal standards that protect bloggers and journalists alike.[21]

Given the critical role bloggers play in disseminating information, they, like journalists, should operate in an enabling environment that promotes free expression and the sharing of opinions. Unfortunately, the rising trend of blogger registration threatens that goal:

- In 2018, Tanzania introduced new laws that require bloggers to pay licensing and registration fees. The fact that Tanzania's GDP per capita is approximately $1 000 (USD), and the licence fee for bloggers is approximately $900 (USD) raises serious questions about the economic feasibility of this initiative. The law makes blogging without a license a criminal offence, which drew heavy criticism from civil society organisations. Human Rights Watch notes that the licensing fee has introduced a severe barrier to freedom of expression and the dissemination of information and that the disproportionately high fees are pushing bloggers offline.
- In Kenya, a 2019 private members' bill, the Information and Communication (Amendment) Bill, sought to introduce regulations relating to the licensing of social media platforms and sharing of information by licensed persons. The Bill would require the registration of bloggers and allow the Communications Authority to develop a bloggers' code of conduct.

Growing threats to formal and informal modes of journalism are on the rise. Imposing burdensome obligations on bloggers and journalists should be strongly condemned, and states should be compelled to respect and protect their international human rights obligations.

*Increased access and the need for digital literacy and safeguards*

Information and Communication Technologies (**ICTs**) have become critical tools for boosting economic growth and development. In doing so, they have the potential to assist with the achievement of socio-economic goals and aspirations. Resultantly, there ought to be appropriate access to ICTs, coupled with digital literacy, to ensure that these goals can be reached.

Almost all countries around the world have experienced a dramatic increase in access to ICTs in recent years. Statista records that Africa has taken great strides in recent years, with an estimated 600 million African internet users in 2021 – representing exponential growth in the previous decade.

[21] The UN's General Comment 34 to the International Covenant on Civil and Political Rights (ICCPR) includes bloggers in its assessment of journalism, stating that any restriction on the operation of websites, blogs or any other internet-based systems are not compatible with the right to freedom of expression.s

These shifting digital frontiers bring a corresponding need to ensure support for digital literacy and inclusion. Digital literacy is critical to realising the full potential of digital development and that all users are able to use online spaces safely and inclusively and leverage the benefits of the digital era. As societies have become increasingly dependent on digital tools in the wake of the COVID-19 pandemic, the necessity of digital literacy has only become more urgent.

**Digital literacy in Africa**

Afrobarometer has found that 55% of adults in Africa are likely to be ill-prepared for remote learning to participate in or assist members of their household with a transition to an online learning environment. Measures of African citizens' ability to use digital devices and applications and to access the internet show that while there have been dramatic improvements in recent years, there are still significant differences between countries. In Mozambique, for example, only 10% of people had successfully adopted digital skills in 2019, compared to 30% in Kenya.

It is forecasted that by 2030 there will be 230 million jobs in Sub-Saharan Africa that require digital literacy. To match this expectation, it is reported that 650 million training opportunities will need to be made available by 2030.[22]

While there are pockets of progress, it is vital that improvements in internet access and increases in demand are proportionally matched with efforts to boost digital literacy rates in order to protect new internet users from online harms, to build safe, inclusive, and constructive online public domains, and to ensure that the full spectrum of ICT opportunities is available to everyone. Without appropriate digital literacy as internet access continues to grow, online harms will persist and may increase, putting some of the most vulnerable members of our society at risk.

*The interplay between net neutrality and zero-rated content*

Net neutrality refers to the principle of seeking to ensure that access to digital content is open, free-flowing, fair, and equal. It has been flagged that net neutrality may be under threat by the increasingly popular initiative of zero-rating, a process in which specific online content is made available for free to users (i.e., without the need to pay telecommunications providers for the associated data costs) on the grounds that it is of public interest, such as news or educational content.

The Electronic Frontier Foundation (**EFF**) explains that net neutrality fulfils the critical role of ensuring that people can freely access information and impart ideas across the digital information society, without interference or direction from other actors. Efforts to control the free flow of information have the potential to distort content consumption by enabling free

[22] International Finance Cooperation, 'Digital Skills in Sub-Saharan Africa' (2019) (accessible at https://www.ifc.org/wps/wcm/connect/ed6362b3-aa34-42ac-ae9f-c739904951b1/Digital+Skills_Final_WEB_5-7-19.pdf?MOD=AJPERES).

access to certain content in preference to other content, as well as access to the market. Zero-rating has been flagged as one example of such a control measure. There are levels to this debate, with some arguing that zero-rating can be a tool to facilitate universal access to the internet and to critical public good information. Many digital rights activists, such as the EFF, are not swayed by the argument that some access is better than no access. They argue that zero-rating is a means for the new internet gatekeeps to centralise power and control access.

### Net neutrality in contestation

During 2015 and 2016, the net neutrality debate took centre stage in India when Facebook and Airtel offered differential pricing for access to certain content and no-fee access to other content. Following public outcry, the Indian Telecom Regulatory Authority announced that shaping users' access to the internet would not be allowed. India has since adopted strong net neutrality regulations.[23]

The United States has also recently engaged in this issue, resulting in the 2018 Federal Communications Commission decision to repeal net neutrality laws.[24] In 2021, US President Joe Biden sought to reverse the repeal after he assumed office, calling on regulators to reinstate net neutrality rules.[25] The net neutrality debate is continuing in the US and around the world, illustrating the difficult challenges involved in finding a balance between enabling greater access to content while ensuring that it remains equal and free.

African countries – many of which continue to face low internet penetration rates – are often supportive of zero-rating policies that advance access to public good content. In South Africa, for example, the government required mobile operators to zero-rate a wide range of websites to enable virtual learning to continue when the COVID-19 pandemic hit the country in early 2020, forcing the rapid closure of schools, universities, and other educational institutions and threatening to undermine the right to education for millions of young South Africans. The South African Department of Communications and Digital Technologies later published directions providing a framework for the zero-rating of websites for education and health. The pandemic-related initiatives also led to new mandatory zero-rating obligations being placed on mobile operators that were vying for new spectrum licenses in a long-awaited spectrum auction which took place in March 2022.

[23] New York Times, 'Facebook Loses a Battle in India Over Its Free Basics Program' (2016) (accessible at https://www.nytimes.com/2016/02/09/business/facebook-loses-a-battle-in-india-over-its-free-basics-program.html); and BBC 'India adopts 'world's strongest' net neutrality norms' (2018) (accessible at https://www.bbc.com/news/world-asia-india-44796436). In 2018, the Department of Telecommunications approved recommendations from the Telecom Regulatory Authority of India on net neutrality that aimed to ensure that net neutrality is enforced nationwide (see: https://www.theverge.com/2018/7/11/17562108/india-department-of-telecommunications-trai-net-neutrality-proposal-approval).

[24] Washington Post, 'Appeals court ruling upholds FCC's cancelling of net neutrality rules' (2019) (accessible at https://www.washingtonpost.com/technology/2019/10/01/appeals-court-upholds-trump-administrations-cancelling-net-neutrality-rules/).

[25] Office of the US Presidency, 'Fact Sheet: Executive Order on Promoting Competition in the American Economy', (2021) (accessible at https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/).

As these examples show, while zero-rating carries implications for net neutrality, in societies with challenges to ICT access the policy is often viewed favourably. The potential effects require careful consideration of who is empowered to make decisions about what content should be freely accessible, and the involvement of affected populations in such decisions. There are also concerns that developing and transitioning economies may be pressured into accepting distortive zero-rating by powerful international multinationals. The experience in India has highlighted the need to ensure access to ICTs is not controlled or shaped by service providers who may use development priorities as a guise to control access for the most marginalised people.

*The rise in cybercrimes and cyber attacks*

There is growing attention to the prevalence of cybercrime as a threat to digital rights and inclusion, and the need for more appropriate state response mechanisms. Attacks on individual users, businesses, CSOs, and states are becoming commonplace: it has been reported that more than 61% of companies in Africa were affected by ransomware attacks in 2020 alone, with attacks happening every 11 seconds in a context in which countries are reported to be especially ill-prepared and vulnerable. Further to this, there is a substantial economic concern with cybercrime reported to have reduced GDP within Africa by more than 10%, at a cost of an estimated 4.12 billion USD, in 2021.

Interpol has identified the following as the top five cyberthreats in Africa at present:

- **Online scams**: fake emails or text messages claiming to be from a legitimate source that are used to trick individuals into revealing personal or financial information;
- **Digital extortion:** victims being tricked into sharing intimate images which are used for blackmail;
- **Business email compromise**: criminals hacking into email systems to gain information about corporate payment systems, then deceive company employees into transferring money into their bank account;
- **Ransomware:** cybercriminals blocking the computer systems of hospitals and public institutions, then demanding money to restore functionality;
- **Botnets:** networks of compromised machines being used as a tool to automate large-scale cyberattacks.

While cybercrime itself poses a serious threat to human rights, the corresponding rise of oppressive and aggressive cybercrime and cybersecurity measures is also jeopardising the realisation of an array of digital rights.

Despite legitimate security concerns, there is a growing trend of oppressive cybercrime laws that "do little other than robbing internet users of their basic human rights."[26] The intense and often vague legislative measures implemented to counteract cybercrime are frequently weaponised by oppressive states to restrict fundamental human rights and freedoms, leaving internet users vulnerable to both these crimes and the harsh response they elicit. In response to rapidly growing and evolving cybercrime risks, states will likely continue to be reactive and adopt measures that are unlikely to accord with international human rights norms.

## The Right to Privacy

In the last decade, there have been considerable developments relating to the exercise of the right to privacy online.

*Data Privacy*

The last decade saw the coming into force of the General Data Protection Regulation (**GDPR**). The coming into force of the GDPR was a significant development as it exposed the increasing need to protect the right to privacy in the rapidly changing technological landscape. Human Rights Watch has noted that comprehensive data protection laws are vital for securing human rights. It further stated that the GDPR has developed new safeguards that are necessary for the advancement of human rights in a digital age. In particular, it protects people against gratuitous and excessive data collection. From the time it came into effect until 2019, approximately 95 000 complaints were filed, and 59 000 breaches were reported, with approximately 60 million euros worth of fines being imposed.[27]

Another flagship data protection law, the California Consumer Privacy Act (**CCPA**), also came into effect in January 2020, seeking to address how private companies are allowed to collect and use the data of California residents. The CCPA allows residents of California to know:

- What personal information a data company has collected about them.
- What personal information third parties have obtained about them.
- The specific personal information a company has compiled about them.
- Specific inferences that have been made about them based on their personal information.[28]

[26] Open Global Rights, 'Restricting cybersecurity, violating human rights: cybercrime laws in MENA region' (2019) (accessible at https://www.openglobalrights.org/restricting-cybersecurity-violating-human-rights/). See further Public Knowledge, 'Cybersecurity and Human Rights' (2019) (accessible at https://www.publicknowledge.org/cybersecurity-and-human-rights/).
[27] Access Now, 'A GDPR progress report: how is the law being implemented in the EU?' (2019) (accessible at https://www.accessnow.org/a-gdpr-progress-report-how-is-the-law-being-implemented-in-the-eu/).
[28] New York Times, '*How California's New Privacy Law Affects You*' (2020) (accessible at https://www.nytimes.com/2020/01/03/us/ccpa-california-privacy-law.html).

The CCPA undoubtedly increases data privacy protections and sends a strong message that "[i]n a GDPR + CCPA world, negligence of data privacy protections will not be tolerated and will result in higher fines."[29]

The GDPR and CCPA set off a wave of other countries passing revised or new data privacy laws which are aimed at protecting people's data in the modern age. The UN Conference on Trade and Development (**UNCTAD**) has found that of the 194 countries they reviewed:

- 71% of countries have data protection legislation.
- 9% of the states have draft legislation.
- 15% of countries have no legislation.
- 5% of countries have no data available.

### Mapping the state of data protection in Africa

Data protection legislation is crucial to protecting the right to privacy in the digital age. The progression of legislation and regulation in this area has been rapid in Africa in recent years. dataprotection.africa is an open, online resource that aims to provide a detailed analysis of the governance of data protection across the continent, mapping and analysing the legislation in place in all 55 member states of the African Union.

Most recently, Zambia, Zimbabwe, and Rwanda passed new data protection laws in 2021, with Eswatini doing the same in 2022.

dataprotection.africa allows lawyers, activists, and individuals to navigate the data protection space and learn about:

- What constitutes personal information in a particular jurisdiction.
- How that information should be collected and processed.
- How that data can be transferred across borders.
- What breach notifications apply in a jurisdiction if data is leaked to an unauthorised third party.
- What steps can be taken to remedy such breaches, including the contact information of operational data protection authorities.

While many countries have data protection frameworks in place, there is a significant lack of implementation of these frameworks, with many countries failing to establish or appoint data protection authorities to enforce these laws.[30]

Cross-border transactions and multinational corporations that function across multiple jurisdictions require data protection regulations, demonstrating the importance of data

[29] PWC, 'Top Policy Trends 2020: Data privacy' (2020) (accessible at https://www.pwc.com/us/en/library/risk-regulatory/strategic-policy/top-policy-trends/data-privacy.html).
[30] Accessible at: www.dataprotection.africa.

protection to enabling trade. African states are increasingly recognising the need to enact data protection laws and the focus should now shift towards ensuring the content of these laws meaningfully enables fundamental rights as recognised in international human rights law and ensuring that laws and implemented and enforced.

*Surveillance*

Mass and targeted surveillance practices are on the rise, and there is a notable absence of international legal frameworks and strict safeguards in place. State-led surveillance is frequently implemented without underlying legal regulation and in a way that lacks transparency and accountability, initiatives which are a genuine affront to the right to privacy.

| **United Kingdom** | **South Africa** |
|---|---|
| The ECtHR has addressed the British government's powers to engage in surveillance, holding that the country's bulk surveillance programme was a violation of the right to privacy and the right to freedom of expression under the European Convention on Human Rights due to a lack of independent oversight, an overly broad application of surveillance, and a failure to sufficiently protect journalists' confidential communication.[31] | In South Africa, the Constitutional Court in 2021 declared various provisions of the domestic surveillance law to be unconstitutional as a result of a complaint brought by an investigative journalist whose communications had been monitored by intelligence officials; the Court ordered a range of amendments to improve transparency, safeguards, and oversight mechanisms state surveillance operations.[32] |

These two developments indicate that the issue of surveillance is a continued concern for digital rights, especially in the context of increased global digital reliance and data flows – but also that effective litigation and advocacy can result in important protections and safeguards. States may be obligated to put in place more robust legal frameworks and strict safeguards relating to surveillance in the future to avoid such challenges.

[31] Big Brother Watch v. The United Kingdom (Big Brother I) App nos. 58170/13, 62322/14 and 24960/15 (2018) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/).
[32] *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* ZACC 3 (2021) (accessible at: http://www.saflii.org/za/cases/ZACC/2021/3.html).

### Surveillance and press freedom

In recent years, the use of sophisticated surveillance technology on mobile phones has gained increasing prominence amidst concerns about its extensive abuse to monitor political opponents and activists. In 2021, news broke that at least 180 journalists had been targeted for surveillance by the Pegasus spyware, a system that can be remotely installed on a smartphone enabling complete control over the device.[33] The prevalence and seeming unrestricted usage of such technologies is deeply concerning for the right to freedom of expression, particularly considering its usage in many contexts in which the safety of journalists continues to be seriously at risk.

The Supreme Court of India in 2021 ordered an independent inquiry into allegations that the government deployed the Pegasus spyware against various journalists, politicians and dissidents, and found that the free press's democratic function was at stake, and that "such chilling effect on the freedom of speech is an assault on the vital public watchdog role of the press, which may undermine the ability of the press to provide accurate and reliable information."[34]

The use of video surveillance and closed-circuit television (**CCTV**) is also a common surveillance occurrence across the world, including in combination with facial recognition technology (**FRT**). State and non-state actors frequently invoke security threats to justify the widespread use of video surveillance and FRT. This form of surveillance and monitoring is susceptible to an array of abuses. The American Civil Liberties Union has identified the following:

- Institutional abuse.
- Abuse for personal gain.
- Discretionary targeting.
- Voyeurism.
- Location monitoring.

Such surveillance is often unregulated or under-regulated and can have a chilling effect on public life, and risks being abused to monitor critics or activists, to target marginalised groups, and to collect excessive data, often without consent. The quality and sophistication of video surveillance are also becoming more salient, with concerns, for example, that data from video surveillance systems can be combined with other forms of private and public information to create incredibly detailed profiles of people. Conversely, while such surveillance systems are often invasive, the potential inaccuracy and fallibility of the technology is also a concern, with a growing body of evidence that FRT systematically misidentifies certain populations and is vulnerable to racial bias.

[33] Forbidden Stories, 'Journalists Under Surveillance,' (2021) (accessible at: https://forbiddenstories.org/pegasus-journalists-under-surveillance/).
[34] Accessible at: https://main.sci.gov.in/supremecourt/2021/16884/16884_2021_1_1501_30827_Judgement_27-Oct-2021.pdf.

European Digital Rights (**EDRi**) explains that facial recognition technology is a type of biometric identification that "uses statistical analysis and algorithmic predictions to automatically measure and identify people's faces to make an assessment or decision." EDRi, however, notes that facial recognition technology is criticised for reflecting social biases resulting in the racial profiling of individuals and the creation of assumptions regarding sexual orientation and gender identity.

The 2020 Report by Gemalto on the top seven trends recorded:

- Facial recognition technologies are increasingly used to identify and verify a person using their facial features by capturing, analysing, and comparing patterns based on the person's facial details.
- Facial recognition technologies are predominately used for security and law enforcement, health and marketing, and retail.

Forbes anticipates that facial recognition technology is here to stay, with expected industry growth of $7 billion (USD) in 2024 in the United States.[35] Facial recognition is increasingly being used for surveillance. Fortunately, a wave of activism has recently begun to raise awareness about the potential rights implications of these technologies, with some notable successes in both litigation and policy change.

**Legal challenge to FRT**

In August 2020, British civil liberties organisation Liberty brought a legal challenge against the use of facial recognition technology by police in South Wales. The Court of Appeal ruled that the use of facial recognition technology breaches privacy rights, data protection laws, and equality laws and that there were "fundamental deficiencies" in the legal framework governing its use.[36] In 2019, San Francisco became the first major city in the United States to ban government use of face surveillance technology, with various cities across the world following suit. On calling for such bans, activists frequently cite the discriminatory effects of such technology and its potential risks to privacy, freedom of expression, information security, and social justice.

*The collection of biometric data*

Biometric data collection entails the identification and authentication of a person based on unique biological characteristics. FRT is considered a form of biometric data that is specifically

[35] Forbes, 'The Major Concerns Around Facial Recognition Technology' (2019) (accessible at https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/#1698a3824fe3).
[36] Liberty, 'Liberty Wins Ground-Breaking Victory Against Facial Recognition Tech,' (2020) (accessible at: https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/).

widely used for surveillance purposes. According to the 2020 Review of biometrics by Gemalto, biometric technologies are most frequently used for the following:

- **Law enforcement and public security**: identifying criminals, suspects and victims.
- **Military**: identifying enemies and allies.
- **Border, travel, and migration control**: identifying travellers, passengers, and nationality.
- **Civil identification**: identifying citizens, residents and voters.
- **Healthcare and subsidies**: identifying patients, beneficiaries, and healthcare professionals.
- **Physical and logistical access**: identifying owners, users, employees and contractors.
- **Commercial applications**: identifying consumers and customers.

The use of biometric technology is proliferating at a rapid rate, causing significant concern with regard to human rights. States are often ill-equipped to deal with the security and data storage challenges that come with collecting and storing such sensitive personal information, and examples of biometrics being used either for nefarious purposes or to the exclusion of already-marginalised populations abound. There are also growing concerns that the frequent use of biometric technologies has become unduly intrusive, contributing to the bourgeoning network of surveillance technologies. Liberty has noted that:

> "Use of big data and new technologies is often viewed as a panacea for the challenges that modern-day law enforcement faces. Technologies such as mobile fingerprint scanners, facial recognition and mobile phone data extraction, used in conjunction with one another and police super-databases, risk changing the relationship between the individual and the state, creating a society in which anonymity is the exception, and pervasive surveillance is the norm."

As with most technologies, the positive potential is significant, but the potential for rights violations is often ignored or underestimated. The 2020 Report by Gemalto on biometric voter registration argues that value can be gained from biometric technology, particularly in ensuring the improvement of electoral processes, with some advocates arguing that biometrics can potentially:

- Improve voter registration and identification;
- Produce a credible electoral register; and
- Reduce electoral fraud.

**Biometrics and elections in Africa**

The 2012 and 2016 elections in Ghana relied on biometric technologies. Some voters found the experience easy and time-efficient; some said it encouraged them to vote, while others were frightened by the experience and did not vote as a result.[37]

The use of biometrics for voting is on the rise in Africa, particularly in elections contexts. Examples include Niger, Kenya, and Ghana, amongst others. A long list of other African countries has reportedly either implemented or is considering implementing biometric systems for elections. The Collaboration for International ICT Policy for East and Southern Africa (**CIPESA**) has documented the deployment of other national biometric technology-based programmes in 16 African countries in recent years.

Despite the potential to facilitate well-functioning free and fair elections, there are concerns around the use of biometrics in developing or transitioning economies, including high costs, limited data literacy, and ineffective data protection regimes, causing serious risks to privacy. There have also been examples of high levels of exclusion of certain populations and abuse by governments embracing the trend of rising digital authoritarianism.

*Anonymity and encryption*

The 2015 Report of the UNSR on FreeEx highlights that encryption and anonymity are meant to "provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks." In the 2018 Follow-up Report, the UNSR stated:

> "the challenges users face have increased substantially, while States often see personal digital security as antithetical to law enforcement, intelligence, and even goals of social or political control. As a result, competing trends and interests have led, on the one hand, to a surge in State restrictions on encryption and, on the other hand, increased attention to digital security by key sectors of the private Information and Communications Technology ("ICT") sector."

As society's reliance on digital technologies has increased, users have become increasingly aware of the value of encryption as a tool to protect private communications in the digital era. This is particularly true for users such as journalists, activists, and lawyers, for whom the protection of communications is not merely a personal but also a professional imperative. In parallel with the rise in digital surveillance and cybercrimes discussed above, encryption has become a protective tool for the average internet user rather than something specialised, technical, and out of reach, as it was a few years ago. The United Nations Special Rapporteur on Freedom of Expression has highlighted that "encryption and anonymity enable individuals

[37] Adams and Asant, 'Biometric Election Technology, Voter Experience and Turnout in Ghana' Journal of African Elections (2019) (accessible at https://www.eisa.org.za/pdf/JAE18.1Adams.pdf).

to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection."[38]

Simultaneously, the rise of social media as a powerful platform for communication has enabled greater anonymity. States, particularly law enforcement agencies, have begun to push back against this growing use of encryption and anonymity, ostensibly in the interest of safety and security.

### The pros and cons of anonymity

While threats to encryption are frequently seen to be mere fronts to authoritarian attempts to control the flow of information and disproportionate efforts to crack down on crime, online anonymity has also drawn contested debates about the need to ensure accountability for online harms while protecting freedom of expression in digital spaces. For example, social media users in LGBTQIA+ communities have cited the importance of online anonymity to facilitating safe discussions about sexuality in environments where such discussions might put them at risk.

Rules on social media passed in India in 2020 reportedly require large social media companies to reveal users' identities if requested to do so by the Indian government, potentially stripping 400 million social media users of anonymity. CIPESA has reported that state agencies in several African countries can request for decryption of data held by service providers, potentially undermining the very essence of encryption services.

As challenges to privacy rise, so will the need to secure anonymity and promote reliance on encryption technologies. These technologies will continue to develop and become more sophisticated, but as they do, the threat of increased state intrusions in the private lives of citizens and attempts to weaponise and abuse such technologies are also likely to increase.

### Recent case law from the EctHR on anonymity

In 2021, the ECtHR ruled in the case of *Standard Verlagsgesellschaft mbH v Austria (no. 3)* that the Supreme Court of Austria's ruling requiring that a media company disclose the identities of registered users that had made comments on its site was a violation of its freedom of expression, because it had failed to take into account the political nature of the comments and to run a test balancing the competing interests.[39]

[38] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2015) (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement).
[39] Standard Verlagsgesellschaft mbH v. Austria (no. 3) Case No. 39378/15 (2021) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/standard-verlagsgesellschaft-mbh-v-austria-no-3/).

## The Right to Freedom of Expression

Recent trends indicate that the most significant threat to freedom of expression is the criminalisation of online speech. Criminalisation is effected through the enactment of laws which are generally vague and broad and give governments a wide range of powers to declare certain forms of online expression as offences. In recent years, legislation relating to cybercrime, social media, and disinformation (or "fake news") have become increasingly popular tools through which to do so. Journalists and political dissidents and critics are particularly susceptible to these challenges and examples abound, particularly in Africa, of journalists being silenced, detained, and convicted on such laws. In Nigeria, for example, civil society has condemned the abuse of the 2015 Cybercrimes (Prohibition, Prevention, Etc) Act to harass journalists and other citizens. In Zimbabwe, journalists have been charged under various new "false news" provisions recently introduced into law.

*Efforts to address disinformation*

The Independent High-level Group on Fake News and Online Disinformation recorded that the spreading of false, inaccurate, or misleading information that is designed to intentionally cause harm or generate profit continues to be one of the most significant threats to freedom of expression. The World Economic Forum noted that in 2013 the terms "fake news" and "post-truth" began gaining traction. However, with Brexit and the election of Donald Trump, the "prevalence and impact of digital wildfires have surged", with some instances of fake news stories outperforming legitimate stories from primary news sources. The COVID-19 pandemic from 2020 onwards added fuel to the fire with the rapid and widespread proliferation of false information relating to the spread of the virus, treatments, and vaccines.

Disinformation continues to poison the digital sphere creating serious risks for freedom of expression as states tighten controls. In 2021 Freedom House reported that global internet freedom declined for the 11th consecutive year and in 2020 that "in many places, it was state officials and their zealous supporters who actually disseminated false and misleading information with the aim of drowning out accurate content, distracting the public from ineffective policy responses, and scapegoating certain ethnic and religious communities." The Disinformation Tracker, a collaborative civil society initiative, has documented the various responses taken by African states to the COVID-19 pandemic, including many laws criminalising false publications.

Even prior to the pandemic, the criminalisation of false news was popular around the world:

- Towards the end of 2019, the Protection from Internet Falsehood and Manipulation Bill 2019 was tabled in Nigeria. The Bill seeks to prohibit a long list of statements including false statements of fact and statements that are likely to be prejudicial to the country's security, public health, public safety, public tranquillity, or finances. Statements that prejudice Nigeria's relations with other countries, influence the outcome of an election or referendum, incite feelings of enmity, hatred towards a person, or ill will between a

group of persons would also be monitored, and those who utter such statements would be liable to fines and, possibly, imprisonment.[40]

- Ethiopia has recently criminalised disinformation with the adoption of a new law that seeks to increase jail sentences and fines for hate speech and the dissemination of disinformation.[41]
- The Protection from Online Falsehoods and Manipulation Act (**POFMA**), enacted in Singapore in 2019, seeks to prevent the communication of false information and to suppress support for and counteract the effects of such information. POFMA further seeks to enable measures to detect, control and safeguard against coordinated inauthentic behaviour. POFMA prohibits a person who communicates a statement that is a false statement of fact, and that is likely to be (i) prejudicial to the security of Singapore; (ii) prejudicial to public health, public safety, public tranquillity or public finances; (iii) prejudicial to the friendly relations of Singapore with other countries; (iv) influence the outcome of an election; (v) incite feelings of enmity, hatred or ill-will between different groups of persons; or (vi) diminish public confidence in government. A person who contravenes these provisions is guilty of an offence and liable on conviction to a fine or imprisonment.[42]

Despite the alarming and current rise of disinformation and the often disproportionate responses from state actors that threaten freedom of expression online, there is some comfort in knowing that there are organisations, institutions and states making a concerted and decisive effort to address this unfortunate and harmful trend.

[40] Al Jazeera 'Nigerians raise alarm over controversial Social Media Bill' (2019) (accessible at https://www.aljazeera.com/news/2019/12/nigerians-raise-alarm-controversial-social-media-bill-191218130631539.html).
[41] Al Jazeera, 'Ethiopia passes controversial law curbing 'hate speech' (2020) (accessible at https://www.aljazeera.com/news/2020/02/ethiopia-passes-controversial-law-curbing-hate-speech-200213132808083.html).
[42] Protection from Online Falsehoods and Manipulation Act, 2019 (accessible at https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625).

**Positive resources and examples for overcoming disinformation challenges**

- UNESCO developed a "Journalism, fake news & disinformation: handbook for journalism education and training".
- The European Union has published its "Code of Practice on Disinformation".
- InterAction released a toolkit to assist people with preparing for online disinformation threats.
- In Finland, schools and community colleges are introducing lessons on disinformation to inform people at a young age about disinformation and how to guard against it.
- Viral Facts Africa was launched by the World Health Organisation (**WHO**) together with a network of fourteen fact-checking organisations and public health bodies to undertake health fact checks, explainers, myth busters and misinformation literacy messages optimised for sharing on Facebook, Twitter and Instagram, aiming to rapidly debunk myths where they occur and provide viral, credible information on the COVID-19 pandemic.

**African courts engaging with issues regarding false news**

The East African Court of Justice in *Media Council of Tanzania and Others v Attorney-General of the United Republic of Tanzania* and the Court of Justice of the Economic Community of West African States in *Federation of African Journalists and Others v The Republic of The Gambia* have ruled in favour of upholding the fundamental right to freedom of expression and have called for the repeal of vague and broad provisions that seek to stifle freedom of expression.

There is a corresponding trend that is seeking to overcome disinformation threats through education, media literacy, awareness, and dialogue. Despite negative forecasts, the rise of digital activism looks to play a critical and positive role in rerouting the current trajectory.

*Efforts to address hate speech*

The 2019 UN Strategy and Plan of Action on Hate Speech advises:

> "Around the world, we are seeing a disturbing groundswell of xenophobia, racism and intolerance – including rising anti-Semitism, anti-Muslim hatred and persecution of Christians. Social media and other forms of communication are being exploited as platforms for bigotry. Neo-Nazi and white supremacy movements are on the march. Public discourse is being weaponised for political gain with incendiary rhetoric that stigmatises and dehumanises minorities, migrants, refugees, women and any so-called 'other'."

There is undoubtedly a need to counteract the above groundswell. However, states are quickly turning to criminalisation to address this, rather than addressing the systemic issues of perceptions, ignorance, privilege, and inequality. Hate speech is a vague term that lacks universal understanding, and legal provisions are often open to abuse and restrictions on a wide range of lawful expression.

A range of legislative developments are in motion across Africa, such as:

- South Africa's Parliament is considering the Prevention of Combating of Hate Crimes and Hate Speech Bill which aims to create new legal definitions and procedures to combat hate crimes and hate speech
- In Kenya, the 2008 National Cohesion and Integration Act (NCIC) seeks to foster national cohesion and integration by outlawing discrimination and hate speech on ethnic grounds. The proposed Prohibition of Hate Speech Bill in Nigeria is another relevant example.

However, international law standards and guidance are increasingly encouraging states to move away from sanctions and prohibitions towards more positive measures. ARTICLE 19 emphasises that states should engage with the symptomatic causes of hate speech rather than adopting a singularly punitive approach. The 2019 UN Strategy and Plan of Action on Hate Speech seeks to focus on the root causes and drivers of hate speech and to ensure effective responses that do not criminalise freedom of expression that should be protected. The plan lists a variety of commitments, including:

- Monitoring and analysing hate speech.
- Engaging and supporting the victims of hate speech.
- Convening relevant actors.
- Engaging with new and traditional media.
- Using education as a tool for addressing and countering hate speech.
- Fostering peaceful, inclusive and just societies to address the root causes and drivers of hate speech.
- Developing guidance for external communications.

Continued disinformation and the promotion of hateful speech should be anticipated as our reliance on online spaces continues to increase and political polarisation continues to be amplified by automated online systems. However, there are parallel pushes to engage more meaningful and substantively with hate speech and find ways that address hate speech without limiting freedom of expression.

*Harassment of journalists, bloggers, and other professionals*

In 2022, the UN reported that threats to media workers' freedoms are growing by the day, with journalists facing "increasing politicisation" of their work and threats to their freedom to simply do their jobs. In particular, the COVID-19 pandemic and coverage of climate change, biodiversity and pollution have attracted threats and efforts to silence journalistic outputs. The UN Secretary-General noted that journalists are threatened "by the weapons of falsification and disinformation" and that digital technology is making censorship easier for authoritarian governments and others seeking to suppress the truth. Women journalists are particularly at risk of online violence and harassment, with the UN Educational, Scientific and Cultural Organization (**UNESCO**) reporting that nearly three-quarters of women journalists having experienced online violence, and 30% having responded to online violence by self-censoring on social media.

Journalists fulfil an important role in any society but are too often at risk, threatening their ability to fulfil their critical function as the fourth estate. Comprehensive statistics illustrate the challenges faced by journalists:

- Reporters Without Borders found that 68% of journalists in Pakistan have reported being harassed online.
- The Committee to Protect Journalists found that in the United States, 90% of journalists believe that online harassment is the biggest threat to their profession.
- A global survey conducted by the International Centre for Journalists and the Tow Center for Digital Journalism shows that 20% of respondents describe their experience of online abuse as "much worse than usual" during the COVID-19 pandemic.

A 2017 Reporters without Borders study by the Council of Europe indicated that:

- 31% of journalists water down their coverage of stories after being harassed.
- 15% of journalists drop the story.
- 23% of journalists don't cover specific stories.
- 57% of journalists do not report that they have been the targets of online violence.

UNESCO has also found that in addition to large-scale attacks or extreme threats, the "slow burn" of lower but nearly constant levels of abuse also has insidious effects, causing PTSD, depression, and anxiety to drive journalists out of the newsroom. Black, Indigenous, Jewish, Arab, and lesbian women journalists participating in the UNESCO survey experienced both the highest rates and most severe impacts of online violence.

The harassment of journalists is a global issue and remains deeply entrenched. UN bodies are calling for protection, and civil society actors are assisting where they can. Still, there needs to be a far more concrete and legitimate effort, particularly by states, to ensure the safeguarding of journalists.

With the growing reach and influence of social media, new methods of harassing journalists are also becoming prominent. This includes, for example, cyber-harassment, online gender-based violence, and the use of Strategic Litigation Against Public Participation (SLAPP) suits

to stifle and silence critics, leveraging either civil defamation or other legal strategies to bury critics in legal challenges. Efforts to counter these new online threats can rely on a robust body of case law holding that journalists must be protected and enabled to carry out their jobs safely. In the important case of *Brown v Economic Freedom Fighters* in South Africa, the High Court held that the failure of a political party to condemn its supporters' harassment of and threats against a journalist violated the South African Electoral Code.[43]

## Conclusion

Recent years have seen unprecedented online development, exposing emerging opportunities and threats. It is likely that the coming years will pose many of the same risks and opportunities, with new complexities related to the regulation of the online sphere arising that both enable and threaten freedom of expression and access to information.

In future, it is hoped that digital divides will decrease with improved access and increased efforts towards digital literacy. Threats to privacy are likely to magnify in quantity and intensity as the scale of datafication continues to increase. Freedom of expression will remain in a precarious position with misguided attempts to address legitimate concerns. There is a pressing need now, more than ever, to develop powerful advocacy strategies, establish impactful jurisprudence and to equip people with the necessary knowledge and skills to be empowered to advocate for their rights. New technologies are consistently emerging and giving rise to new opportunities and threats. Important steps are being taken every day by ordinary people, digital rights activists, the international community, courts, and some states to ensure that the internet remains a source of agency and development and that it becomes a safe space for all users to reach their full potential.

[43] South Gauteng High Court, *Brown v Economic Freedom Fighters* (2019) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/brown-v-economic-freedom-fighters/).

*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.<br><br>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.

*Module 3*

# Criminalisation of Online Speech

*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 3

## Criminalisation of Online Speech

**The objectives of this module are:**

- **To provide an overview of the criminalisation of online speech.**
- **To set out the applicable international human rights standards and fundamental international and regional legal principles.**
- **To understand the impact of criminalisation on freedom of expression and identify legitimate purposes for limiting freedom of expression.**
- **To set out and to examine the different forms of criminalisation, including hate speech, cybercrime and disinformation.**
- **To identify practical ways to deal with the competing interests of criminality and free speech.**

---

## Introduction

There has been a growing trend of criminalising online speech over recent years. Many states have attempted to justify this as a response to threats of hate speech, national security, the mushrooming of cybercrimes, and the proliferation of disinformation. In many instances, this has led to the stifling of free speech and access to information. While some of the online harms that prompt criminalisation are a genuine concern which may warrant responses from states, there is an urgent need to ensure that states do not use these to justify restricting speech or controlling content.

This module provides an overview of the criminalisation of online speech. It looks at the applicable legal framework that guides what is permissible in terms of restrictions on the right to freedom of expression, and the relevant considerations for balancing competing rights. This module will also touch on hate speech, cybercrimes, and disinformation.

## Overview of Criminalising Online Speech

Criminalisation, in the context of online speech, refers to the enactment of laws and policies that render specific forms of online expression illegal. Such criminalisation may be targeted at a range of harmful expressions, including:

- Hate speech;
- Threats or incitement to terrorism and violence;
- Disinformation;
- Defamation;

- Sexual abuse material including child sexual abuse material, the non-consensual dissemination of intimate images (**NCII**), and sexual exploitation online; and
- Cybercrimes.

From a criminal justice perspective, certain actions may warrant criminal consequences. However, in the context of online speech offences, there are a variety of competing considerations in the interplay between the offences, the rights they limit, and the limitations caused by creating the offences.

**Walking the tightrope: criminalising online speech**

The complexities of criminalising online speech should not be underestimated. The digital landscape, which in many ways has brought people together and facilitated free speech and dissent, has also created spaces that breed divisiveness, division, and exclusion. Supremacist ideologies, populist nationalism, gendered violence, and racism and xenophobia are some of the social ills that can take root in both our offline and online societies. Balancing dignity, equality, autonomy, and development against the right to free speech is not an easy task.

It is arguable that states' moves to impose restrictive measures on harmful speech, instead of addressing the systemic issues, such as the factors that enable the spread of misinformation online, are short-sighted solutions that restrict both those who are affected by online harms and those who are lawfully and legitimately expressing themselves. Organisations like the Collaboration on International ICT Policy in East and Southern Africa (**CIPESA**) and the Council of Foreign Relations (**CFR**) have noted with concern that governments the world over are adopting legislation that curtails free expression rights on the internet, either through the criminalisation of specific actions or through laws aimed at combating criminal activity online.

The right to freedom of expression is a fundamental human right that is protected in the Universal Declaration of Human Rights (**UDHR**), the International Covenant on Civil and Political Rights (**ICCPR**), and the African Charter on Human and People's Rights (**African Charter**). It is a right that is necessary for good governance and economic and social progress because it enables accountability by allowing people to freely debate and raise concerns with the government, including the protection and promotion of other human rights.[1]

Understanding the role of online speech offences, and their intended and unintended consequences requires careful navigation. Many laws that criminalise online speech are seen to be vague and overbroad and often fail to strike the appropriate balance between competing rights. These laws result in a chilling effect on the right to freedom of expression, whereby individuals steer clear of controversial topics because there is uncertainty about what is

[1] ARTICLE 19, 'Hate Speech' Explained: Toolkit (2015) (accessible at: https://www.article19.org/resources/hate-speech-explained-a-toolkit/).

permitted and what is not.[2] The chilling effect may be exacerbated where penalties for breach of the law are unduly harsh, as is the case with certain laws that criminalise online speech.

## Applicable International Human Rights Standards

*Overview of the right to freedom of expression and associated rights*

It is trite that the right to freedom of expression is deeply entrenched as a fundamental human right and given protection through various international and regional instruments. Article 19 of the UDHR states:

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

Article 19 of the ICCPR gives further effect to this, and article 20 of the ICCPR provides for certain restrictions on speech:

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

In 2011, the United Nations Human Rights Committee published General Comment 34, which provides valuable guidance on how the right to freedom of expression should be interpreted. It states that freedom of expression is the "foundation stone for every free and democratic society", and that it is a "necessary condition for the realisation of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights." General Comment 34 notes that the right to freedom of expression includes:

- Political discourse.
- Commentary on one's own affairs and on public affairs.
- Canvassing ideas.
- Discussing human rights.
- Journalism.
- Cultural and artistic expression.
- Teaching, and religious discourse.

Freedom of expression may even extend to speech that may be regarded as deeply offensive by some people. The right applies both to verbal and non-verbal communications as well as all modes of expression, including audio-visual, electronic, and internet-based communication.

[2] Centre for Law and Democracy 'Restriction on freedom of expression' (accessible at: http://www.law-democracy.org/live/wp-content/uploads/2015/02/foe-briefingnotes-2.pdf)

### Freedom of expression as an enabling right

- The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (**UNSR on FreeEx**) in a 2011 Report noted that the "right to freedom of opinion and expression is as much a fundamental right on its own accord as it is an 'enabler' of other rights". The UNSR went on to recognise that the right to freedom of expression also impacts economic, social, and cultural rights, such as the right to education and the right to take part in cultural life and to enjoy the benefits of scientific progress and its applications.

- General Comment 34 acknowledged that freedom of expression embraces the right of access to information, plays an important role in the conduct of public affairs, contributes to the effective exercise of the right to vote, and is integral to the enjoyment of the rights to freedom of assembly and association.

The 2017 Report of the UNSR on FreeEx sets out states' obligations under article 19 of the ICCPR. States may not interfere with, or in any way restrict, the holding of opinions, unless there are instances that warrant restriction – which must be provided by law and necessary for the respect of the rights or reputations of others, or for the protection of national security or public order, or public health or morals. States are also under an obligation to take steps to protect individuals from undue interference with human rights when committed by private actors, including taking appropriate steps to prevent, investigate, punish, and redress private actors' abuse. Such steps include the adoption and implementation of legislative, judicial, administrative, educative, and other appropriate measures that require or enable businesses to respect freedom of expression, and, where private sector abuses occur, access to an effective remedy.

In the African context, article 9 of the African Charter provides that:

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

### African regional case law: limiting freedom of expression

- In *Constitutional Rights Project v Nigeria*, the African Commission on Human and People's Rights (**ACHPR**) held that the "only legitimate reasons for limitations of the rights and freedoms of the African Charter are found in Article 27(2), that is, that the rights "shall be exercised with due regard to the rights of others, collective security, morality and common interest". The ACHPR went on to state that the "justification of limitations must be strictly proportionate with and absolutely necessary for the advantages which follow. Most important, a limitation may not erode a right such that the right itself becomes illusory."

- The African Court on Human and People's Rights (**African Court**) in *Konaté v Burkina Faso* held that criminal sanctions for defamation must be necessary and proportionate, failing which they are incompatible with the ACHPR and other human rights instruments. Accordingly, expression must be within the prescripts of the law, and may only be limited in terms of article 27(2) of the African Charter, bearing in mind what is proportionate and necessary.

In 2002, the Declaration of Principles on Freedom of Expression in Africa was adopted to supplement article 9 of the African Charter. Article 2 of the Declaration of Principles established that arbitrary interference with a person's freedom of expression is prohibited and that any restrictions on freedom of expression shall be provided by law, serve a legitimate interest and be necessary in a democratic society. The revised 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa further provide that:

> "States shall criminalise prohibited speech as a last resort and only for the most severe cases. In determining the threshold of severity that may warrant criminal sanctions, States shall take into account the:
>
> a. prevailing social and political context;
> b. status of the speaker in relation to the audience;
> c. existence of a clear intent to incite;
> d. content and form of the speech;
> e. extent of the speech, including its public nature, size of audience
> f. and means of dissemination;
> g. real likelihood and imminence of harm."

It goes on to further state that States should not prohibit speech that merely lacks civility, or which offends or disturbs.[3]

*Other implicated rights*

In the context of online criminalisation, it is important to note that there are other interests and rights involved alongside the right to freedom of expression. These are different to the rights that are enabled through freedom of expression. The divergence of varying rights has been aptly captured in a 2019 Report on the UNSR on FreeEx:

> "[F]reedom of expression is a legal right of paramount value for democratic societies, interdependent with and supportive of other rights throughout the corpus of human rights law. At the same time, anti-discrimination, equality and equal and effective public participation underpin the entire corpus of human rights law. The kind of expression captured in article 20 of the International Covenant on Civil and Political Rights and article 4 of the International Convention on the Elimination of

[3] Principle 23 (3).

> All Forms of Racial Discrimination presents challenges to both sets of norms, something that all participants in public life must acknowledge."

Equality and non-discrimination are among the rights sometimes at odds with freedom of expression. While these rights can be exercised harmoniously, tensions are not uncommon. Beyond equality and non-discrimination, when considering freedom of expression and the criminalisation of online speech, regard should be had to other rights, including the rights of children. In some instances, protection measures online for children have at times taken a back seat to freedom of expression. In contrast, at other times, there have been constraints on children's or others' digital expression due to the need to combat online violence and exploitation. A 2017 UNICEF Report on Children's Rights and Business in a Digital World: Freedom of Expression, Association, Access to Information and Participation explains that what is ultimately required is some form of balancing between children's rights to freedom of expression and access to information and their right to be protected from violence.

There are other instances where there is also a need for balance:

- Balancing the right to freedom of expression with the right to privacy when determining whether to publish content.
- Striking a balance between the right to freedom of expression and the right to reputation.

It is necessary to note that rights are not absolute and may be subject to certain limitations and restrictions in order to balance competing rights and interests.[4] Ultimately, the right to freedom of expression is not unbounded and can be restricted to protect other rights, just as other rights may be subject to certain limitations and restrictions in order to advance freedom of expression. The restrictions of the right to freedom of expression will be dealt with further in the following section.

## Restricting Freedom of Speech Online

As a result of the dramatic changes in the spread of information occasioned by the internet, there has been a proliferation of attempts to address issues relating to terrorism and national security, cybercrimes, and the spreading of disinformation online. Many of these attempts are, to varying degrees, in conflict with the right to freedom of expression.[5] Although the right to freedom of expression is a fundamental human right, it is not absolute. As with most rights, freedom of expression may be lawfully restricted where the restrictions are reasonable and justifiable in an open and democratic society. However, as confirmed in General Comment 34, the restrictions imposed by states should not put the right to freedom of expression in jeopardy.

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

[4] Media Defence, 'Training Manual on Digital Rights and Freedom of Expression Online Litigating digital rights and online freedom of expression in East, West and Southern Africa' at (accessible at https://www.mediadefence.org/resources/mldi-training-manual-digital-rights-and-freedom-expression-online).

[5] Shepard, 'Extremism, Free Speech and the Rule of Law: Evaluating the Compliance of Legislation Restricting Extremist Expressions with Article 19 ICCPR' Utrecht Journal of International and European Law (2017) (accessible at https://www.utrechtjournal.org/articles/10.5334/ujiel.405/).

- Provided by law.
- Necessary for respect for the rights of others, and for the protection of national security or of public order, or of public health or morals.

To determine whether a limitation of the right to freedom of expression is justifiable, a three-stage test must be applied in which it must be established that the limitation is:

- Provided by law.
- Pursues a legitimate aim.
- Necessary for a legitimate purpose.[6]

It is important to note that articles 19(3) and 20 of the ICCPR are compatible, and the prohibited grounds listed in article 20 can also be restricted in terms of article 19(3) and must also pass the three-stage test. It is further necessary to note that within the context of article 20, there is a need to recognise the distinction between protected and unprotected speech, and between what is prohibited and what is discriminatory, derogatory and demeaning discourse. Article 4(a) of the International Convention on the Elimination of All Forms of Racial Discrimination (**ICERD**) provides that certain forms of expression are prohibited and punishable by law. These include:

- Dissemination of ideas based on racial superiority or hatred.
- Incitement to racial discrimination.
- Acts or incitement of violence against any race or group of persons of another colour or ethnic origin of racially motivated violence.
- The provision of assistance, including of a financial nature, to racist activities.

### Three-stage test for the justifiable criminalisation of online speech

The **first limb** (that the restriction is provided for by law) is relatively straightforward in relation to the criminalisation of online speech. The legislation must be clear, accessible, apply equally to everyone and be consistent with international human rights norms. Despite this, governments continue to enact laws that are vague, and which give themselves wide-ranging powers, including the power to decide what constitutes a legitimate purpose to restrict freedom of expression. On counter-terrorism measures, General Comment 34 provides that any offences relating to the encouragement of terrorism or extremist activity, or to the praising, glorifying, or justifying of terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interferences with freedom of expression. Excessive restrictions on access to information must also be avoided.

The **second limb** (that it pursues a legitimate aim) is more complicated and is important for the broader discussion on the criminalisation of online speech. In the current digital

[6] For a detailed outline of the limitation of freedom of expression see Module 2 on Restricting Access and Content at 4-5.

and political climate, the criminalisation of online speech is commonly used for political or other illegitimate purposes. Although there are legitimate grounds to restrict freedom of expression on the basis of national security, it is frequently subject to abuse.

The **third limb** requires an assessment of whether the restriction is necessary, where legislation provides for restricting freedom of expression for the legitimate purposes of protecting national security, countering terrorism, ensuring public order, or respecting the rights of others. In respect of necessity and proportionality, a 2019 Report of the UNSR on FreeEx notes that "restrictions must be demonstrated by the state as necessary to protect a legitimate interest and to be the least restrictive means to achieve the purported aim." A 2018 UNESCO report on world trends in freedom of expression and media development explains that this leg of the test can also cause controversy, when national security concerns are cited by states "to enact measures that present a clear challenge to media freedom, raising issues of necessity and proportionality." States are often quick to justify restrictions without fully considering the principle of necessity and whether less restrictive means are available. With new online threats, states are also becoming more restrictive, often in violation of the above test.

The different legitimate aims and the potential concerns that arise are discussed below.

*National security*

UNESCO has observed the growing trend of citing national security concerns as a justification for restricting freedom of expression. A legitimate national security interest is one that aims "to protect the existence of the nation or its territorial integrity or political independence against force or threat of force." This definition was laid out in the 1985 Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights. The Siracusa Principles further provide that a national security limitation:

> "cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order" and "cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exists adequate safeguards and effective remedies against abuse."

The Johannesburg Principles on National Security, Freedom of Expression and Access to Information were drawn up in 1996 by a group of experts in international law, national security, and human rights. The principles state that in order for expression to be punished as a threat to national security, a government must show that:

- The expression is intended to incite imminent violence.
- It is likely to incite such violence.
- There is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

The Johannesburg Principles further provide that punishment (for disclosure of information) based on national security grounds is prohibited if the disclosure does not actually cause harm and is not likely to harm a legitimate national security interest.

The 2019 Declaration of the ACHPR further provides that "[f]reedom of expression shall not be restricted on public order or national security grounds unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression."

Issues of national security have caused complications for the advancement of free expression for decades, including in the offline domain, as illustrated by the case note below.

**Case note: Başkaya and Okçuoğlu v Turkey**

In 1991, Mr Başkaya wrote a book which was published by Mr Okçuoğlu. Both Mr Başkaya and Mr Okçuoğlu are Turkish citizens. The book detailed the socio-economic revolution of Turkey and was critical of the ideology adopted by the state. The book came to the attention of the Turkish prosecution authorities, and Mr Başkaya was subsequently charged with disseminating propaganda against the indivisibility of the state. Mr Okçuoğlu was charged as the owner of the publishing company.

The National Security Court acquitted both men in 1992. However, the prosecutor subsequently successfully appealed the decision, which led to the matter being referred back to the trial court, which subsequently found both men guilty of the offences with which they had been charged. They were both sentenced to imprisonment and a fine. This decision was unsuccessfully appealed to the Court of Cassation, leading Mr Başkaya and Mr Okçuoğlu to approach the European Court of Human Rights (**ECtHR**).

Before the ECtHR, they argued, among other things, that their right to freedom of expression had been violated. The respondent state argued that the measures taken against the men were based on a law that was aimed at protecting interests such as territorial integrity, national unity, national security and the prevention of disorder and crime. The state further argued that they were convicted in pursuance of these legitimate aims since they had disseminated separatist propaganda vindicating the acts of the PKK (Workers' Party of Kurdistan), a terrorist organisation, which threatened these interests.

In 1999, the ECtHR delivered its decision, noting that freedom of expression is one of the "essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment", but may be subject to certain restrictions. The ECtHR emphasised that exceptions to freedom of expression must be construed strictly, and the need for any restrictions must be established convincingly. In conducting its limitations analysis, the ECtHR made the following observations:

- The requirement of "**necessary**" implies the existence of a "**pressing social need**".

- The content of the impugned statements and the context in which they were issued must be considered when determining if the interference was "**proportionate to the legitimate aims pursued**".
- Restrictions operate on a spectrum. There is little scope for restrictions on political speech or on debate on matters of public interest. However, there is a wider margin of appreciation when examining the need for an interference with freedom of expression in the context of remarks that incite violence.

The ECtHR, with due regard to Turkey's context, found that the measures taken by the state were in furtherance of the legitimate aim to ensure national security. However, the conviction and sentencing of Mr Başkaya and Mr Okçuoğlu was disproportionate to the aims pursued and therefore not "necessary in a democratic society". The ECtHR accordingly found that the right to freedom of expression had been violated.

National security can indeed be a legitimate aim; however, a restriction on freedom of expression must pass the other legs of the test as well, and cannot be justified on the legitimacy of national security grounds alone.

**Case note: Good v Republic of Botswana**

Mr Good, a political studies professor at the University of Botswana, was declared an undesirable inhabitant following the publication of a co-authored article which was critical of Botswana's presidential succession. Mr Good was deported without reason and was not provided with an opportunity to challenge the decision. After unsuccessfully exhausting all internal remedies, Mr Good approached the ACHPR, where he alleged that his right to be heard, his right to freedom of expression, his right to freedom of movement and his right to family life, all contained in the African Charter, had been violated.

In response to the allegation regarding the restriction of Mr Good's right to freedom of movement, the respondent state relied on national security as a justification, arguing that the ACHPR does not have competency over such issues as "[s]tates must be left alone and allowed to deal with matters of peace and national security". The respondent state did not address the alleged restriction on freedom of expression, and Mr Good argued that the respondent state failed to illustrate the nature of the so-called national security threat posed and why the deportation could be justified as proportionate in severity and intensity to the publication of the academic paper.

Despite the lack of a full response from the respondent state, the ACHPR analysed the alleged infringement and found that there is international consensus on the need to restrict freedom of expression for national security, but such a restriction must be **necessary**, serve a **legitimate interest** and be **provided for by law**. The ACHPR went on to note that notwithstanding the fact that "in the African Charter the grounds of limitation to freedom of expression are not expressly provided as in the other international and regional human rights treaties, the phrase 'within the law' under Article 9(2) provides a leeway to cautiously

fit in legitimate and justifiable individual, collective and national interests as grounds of limitation."

When conducting the limitations analysis, the ACHPR emphasised that a "higher degree of tolerance is expected when it is a political speech and an even higher threshold is required when it is directed towards the government and government officials." The ACHPR found that there was nothing in the article co-authored by Mr Good that could potentially create instability, unrest, or violence in the country; rather, it was merely the expression of opinions and views and did not amount to defamatory, disparaging, or inflammatory expression.

Ultimately, the ACHPR found that:

> "The action of the [r]espondent [s]tate was unnecessary, disproportionate and incompatible with the practices of democratic societies, international human rights norms and the African Charter in particular. The expulsion of a non-national legally resident in a country, for simply expressing their views, especially within the course of their profession, is a flagrant violation of [a]rticle 9(2) of the Charter."

**Case note: SERAP v the Federal Republic of Nigeria**

This case in the Community Court of Justice of the Economic Community of West African States (**ECOWAS**) also bears mention dealt with the Nigerian government's response to Twitter's removal of content tweeted by the President from its platform for violation of its rules.[7] Nigeria suspended the operations of Twitter arguing that its ongoing operations constituted threats to the stability of Nigeria and that "Twitter is undermining Nigeria's corporate existence" by allowing content that referred to separatist politics.

The ECOWAS Court emphasised the role of social media platforms such as Twitter as enablers of the rights to freedom of expression and access to information and held that the suspension was not made under any law or order of a court and that the government's mere reference or allusion to national security threats posed by protests in the country and their supposed potential to destabilise Nigeria did not constitute legal justification for the infringement on the right to freedom of expression.

As evinced in these cases, there are times when states will rely on national security when it is in fact not a legitimate aim. In such instances, courts should be quick to find the distinction between legitimate threats and critical expression.

[7] Media Defence and Mojirayo Ogunlana-Nkanga represented the applicants in this case.

*Counter-terrorism*

Terrorism and extremism, which are largely undefined and often misused terms, are frequently the basis for states to invoke restrictive measures on freedom of expression online in the name of national security. International human rights law provides extensive guidance for states on how to balance the real need to respond to terrorism, with the fundamental right to freedom of expression.

The 2015 Joint Declaration on Freedom of Expression and Responses to Conflict Situations by Special Rapporteurs on Freedom of Expression provides that:

> "States should refrain from applying restrictions relating to 'terrorism' in an unduly broad manner. Criminal responsibility for expression relating to terrorism should be limited to those who incite others to terrorism; vague concepts such as glorifying', 'justifying' or 'encouraging' terrorism should not be used."

The 2016 Joint Declaration on Freedom of Expression and Countering Violent Extremism notes that:

> "Everyone has the right to seek, receive and impart information and ideas of all kinds, especially on matters of public concern, including issues relating to violence and terrorism, as well as to comment on and criticise the manner in which [s]tates and politicians respond to these phenomena."

The 2016 Joint Declaration further provides that states are obliged to ensure that there is an enabling environment for the media to keep society informed, "particularly in times of heightened social or political tensions". This point is also emphasised in General Comment No. 34 on the ICCPR, which states that the media plays an important role in informing the public about acts of terrorism and that it should be able to perform its legitimate functions and duties in this regard without hindrance.[8]

At a minimum, if there is to be a limitation of access to the internet or to content online on the grounds of anti-terrorism, 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.

There is also a general presumption in international law that prior restraint – restricting access to content before it has been published – is unnecessary and disproportionate. Although there may be a strong argument for the need to step in to stop the dissemination of information prior to publication of content relating to terrorism, the courts have stressed that prior restraint can only be allowed in exceptional circumstances and must be robustly justified.[9]

[8] UN Human Rights Council, 'General Comment no. 34 at para 46 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).
[9] For example, see *New York Times Co. v United States (1971)* and *Amnesty International Togo and Ors v. The Togolese Republic.*

*Public order offences*

Public order offences can be developed and implemented to provide for legitimate aims, especially in the context of security forces. This means that laws which allow security forces to limit free speech to protect public order may be legitimate, as long as they comply with the requirements listed above. This legitimate aim is one that should not be abused due to the significant impact it can have on the people affected by the restriction on freedom of speech. This is particularly evident in the recent proliferation of internet shutdowns during crucial election periods. These acts are usually commissioned under the guise of maintaining public order, whereas they constitute an effort by states to silence dissent. The consequences of internet shutdowns are that the public's right to access information, which may be crucial at a particular time, is violated.[10] For more on internet shutdowns, see Advanced Module 2 of this series on Restricting Access and Content.

**UNESCO Training Modules on Public Order and Freedom of Expression**

In response to tensions between the maintenance of public order and the restrictions on freedom of expression, particularly in the context of journalism, UNESCO has developed training modules to empower both security forces and journalists to understand the law and their respective roles and responsibilities.

- The 2015 Freedom of Expression and Public Order Training Manual provides legal references and tools for security forces to promote transparency, facilitate and improve relations between security forces and the media, and encourage respect for the safety of journalists in the field.

- The 2018 report from UNESCO Freedom of Expression and Public Order: Fostering the Relationship between Security Forces and Journalists seeks to facilitate the relationship between security forces and journalists in order to establish an enabling environment for journalists. This training manual aims to empower journalists and citizens in order for them to exercise their rights to freedom of expression and access to information. It focuses on the importance of transparent law enforcement institutions, which respect freedom of expression and the right to information and promote accountability and the rule of law while respecting human rights.

- In 2022, UNESCO, together with the International Police Association and IBZ Gimborn Castle launched a joint Massive Open Online Course (**MOOC**) for members of law enforcement and police officers to raise awareness of international and regional standards on freedom of expression, access to information, and safety of journalists.

[10] For more on internet shutdowns see Module 2 on Restricting Access and Content.

## Forms of Criminalisation

In 2019, the ACHPR recognised that the primary issues relating to freedom of expression include:

- Co-regulation of the media.
- Safety of journalists.
- Restrictions related to cyber-crime laws.
- Regulation of the internet.

While there is an array of actions and forms of speech that have attracted criminal sanctions, this section focuses on hate speech, cybercrimes, and disinformation.[11]

*Hate speech*

### The reconciliation of values

A 2019 Report by the UNSR on FreeEx found that:

> "Under international human rights law, the limitation of hate speech seems to demand a reconciliation of two sets of values: democratic society's requirements to allow open debate and individual autonomy and development with the compelling obligation to prevent attacks on vulnerable communities and ensure the equal and non-discriminatory participation of all individuals in public life. Governments often exploit the resulting uncertainty to threaten legitimate expression, such as political dissent and criticism or religious disagreement."

The above statement of the UNSR illustrates some of the complexities regarding the criminalisation of hate speech. The escalation of prejudice and intolerance has led many governments to criminalise hate speech. However, this creates inherent difficulties because hate speech is a vague term that lacks universal understanding, and such provisions are open to abuse and restrictions on a wide range of lawful expression.

*Overview of international instruments dealing with hate speech*

- Article 20(2) of the ICCPR obliges states to prohibit by law "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence."

- The Rabat Plan of Action was introduced in 2012 to provide recommendations on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. It outlines six factors that should be considered when determining whether a speaker intends and is capable of having the effect of

[11] For more on specific types of speech-related offences, see Media Defence above n 3 at 48-61.

inciting their audience to engage in violent or discriminatory action through the advocacy of discriminatory hatred.

The 2019 report of the UNSR on FreeEx also evaluates the human rights law that applies to the regulation of online hate speech and recommends that States should not treat online hate speech as a separate category from offline hate speech with higher penalties, should strictly define what constitutes prohibited content in their domestic laws, and should resist criminalising speech except in the gravest situations.

**Rabat Plan of Action: Six-part threshold test for expressions considered criminal offences**

"**Context**: Context is of great importance when assessing whether particular statements are likely to incite discrimination, hostility or violence against the target group, and it may have a direct bearing on both intent and/or causation. Analysis of the context should place the speech act within the social and political context prevalent at the time the speech was made and disseminated.

**Speaker**: The speaker's position or status in society should be considered, specifically the individual's or organization's standing in the context of the audience to whom the speech is directed.

**Intent**: Article 20 of the International Covenant on Civil and Political Rights anticipates intent. Negligence and recklessness are not sufficient for an act to be an offence under article 20 of the Covenant, as this article provides for "advocacy" and "incitement" rather than the mere distribution or circulation of material. In this regard, it requires the activation of a triangular relationship between the object and subject of the speech act as well as the audience.

**Content and form**: The content of the speech constitutes one of the key foci of the court's deliberations and is a critical element of incitement. Content analysis may include the degree to which the speech was provocative and direct, as well as the form, style, and nature of arguments deployed in the speech, or the balance struck between arguments deployed.

**Extent of the speech act**: Extent includes such elements as the reach of the speech act, its public nature, its magnitude, and the size of its audience. Other elements to consider include whether the speech is public, what means of dissemination are used, for example, a single leaflet or broadcast in the mainstream media or the Internet, the frequency, quantity, and extent of the communications, whether the audience had the means to act on the incitement, whether the statement (or work) is circulated in a restricted environment or widely accessible to the general public.

**Likelihood, including imminence**: Incitement, by definition, is an inchoate crime. The action advocated through incitement speech does not have to be committed for said speech to amount to a crime. Nevertheless, some degree of risk of harm must be identified. It means that the courts will have to determine that there was a reasonable probability that the speech would succeed in inciting actual action against the target group, recognising that such causation should be rather direct."

*Identifying hate speech*

It is sometimes tricky to distinguish between speech that is protected and that which constitutes hate speech.

- Hate speech may be prohibited only if the prohibition meets the standards of article 19(3), namely:[12]
    - **Legality**: laws criminalising hate speech must be precise, public, and transparent.
    - **Legitimacy**: laws should be justified to protect and respect the rights or reputations of others or to protect national security, public order, public health or morals.
    - **Necessity and proportionality**: the criminalising legislation must protect a legitimate interest and be the least restrictive means to achieve the purported aim.
- Hate speech is lawful and should be protected if it is:
    - Inflammatory or offensive expression that does not meet the above thresholds. Notably, this may include speech that is critical or that causes shock or offence.

*Online hate speech*

The nature of online domains, such as social media, creates conditions for the sharing and spreading of hate speech that are relevant to considerations of how to appropriately regulate hate speech. For example:

- Content is more easily posted online without due consideration or thought. Regulation must distinguish between poorly considered statements posted hastily online, and an actual threat that is part of a systemic campaign of hatred.
- Once something is online, it can be difficult (or impossible) to get it off entirely. Hate speech posted online can persist in different formats across multiple different platforms, which can make it difficult to police.
- Online content is frequently posted under the cover of anonymity, which presents an additional challenge to dealing with hate speech online.

[12] Article 19, 'Hate Speech Explained: A Toolkit,' (2015) (accessible at: https://www.article19.org/data/files/medialibrary/38231/'Hate-Speech'-Explained---A-Toolkit-%282015-Edition%29.pdf).

- The internet has transnational reach, which raises cross-jurisdictional complications in terms of legal mechanisms for combatting hate speech.

### ARTICLE 19 Hate Speech Explained: A Toolkit

ARTICLE 19 has published a toolkit on identifying and countering hate speech while protecting the rights to freedom of expression and equality. The toolkit responds to a growing demand for clear guidance on identifying 'hate speech' and for responding to the challenges hate speech poses within a human rights framework.

It is clear that cooperation from the state can be an effective means of safeguarding human rights. However, states are not always fulfilling their duties. Accordingly, lawyers, civil society organisations (**CSOs**), individuals, and community members need to work together to ensure that states are acting in compliance with their international human rights obligations. This can include strategic litigation, policy reform and advocacy, such as:

- Ensuring that states are creating an **enabling environment** for the right to freedom of expression. This can include ratifying international and regional human rights instruments, adopting domestic laws to protect freedom of expression and repealing any laws that unduly limit the right to freedom of expression.
- Ensuring that states **safeguard** the rights of individuals who exercise their right to freedom of expression. This requires ensuring that states make a concerted effort to end impunity for attacks on independent and critical voices.
- Ensuring that **domestic laws** guarantee equality before the law and equal protection of the law. That includes protection against discrimination on all grounds recognised under international human rights law.
- Ensuring that states establish or strengthen the role of **independent equality institutions** or expand the mandate of national human rights institutions.
- Ensuring that states adopt a **regulatory framework** for diverse and pluralistic media, which promotes pluralism and equality.

Some of these elements of online hate speech were addressed in recent cases in South Africa:

- In *South African Human Rights Commission (**SAHRC**) v Matumba,* involving the posting of hate speech online by a person allegedly using a false account on a social media platform, the Equality Court in South Africa considered whether a series of tweets posted in 2020 constituted harassment in terms of the country's law protecting equality. The SAHRC argued that the tweets included "serious, demeaning and humiliating comments against women, and black women in particular". An *amicus curiae* brief submitted by Media Monitoring Africa (**MMA**), a civil society organisation, highlighted the speed and application of content on Twitter, as opposed to more traditional formats, and analysed how to determine the reasonable reader in the context of social media.

- Another case in South Africa provided a detailed analysis of the line between "hurtful" and "hate" speech. In *Qwelane v. South African Human Rights Commission*, the South African Constitutional Court held that the prohibition of "hurtful" speech was an unjustifiable infringement of the right to freedom of expression, but held that the hate speech provision could be made constitutional by limiting it to expression that was intended *to be harmful or incite harm and to promote or propagate hatred.*

*Incidences of hate speech regulation*

Unfortunately, there are numerous examples of countries attempting to pass, or successfully passing, hate speech legislation that includes criminal penalties, particularly in Africa:

- In 2020 Ethiopia enacted the Hate Speech and Disinformation Prevention and Suppression Proclamation which, while having seemingly well-intentioned objectives, has been decried by civil society as a threat to freedom of expression and access to information online.[13]

- In Nigeria, the National Commission for the Prohibition of Hate Speech Bill was tabled in 2019 which would prohibit "abusive, threatening, and insulting behaviour", and another bill under consideration in 2022 proposes to classify hate speech as an electoral offence that may attract a jail term of 10 years or a fine of N40m or both.

- In South Africa, a bill on the prevention of hate crimes and hate speech has been criticised for its potential to be used to silence free speech and criticism and to stymie difficult discussions about race, gender, and sexuality.

*Cybercrime*

There is no single uniform or universally accepted definition for cybercrime, and there is an ongoing debate as to what the term entails. Some of the explanations and definitions advanced cover "a whole slew of criminal activity" including the theft of personal information, fraud, and the dissemination of ransomware.[14] Cybercrimes can also be the online extension of existing offline crimes such as harassment and sexual abuse, or producing, offering to make available, or making available, and distributing racist and xenophobic material.[15] For ease of reference, cybercrimes may be categorised as follows:[16]

[13] CIPESA, Edrine Wanyama, 'Ethiopia's New Hate Speech and Disinformation Law Weighs Heavily on Social Media Users and Internet Intermediaries' (2020) (accessible at: https://cipesa.org/2020/07/ethiopias-new-hate-speech-and-disinformation-law-weighs-heavily-on-social-media-users-and-internet-intermediaries/).
[14] Microsoft, 'Cybercrime and freedom of speech – a counterproductive entanglement' (2017) (accessible at https://www.microsoft.com/security/blog/2017/06/14/cybercrime-and-freedom-of-speech-a-counterproductive-entanglement/).
[15] See UNODC, 'Module 2: General Types of Cyber Crime; E4J University Module Series: Cybercrime (2019) (accessible at https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/intro.html) and UNODC 'Module 3: Legal Frameworks and Human Rights' E4J University Module Series: Cybercrime (2019) (accessible at https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-human-rights-and-cybercrime-law.html).
[16] Id. See further ITU 'Understanding cybercrime: Phenomena, challenges and legal response' (2012) (accessible at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf).

| Category | Examples of crimes |
|---|---|
| Offences against the confidentiality, integrity and availability of computer data and systems | Illegal access (hacking)<br>• Password breaking<br>• Distributed denial-of-service (DDoS) attacks<br>• Automated attacks and botnets |
| | Illegal data acquisition (data espionage)<br>• Scanning for unprotected ports<br>• Circumventing protection measures<br>• Social engineering<br>• Phishing |
| | Illegal interception<br>• Intercepting communications to record the information exchanges<br>• Setting up fraudulent access points |
| | Data interference<br>• Deleting, suppressing, or altering computer data<br>• Creation of malware and computer viruses |
| Content-related offences | • Sexual exploitation material<br>• Child sexual abuse material<br>• Commercial sexual exploitation of children<br>• Racist and xenophobic speech, hate speech and promotion of violence<br>• Disinformation and fake news |
| Copyright and trademark-related offences | • Reproduction of material<br>• Exchange of copyright-protected material (songs and movies)<br>• Certain file-sharing systems<br>• Domain name-related offences |
| Computer-related offences | • Computer-related fraud<br>• Online auction fraud<br>• Advance fee fraud<br>• Identity theft<br>• Cyberstalking, cyberharassment, and cyberbullying |

Cybercrime and cybersecurity are two interlinked issues in an interconnected digital environment. Cybersecurity, or the management and prevention of cybercrime, refers to the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber-environment and organisational and user's assets, such as computing devices, applications, and telecommunication systems.[17]

[17] ITU Definition of Cybersecurity, (accessible at: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx).

*Overview of international instruments*

Currently, there are three prominent international instruments that engage the topic of cybercrime:[18]

- The 2001 Convention on Cybercrimes (Budapest Convention) is the first international treaty that seeks to address internet and computer crimes. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrimes by adopting appropriate legislation and fostering international co-operation.

- The Additional Protocol to the Convention on Cybercrimes concerns the criminalisation of acts of a racist and xenophobic nature committed through computer systems. As an international legal instrument, the Protocol provides guidance and plays a key role in facilitating harmonisation across different legal regimes on the issue of specific forms of online speech.

- The 2014 African Union Convention on Cybersecurity and Personal Data (Malabo Convention), is a treaty dealing with cybercrime, data protection and related issues for the African continent. As of 2022, the Malabo Convention was still undergoing ratification, but if brought into force the Convention, among other things, encourages states to take necessary legislative and/or regulatory measures to establish criminal offences relating to cybercrimes. The offences include:

    - Creating, downloading, disseminating, or making available in any form writings, messages, photography, drawings or any other presentation of ideas or theories of racist or xenophobic nature through a computer system.
    - Threatening, through a computer system, to commit a criminal offence against a person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion, where such membership serves as a pretext for any of these characteristics.
    - Insulting, through a computer system, persons for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion or political opinion if used as a pretext for any of these factors, or against a group of persons distinguished by any of these characteristics.

Under the Malabo Convention, states are also urged to enact legislation criminalising acts related to child pornography. Importantly, the Malabo Convention does identify acts that warrant criminalisation, such as child pornography and racist and xenophobic acts. However, there are some concerns when it comes to free speech in the online context. For instance, the Malabo Convention uses vague language which may be open to abuse by states. An example is the provision that criminalises the use of **insulting language,** which is problematic because it describes a significant portion of the language used on the internet. This can lead to subjective prosecutions and, eventually, may lead to criminal convictions for what should be

[18] Global Action on Cybercrime Extended, 'Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime' (2016) (accessible at https://rm.coe.int/16806bf0f8).

protected speech. The Convention also raises concerns in that it expands the search and seizure powers of the state.

*The rise in cybercrime laws*

The UNODC has found that cybercrime laws are of particular relevance to the criminalisation of online speech because the laws that are enacted to regulate cybercrimes can result in the restriction of freedom of expression. Access Now notes that one of the main concerns about the plethora of laws that are currently being enacted to regulate cybercrimes is that many of them lack clear definitions and are susceptible to being used to regulate online content and restrict freedom of expression. This is a growing concern among human rights defenders as many have been subjected to a wave of arrests and convictions in what is an escalating assault on freedom of expression through cybercrime laws.

**Cybercrime laws in Nigeria**

While there may be legitimate aims in enacting these laws, there are serious concerns that many of these laws are vague and overbroad and are susceptible to being used to restrict freedom of expression. Amnesty International has reported a growing trend of arrests, detention and torture of journalists and bloggers as well as pointed attacks on major media houses. Journalists and bloggers are reportedly being charged with cybercrimes under Nigeria's Cybercrime Act, which criminalises a substantial number of online forms of expression.

This situation may be exacerbated if the proposed Protection from Internet Falsehoods and Manipulation Bill is passed into law. The Bill is aimed at enabling measures to be taken to detect, control and safeguard against uncoordinated and inauthentic behaviour and other misuses of online accounts and bots, enabling measures to be taken to enhance disclosure of information regarding paid content directed towards a political end and to sanction offenders.

The Bill seeks to criminalise, among other things, prohibited statements of facts which include false statements of fact and statements that are likely to be prejudicial to the country's security, public health, public safety, public tranquillity or finances, prejudice Nigeria's relations with other countries, influence the outcome of an election or referendum, incite feelings of enmity, hatred towards a person, ill will between a group of persons, or diminish public confidence in the performance or exercise of any duty, function or power by the government.

If this Bill is passed it could mean a further affront to freedom of expression in Nigeria, which as it stands is under threat due to the cybercrime legislation that is already in existence. Further, the Bill gives the State wide-ranging powers, which may be susceptible to abuse.[19]

[19] For further commentary on trends in Africa see CIPESA, 'Why are African Governments Criminalising Online Speech? Because They Fear Its Power' (2018) (accessible at https://cipesa.org/2018/10/why-are-african-governments-criminalising-online-speech-because-they-fear-its-power/).

The Government of Nigeria's extended suspension of the operations of the social networking service, Twitter, for close to six months up to January 2022 appear to have reignited the government's interest to implement the proposed Bill.
It is further worth noting that in 2020, the ECOWAS Community Court of Justice ordered Nigeria to repeal its cybercrime legislation, which was held to violate the right to freedom of expression.

In relation to the concerns regarding cybercrime legislation, a 2019 Report of the UNSR on FreeEx noted:

> "A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world. While the role that technology can play in promoting terrorism, inciting violence and manipulating elections is a genuine and serious global concern, such threats are often used as a pretext to push back against the new digital civil society."

**UN Resolution on Countering the Use of Information and Communications Technologies for Criminal Purposes**

In July 2019, the United Nations General Assembly presented a Draft Resolution on countering the use of information and communications technologies for criminal purposes.

CSOs were highly critical of the resolution, calling for delegations to vote against it. In an Open letter to UN General Assembly, the following concerns were raised:

- The "use of information and communications technologies for criminal purposes" is not defined in the resolution, which is not just a concern from an accuracy perspective; but also opens the door to criminalising ordinary online behaviour that is protected.
- While legislation aimed at addressing cybercrime can be necessary and reinforce democratic institutions, when misused, cybercrime laws can create a chilling effect.
- It goes far beyond what the Budapest Convention allows for regarding cross-border access to data, including by limiting the ability of a signatory state to refuse to provide access to requested data.
- Building on and improving existing instruments is more desirable and practical than diverting already scarce resources into the pursuit of a new international framework, which is likely to stretch over many years and unlikely to result in consensus.
- The establishment of an ad hoc intergovernmental committee of experts to address the issue of cybercrime would exclude key stakeholders who bring valuable expertise and perspectives.

Despite these concerns, the resolution was adopted and published in January 2020. Through the resolution, an open-ended ad hoc intergovernmental committee of experts, representative

of all regions, will be established to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional, and international levels on combating the use of ICTs for criminal purposes.

Lawyers and activists should monitor further developments in relation to this and, where possible, engage with relevant stakeholders in order to positively influence future developments and decisions.

*Disinformation and 'fake news'*

Disinformation includes statements which are known or reasonably should be known to be false that seek to mislead the public, and, in turn, interfere and inhibit the ability of the public to seek, receive, and impart information.[20] In 2018, the High-Level Expert Group on Fake News and Online Disinformation defined disinformation to mean—

> "all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit. It does not cover issues arising from the creation and dissemination online of illegal content. Nor does it cover other forms of deliberate but not misleading distortions of facts, such a satire and parody."

Disinformation that is designed to look like news content is sometimes popularly referred to as "fake news." The High-Level Expert Group noted two reasons for avoiding the use of this term:

- The term is inadequate to capture the complex problem of disinformation, which involves content that blends fabricated information with facts.
- The term is misleading as it has been appropriated by some politicians and their supporters to dismiss coverage that they find disagreeable and has thus become a weapon with which powerful actors can interfere in the circulation of information and attack and undermine independent news media.

Concerted disinformation campaigns by foreign state and non-state actors to interfere in the 2016 US presidential elections brought unprecedented light on the issue of "fake news" and the ease with which disinformation can be disseminated online.[21] The COVID-19 pandemic also highlighted the capacity for the rapid spread of disinformation, which undermined efforts to address the disease and roll-out treatments and vaccines.

In response to this growing trend of disinformation, a number of states have enacted legislation criminalising the online publication of false statements. Such responses continue to increase in speed and magnitude and to cause demonstrable and significant public harm. The 2017

[20] Access Now, Civil Liberties Union for Europe and European Digital Rights 'Informing the disinformation debate' (2018) (accessible at https://dq4n3btxmr8c9.cloudfront.net/files/2r7-0S/online_disinformation.pdf).
[21] Vox, '4 main takeaways from new reports on Russia's 2016 election interference' (2019) (accessible at: https://www.vox.com/world/2018/12/17/18144523/russia-senate-report-african-american-ira-clinton-instagram)

Joint Declaration on Fake News, Disinformation and Propaganda by the UN Special Rapporteur on Freedom of opinion and expression together with his counterparts from the Organization for Security and Co-operation in Europe (**OSCE**), the Organization of American States (**OAS**), and the African Commission on Human and Peoples' Rights (**ACHPR**), noted that countering these issues poses complex challenges that could result in censorship and the suppression of critical thinking.

*Addressing fake news*

Various international bodies, states and organisations have grappled with different responses to the complexities of disinformation. However, many countries have responded with harsh legislation that does not strike an appropriate balance between addressing disinformation and protecting the right to freedom of expression. The advent of the COVID-19 pandemic and associated disinformation has further accelerated this trend. Some examples include:

- **Malaysia**: In 2018, the Malaysian government enacted the Anti-Fake News Act, which attaches criminal liability to persons who knowingly create, offer, publish, print, distribute, circulate, or disseminate fake news. The Act defined "fake news" as including "any news, information, data and reports, which is or are wholly or partly false, whether in the form of features, visuals or audio recordings or in any other form capable of suggesting words or ideas."[22] However, the existence of the Act was short-lived. It was repealed by the Anti-Fake News (Repeal) Act 825 of 2020, with government citing its commitment to abolish draconian laws and protect media freedom. However, in March 2021, the government issued the Emergency (Essential Powers) (No. 2) Ordinance 2021 which criminalises the dissemination of fake news related to COVID-19 and repeated many of the problematic provisions of the Anti-Fake News Act.

- **Cameroon:** The Penal Code in Cameroon criminalises the sending out or propagation of false information. Section 113 imposes a penalty of imprisonment between three months to three years and a fine between CFAF 100 000 (approximately USD172) to CFAF 2 000 000 (approximately USD3400) for persons found guilty of this offence. The Committee to Protect Journalists (**CPJ**) has noted with concern the arrest and detention of journalists under this provision, in particular, a journalist who was sent to maximum-security prison on charges of defamation and spreading false news.

- **Russia**: In 2019, the State Duma (the Russian Federal Assembly) passed legislation on Information, Information Technologies and Protection of Information, and a Code of Administrative Offenses both aimed at countering "fake news". ARTICLE 19 explains that these amended laws allow authorities in Russia to block websites that they consider to be publishing disinformation. Websites are also liable for insulting Russian authorities. The Moscow Times reported that "online news outlets and users that spread "fake news" will face fines of up to 1.5 million Rubles (USD20 000) for repeat offences. Insulting state symbols and the authorities, including Vladimir Putin, will carry a fine of up to 300 000 Rubles (USD4 000) and 15 days in jail for repeat offences."

[22] The Law Library of Congress, 'Initiatives to Counter Fake News in Selected Countries' (2019) (accessible at https://www.loc.gov/law/help/fake-news/counter-fake-news.pdf).

- **Kenya:** Kenya's Computer Misuse and Cybercrime Act criminalises the 'publication of false information in print, broadcast, data or over a computer system' in Articles 22 and 23. Despite legal challenges to various provisions that were alleged to stifle freedom of expression online, the Act was upheld as constitutional and came into effect in 2020.

- **COVID-19 false news laws:** the COVID-19 pandemic sparked a raft of oppressive false news laws across the world. The Disinformation Tracker, a collaborative civil society initiative, has documented the various responses, including laws criminalising false publications, initiated across the continent.

The criminalisation of the dissemination of fake news is likely to increase and may cause significant violence to freedom of expression. Such developments should be closely monitored and challenged where necessary. Fortunately, criminalisation is not the only option in addressing the rise of disinformation. Media and information literacy campaigns can effectively counter disinformation but providing a flood of accurate, reliable information instead and immunising audiences against false information before they are exposed to it. International bodies, states and CSOs are continually presenting new and innovative ways to address disinformation. Some notable contributions from international bodies include:

- **UNESCO**: UNESCO has developed the Journalism, fake news & disinformation: Handbook for journalism education and training. The handbook shares international good practices and serves as an internationally-relevant model curriculum, open to adoption or adaptation, which responds to the emerging global problem of disinformation that confronts societies in general, and journalism in particular.

- **European Union**: In 2018, the European Union published its Code of Practice on Disinformation. The purpose of the Code is to identify the actions that signatories could put in place in order to address the challenges related to disinformation. The Code discusses the need for safeguards against disinformation, implementation of reasonable policies, effective measures to close discernible fake accounts; and the improvement of the scrutiny of advertisement placements. The Code identifies best practices that signatories – such as Facebook, Google, Twitter, and Mozilla – should apply when implementing the Code's commitments.

- **Viral Facts Africa**: In response to the flood of COVID-19 mis- and disinformation on social media, the World Health Organisation (**WHO**) launched the Viral Facts Africa initiative, a network of fourteen fact-checking organisations and public health bodies that undertook health fact checks, explainers, myth busters and misinformation literacy messages optimised for sharing on Facebook, Twitter and Instagram. The initiative aims to rapidly debunk myths where they occur and provide viral, credible information.

At a state level, there have also been promising developments. In 2019, the US Library of Congress produced a report on Initiatives to Counter Fake News in Selected Countries. Some positive initiatives include:

- **Argentina:** The Commission for the Verification of Fake News was established. The Commission is envisaged to form part of the National Election Chamber, to assist with overcoming issues of disinformation during elections.

- **Sweden**: Bamse the Bear, a popular cartoon character in Sweden, has adopted a new role in teaching children about the dangers of disinformation by illustrating what happens to the bear's super-strength when false rumours are circulated about him.

- **Kenya:** The United States Embassy in Kenya started a media literacy campaign known as "YALI Checks: Stop.Reflect.Verify" to counter the spread of false information in Kenya. The campaign relies on an email series, an online quiz, blog posts, online chats, public outreach, educational videos, and an online pledge to engage with the Kenya chapter of the Young African Leaders Initiative (YALI) about disinformation.

- **Finland**: Finland has been lauded for winning the war on disinformation due to its initiatives aimed at teaching residents, students, journalists and politicians how to counter false information. The initiatives include courses at community colleges and the introduction of lessons in schools about disinformation.

- **Canada**: In January 2019, the Canadian government announced a multi-pronged effort to combat misinformation ahead of elections in the fall, comprised of four prongs. First, it created a "Critical Election Incident Public Protocol" to monitor and notify other agencies and the public about disinformation attempts, led by non-political officials. The government also called on social media platforms to do more to combat disinformation ahead of the election, in tandem with seeking to pass legislation to compel tech companies to be more transparent about their anti-disinformation and advertising policies. Third, Canada announced it was giving $7 million to projects aimed at increasing public awareness of misinformation online, and finally, the country launched a digital charter that set out principles for protecting freedom of expression while defending against online threats and disinformation.

**Suggested standards for addressing disinformation**

In the Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda, the following standards are suggested:

- General prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information', are incompatible with international standards for restrictions on freedom of expression, and should be abolished.
- Criminal defamation laws are unduly restrictive and should be abolished. Civil law rules on liability for false and defamatory statements are legitimate only if defendants are given a full opportunity and fail to prove the truth of those statements and also benefit from other defences, such as fair comment.

- State actors should not make, sponsor, encourage or further disseminate statements that they know or reasonably should know to be false (disinformation) or which demonstrate a reckless disregard for verifiable information (propaganda).
- State actors should, in accordance with their domestic and international legal obligations and their public duties, take care to ensure that they disseminate reliable and trustworthy information, including about matters of public interest, such as the economy, public health, security and the environment.

In line with these standards, the ACHPR's 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa provides under Principle 22 that States should repeal all laws that criminalise the publication of false news.

**Determining limitations on freedom of expression**

Global Partners Digital, in an attempt to determine how to tackle disinformation in a way that respects human rights, proposes an information-gathering approach to determine if disinformation amounts to a justifiable limitation of freedom of expression. Some of the suggested questions include:

- Is the basis for any restrictions on what information individuals can search for, receive, or impart set out in law?
- Is there clarity over the precise scope of the law so that individuals will know what is and is not restricted?
- Is speech restricted only where it is in pursuance of a legitimate aim?
- Are there exceptions or defences where the individual reasonably believed the information to be true?
- Are determinations made by an independent and impartial judicial authority?
- Are responses or sanctions proportionate?
- Is disinformation clearly defined?
- Are intermediaries liable for third-party content?
-

*Fake news in the courts*

In Africa, fake news laws have been challenged in the courts both domestically and at the regional level. In the case of *Chipenzi v The People* (2014), the High Court of Zambia found that a provision of Zambia's Penal Code that prohibited the publication of false information likely to cause public fear violated the Constitution as it did not amount to a reasonable justification for limiting the freedom of expression.

the Court of Justice of the Economic Community of West African States (**ECOWAS Court**) and the East African Court of Justice (**EACJ**) have both delivered landmark rulings on cases relating to the criminalisation of fake news.

In 2018, the ECOWAS Court decided the *Federation of African Journalists and Others v The Republic of The Gambia* matter, in which it considered offences of sedition, false news and criminal defamation in The Gambia's Criminal Code. Several journalists were arrested on charges of spreading false news. They argued that their rights to freedom of expression had been violated and sought a declaration from the Court that certain provisions of The Gambia's Criminal Code were inconsistent with regional and international law. The ECOWAS Court found that the criminal laws of the Gambia imposed criminal sanctions that are disproportionate and not necessary in a democratic society where freedom of speech is a guaranteed right and ordered that the legislation be reviewed. The Criminal Code was found to be broad and capable of casting an:

> "[E]xcessive burden upon the applicants in particular and all those who would exercise their right of free speech and violates the enshrined rights to freedom of speech and expression under Article 9 of the African Charter, Article 19 of the ICCPR and Article 19 of UDHR".

More recent developments in respect of the criminalisation of fake news came from the EACJ in the matter between the *Media Council of Tanzania and Others v Attorney-General of the United Republic of Tanzania*. In this case, the applicants challenged various provisions of the Tanzanian Media Services Act on the basis that "the Act in its current form is an unjustified restriction on the freedom of expression which is a cornerstone of the principles of democracy, the rule of law, accountability, transparency and good governance which [Tanzania] has committed to abide by, through the Treaty." The applicants argued that it violated freedom of expression by restricting the types of news or content without reasonable justification, criminalising the publication of false news and rumours, criminalising seditious statements, and vesting the Minister with absolute power to prohibit the import of publications or to sanction media content. The respondent argued that all the provisions are just and did not violate the right to freedom of expression and associated rights.

The EACJ held that although the sections were set out in law, the contents of these sections were vague, unclear, and imprecise. It noted that the use of the word "undermine" in the impugned provision, which formed the basis of the offence, was too vague to provide assurance to a journalist or other person who sought to regulate their conduct within the law. The EACJ further noted that the words "impede", "hate speech", "unwanted invasion", "infringe lawful commercial interests", "hinder or cause substantial harm", "significantly undermines" and "damage the information holder's position" are too broad or vague.

It further stated that it was persuaded by the applicants' submissions that section 52(1) of the Act failed the test of clarity and certainty. In this regard, it noted that definitions of sedition hinged on the possible and potential subjective reactions of audiences to whom the publication was made. This makes it impossible for a journalist or other individual to predict and thus plan their actions. In conclusion, the EACJ found in favour of the applicants and declared that, among other things, all the challenged provisions were in violation of articles 6(d) and 7(2) of the Treaty for the establishment of the East African Court of Justice (**EACJ Treaty**) and directed the Republic of Tanzania to take such measures as are necessary to bring the Media Services Act in compliance with the EACJ Treaty.

In an interesting case that addressed disinformation on social media, the High Court in South Africa in 2019 awarded damages to a public official who had been subject to a defamatory statement made by an opposition political party accusing him of nepotism and corruption. In the case of *Manuel v Economic Freedom Fighters and Others*, the court found that the political party had failed to prove the statement was true and taken no steps to verify its truthfulness, had published the tweet unreasonably, and had acted "with reckless indifference as to whether it was true or false". Most notably, the court held that the reasonable publication defence is not only available to the media:

> "Because of social media platforms like Twitter, Facebook and others, ordinary members of society now have publishing capacities capable of reaching beyond that which the print and broadcast media can".

On appeal, the damages award was subsequently overturned while the finding of defamation was upheld.

These landmark judgments provide guidance on the appropriate balance between legislating disinformation and protecting freedom of expression, and it is hoped they will have a far-reaching impact on other jurisdictions across the African region in ensuring that any responses to disinformation are based on international freedom of expression standards.

*Defamation*

Defamation is an important legal remedy for people whose reputation and dignity are harmed by the statements or actions of others. However, it is also frequently abused to unjustly stifle dissent. In particular, criminalising defamation is generally considered, under international human rights law, to be disproportionate and an unjustifiable infringement on the right to freedom of expression. The spread of the internet, and particularly social media platforms, has made it easier than ever to publish content to a wide audience, resulting in a rise in defamation being used against critical statements published online, and in speech that should be protected being criminalised under criminal defamation laws.

*Overview of international instruments*

The foundation for defamation in international law is article 17 of the ICCPR, which provides for protection against unlawful attacks on a person's honour and reputation. Article 19(3) of the ICCPR also refers to the rights and reputation of others as a legitimate ground for limiting the right to freedom of expression.[23] Reputation is therefore the underlying basis in any claim of defamation, whether slander or libel.[24]

---

[23] ICCPR: International Covenant on Civil and Political Rights (1976) (accessible at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx).

[24] For a fuller discussion on the law on defamation, see the training manual published by Media Defence on the principles of freedom of expression under international law: Richard Carver, 'Training manual on international and comparative media and freedom of expression law', Media Defence at pp 48-64 (2018) (accessible at: https://www.mediadefence.org/sites/default/files/resources/files/MLDI.FoEManual.Version1.1.pdf). See also above no. 6 for a definition of libel and slander.

It is also noteworthy that in 2010 the ACHPR issued a Resolution calling on states to repeal criminal defamation laws or insult laws.[25]

*Defamation in the courts*

In recent years, many countries around the world have taken steps to decriminalise defamation in line with human rights standards. The UN Human Rights Council (UNHRC) General Comment No. 34 provides that: "States Parties should consider the decriminalisation of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty".[26] Principle 22 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa calls on States to amend criminal laws on defamation and libel in favour of civil sanctions, and that the imposition of custodial sentences for defamation is a violation of the right to freedom of expression.

Several recent judgments across Africa demonstrate this trend, including the 2013 matter of *Konaté v Burkina Faso* in the African Court on Human and Peoples' Rights, *Misa-Zimbabwe et al v Minister of Justice et al in the Zimbabwe Constitutional Court*, *Peta v Minister of Law, Constitutional Affairs and Human Rights* in the Constitutional Court of Lesotho, and the 2018 case of *Federation of African Journalists and Others v The Gambia* in the ECOWAS Court. Most recently, the ACHPR ruled that Rwanda's criminal defamation laws violated freedom of expression and impeded development in democracies. It noted that such laws "constitute a serious interference with freedom of expression, impeding the public's right to access information, and the role of the media as a watchdog, preventing journalists and media practitioners from practising their profession in good faith, without fear of censorship".

Despite this, some countries, including South Africa and Zambia retain criminal defamation laws, underscoring the need for advocacy and litigation to address the situation.

The growth of Strategic Lawsuits Against Public Participation (SLAPP) suits by corporate actors using defamation laws to silence or intimidate is another concerning contemporary development that needs to be challenged. The ECtHR referred for the first time to the notion of a SLAPP suit in *OOO Memo v Russia* (2022) which involved a civil defamation suit brought by a Russian regional state body against a media company. In *Koko v Tanton* (2021), the Johannesburg High Court in South Africa held that a defamation case brought by a former executive of a state entity constituted a SLAPP suit.

## Conclusion

The criminalisation of online speech presents an affront to the exercise of the right to freedom of expression online. However, as illustrated above, there are competing interests that need to be considered. With the rise of nefarious activities and feeble excuses from governments, it is important, now more than ever, that activists, lawyers, and individuals ensure that freedom

[25] ACHPR/Res.169(XLVIII)10, 'Resolution on Repealing Criminal Defamation Laws in Africa,' (2010) (accessible at: https://www.achpr.org/sessions/resolutions?id=343).
[26] UN Human Rights Council, 'General Comment No. 34 at article 47 (2011) (accessible at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf).

of expression is protected, and only limited in terms of the clear prescripts of international human rights law.

*Module 4*

# Privacy and Security Online

*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 4

## Privacy and Security Online

**This module aims:**

- **To provide an overview of the right to privacy.**
- **To set out data protection principles and explain data retention.**
- **To identify emerging issues in communications surveillance, To explain the rights-related concerns about biometrics and facial recognition.**
- **To unpack the relationship between encryption and anonymity.**
- **To set out the principles of journalistic source protection.**
- **To identify emerging issues in online harassment.**

---

## Scope and the Right to Privacy

In the current data-driven era, the right to privacy has gained increasing recognition as a fundamental right, both in itself and as an enabler of other rights. This includes enabling the right to freedom of expression, for instance by allowing individuals to share views anonymously in circumstances where they may fear being censured for those views, by allowing whistle-blowers to make protected disclosures, and by enabling members of the media and activists to communicate in a secure manner beyond the reach of unlawful government interception.

The key provision under international law regarding the right to privacy is contained in article 17 of the International Covenant on Civil and Political Rights (**ICCPR**):

- Sub-article (1) provides that no one shall be subjected to arbitrary or unlawful interference with his (or her) privacy, family, home or correspondence, nor to unlawful attacks on his (or her) honour and reputation.
- Sub-article (2) goes on to provide that everyone has the right to the protection of the law against such interference or attacks.

In the African context, the African Charter on Human and Peoples' Rights (**African Charter**) does not contain an express provision on the right to privacy. However, it has been argued that the right can – and should – be read into the African Charter through to the right to respect for life and integrity of the person, the right to dignity, and the right to liberty and security of

the person.[1] This argument is based on the approach taken by the African Commission on Human and Peoples' Rights (**African Commission)** in *Social and Economic Rights Action Centre and Another v Nigeria* and the comparative jurisprudence from the Supreme Court of India in *Justice KS Puttaswamy (Retd) and Another v Union of India and Others*.[2]

It bears mention that other African regional instruments do recognise the right to privacy. For example, article 10 of the African Charter on the Rights and Welfare of the Child provides that:

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

Additionally, the African Union (**AU**) Convention on Cyber Security and Personal Data Protection (**the Malabo Convention**) recognises in its preamble the commitment of the AU to build an information society and to protect "the privacy of its citizens in their daily or professional lives, while guaranteeing the free flow of information". However, the Malabo Convention is not yet in force, as it has not yet received the requisite number of ratifications.

At the domestic level, more than 50 African constitutions, inclusive of amendments and recent reviews, include reference to the right to privacy.[3]

---

[1] Singh and Power, 'The privacy awakening: The urgent need to harmonise the right to privacy in Africa' African Human Rights Yearbook 3 (2019) 202 at p 202, (accessible at: http://www.pulp.up.ac.za/images/pulp/books/journals/AHRY_2019/Power%202019.pdf).

[2] Id.

[3] Id. The following 52 African constitutions include reference to the right to privacy: articles 46-7 of the Constitution of Algeria (1989); articles 32-4 of the Constitution of Angola (2010); articles 20-1 of the Constitution of Benin (1990); articles 3 and 9 of the Constitution of Botswana (1966); article 6 of the Constitution of Burkina Faso (1991); article 43 of the Constitution of Burundi (2005); Preamble to the Constitution of Cameroon (1972); articles 38, 41 and 42 of the Constitution of Cape Verde (1980); articles 16 and 19 of the Constitution of the Central African Republic (2016); Preamble to the Constitution of the Comoros (2001); articles 29 and 31 of the Constitution of the Democratic Republic of the Congo (2005); articles 20 and 26 of the Constitution of the Republic of the Congo (2015); article 8 of the Constitution of Côte d'Ivoire; articles 12-3 of the Constitution of Djibouti (2010); articles 57-8 of the Constitution of Egypt (2014); article 13 of the Constitution of Equatorial Guinea (1991); article 18 of the Constitution of Eritrea (1997); article 26 of the Constitution of Ethiopia (1994); article(1)(5)-(6) of the Constitution of Gabon (1991); article 23 of the Constitution of The Gambia (1996); article 18 of the Constitution of Ghana (1992); article 12 of the Constitution of Guinea (2010); articles 44 and 48 of the Constitution of Guinea-Bissau (1984); article 31 of the Constitution of Kenya (2010); article 4(f)-(g) of the Constitution of Lesotho (1993); article 16 of the Constitution of Liberia (1986); articles 11-3 of the Constitution of Libya (2011); article 13 of the Constitution of Madagascar (2010); article 21 of the Constitution of Malawi (1994); article 6 of the Constitution of Mali (1992); article 13 of the Constitution of Mauritania (1991); articles 3(c) and 9 of the Constitution of Mauritius (1968); article 24 of the Constitution of Morocco (2011); article 41 of the Constitution of Mozambique (2004); article 13 of the Constitution of Namibia (1990); articles 27 and 29 of the Constitution of Niger (2017); article 37 of the Constitution of Nigeria (1999); article 2 of the Constitution of Rwanda (2003); articles 24-25 of the Constitution of Sao Tome and Principe (1975); articles 13 and 16 of the Constitution of Senegal (2001); article 20 of the Constitution of the Seychelles (1993); article 15(c) of the Constitution of Sierra Leone (1991); article 19 of the Constitution of Somalia (2012); article 14 of the Constitution of South Africa

## Data Protection

*Key principles of data protection*

Data protection is one of the primary measures through which the right to privacy is given effect. Data protection laws are aimed at protecting and safeguarding the processing of personal information (or personal data).

Although the specific definitions and terms may vary, most data protection laws set out similar basic concepts:

- *Personal information* or an equivalent term generally refers to any information relating to an identified or identifiable natural person which can be used to identify them, whether directly or indirectly, such as their name, contact details, age, race, gender, sexual orientation, health information, financial information, employment details, political or religious views, or biometric information.
- *A data subject* is any person to whom this information relates – in other words, a person whose rights are at stake.
- *A data controller*, which can typically be either a public or private body, is the person or entity responsible for processing the personal information about the data subject.
- *Processing* usually refers to a wide range of actions that can be performed on personal information including collection, organisation, storage, alteration, retrieval, sending, or deletion, and includes both manual and automated means.
- A *data protection authority* is a type of independent authority or public body established to monitor and enforce compliance with a data protection framework. This module explores data protection authorities in more detail below under Use of data protection authorities to vindicate the right to privacy.

While there may be differences across jurisdictions, there are also a number of governing principles that appear in most data protection frameworks. The Personal Data Protection Guidelines for Africa[4] (**Data Protection Guidelines**), a joint initiative of the Internet Society (**ISOC**) and the AU, sets out key data protection principles that appear across most frameworks:[5]

- **Collection limitation**: Personal data must be obtained and processed lawfully, fairly, and, to the extent possible, transparently.

(1996); article 22 of the Constitution of South Sudan (2011); article 14(1)(c) of the Constitution of Swaziland (2005); articles 16 and 18 of the Constitution of the United Republic of Tanzania (1977); article 28 of the Constitution of Togo (1992); article 24 of the Constitution of Tunisia (2014); article 27(1) of the Constitution of Uganda (1995); articles 11(d) and 17 of the Constitution of Zambia (1991); and article 57 of the Constitution of Zimbabwe (2013).

[4] ISOC and AU, 'Personal Data Protection Guidelines for Africa', 9 May 2018, accessible at https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf.

[5] Data Protection Principles at pp 9-10.

- **Data quality**: Personal data must be accurate at the point of collection, and reasonable steps must be taken to ensure its accuracy is maintained over the period of retention.
- **Purpose specification**: Personal data must be collected only for specified, explicit, and legitimate purposes. Personal data should only be used for such other purposes as are compatible with applicable laws, such as archiving data that is in the public interest, or for scientific research.
- **Use limitation**: Personal data must not be disclosed, made available, or used for other purposes except with the consent of the individual or where authorised by law.
- **Security safeguards**: Personal data should be protected by reasonable security safeguards to maintain its integrity and confidentiality.
- **Openness**: There should be a general policy of openness about developments, practices, and policies with respect to personal data.
- **Individual participation**: Individuals must have the right to obtain information about their personal data held by others. This data must be provided within a reasonable period of time, in a form that is readily intelligible, and at a cost that is not excessive. Data subjects have the right to challenge their data and to have it amended if it is inaccurate, or erased if that is appropriate.
- **Accountability**: Those who collect and process personal data must be able to demonstrate their compliance with these principles.

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

Another key principle of data protection frameworks is that personal data should not be transferred to a country that does not ensure an adequate level of protection for the rights and freedoms of data subjects when it comes to the processing of personal information.[6]

**Cross-border data transfers: The case of Max Schrems**

Source: Case No. C-362/14, 6 October 2015, accessible at: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN

In *Maximillian Schrems v Data Protection Commissioner*, Mr Schrems – a European citizen – lodged a complaint with the Irish Data Protection Commissioner that some or all of the data that he had provided to Facebook was transferred from Facebook's Irish subsidiary to servers located in the United States of America (**US**), where it was processed. As the US does not have a comprehensive data protection law, Mr Schrems argued that the law and practice in the US did not offer sufficient protection against surveillance by the US public authorities and did not meet the test for adequacy as contemplated under European law.

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

The Court of Justice of the European Union (**CJEU**) upheld the claim, noting that the protective rules laid out in the data sharing arrangement between the European Union (**EU**) and the US (known as the 'Safe Harbour Agreement') could be disregarded by the US where they conflicted with national security, public interest and law enforcement requirements of the US. The CJEU held that any legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the right to privacy. Furthermore, the CJEU found that legislation that does not provide for an individual to pursue legal remedies to access their personal information, or to have such information rectified or erased, compromises the essence of the right to effective judicial protection.

Accordingly, the CJEU declared the Safe Harbour Decision invalid, with immediate effect. In line with this judgment, the threshold that has been established for determining the adequacy of protection is to ascertain whether it is "essentially equivalent."

This decision was subsequently followed up by another dubbed 'Schrems II' which speaks to the use of "standard contractual clauses" to transfer data between Europe and the US.

*Data protection frameworks in Africa*

A growing number of African states have enacted data protection laws, and more are in the process of doing so. In addition to giving effect to the right to privacy, data protection legislation also has a key role to play in facilitating trade amongst states, as many data protection laws restrict cross-border data transfers in circumstances where the state receiving the information does not provide an adequate level of data protection.

**Data Protection Africa**

Source: https://dataprotection.africa/

Many countries in Africa have either an existing or draft data protection framework in place or make reference to data privacy in other sectoral laws. However, even countries with a data protection framework in place are facing challenges with resource constraints, delayed implementation, or a failure to appoint or capacitate the regulatory authorities. Key questions to consider that may differ across jurisdictions include what constitutes personal information in a particular jurisdiction; the exemptions that may apply; the conditions for the lawful processing of data; how that data can be transferred across borders; whether breach notification is required, and if so, what requirements apply.

For a full overview of the data protection landscape in Africa, visit Data Protection Africa: https://dataprotection.africa/.

As noted in the Data Protection Guidelines, in considering the relevant data protection framework, it is necessary to understand the African context and the particular characteristics that arise:[7]

- Significant cultural and legal diversity across the continent, with different privacy expectations.
- Variations in access to technology and online services among member states.
- Sensitivities regarding ethnicity and profiling of citizens without consent.
- Different levels of capability in areas such as technology and technology-related law and governance.
- Risks arising from high dependency on non-African manufacturers and service providers, including the limited ability of African states to influence the behaviour of external service providers, and the potentially increased risk of data misuse where content and services are solely provided by foreign companies.

According to the Data Protection Guidelines, this context presents unique challenges to the enforcement of local data protection laws that may make such enforcement more difficult.

While the Malabo Convention[8] is not yet in force, it still provides useful guidance at the regional level to states looking to implement data protection frameworks at the domestic level. Chapter II of the Malabo Convention sets out the principles relevant to data protection. As set out in article 8(1), the objective of the Convention is for each state party to commit itself to establish a legal framework "aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy with prejudice to the principle of the free flow of personal data."

Article 13 of the Malabo Convention sets out the following basic principles governing the processing of personal data:

- Principle 1: Principle of consent and legitimacy of personal data processing.
- Principle 2: Principle of lawfulness and fairness of personal data processing.
- Principle 3: Principle of purpose, relevance and storage of processed personal data.
- Principle 4: Principle of the accuracy of personal data.
- Principle 5: Principle of transparency of personal data processing.
- Principle 6: Principle of confidentiality and security of personal data processing.

Articles 16 to 19 of the Malabo Convention set out the rights of data subjects, namely the right to information; the right of access; the right to object; and the right of rectification or erasure. Articles 20 to 23 go on to set out the obligations of personal data controllers, namely the confidentiality obligations; the security obligations; the storage obligations; and the sustainability obligations.

[7] Data Protection Principles at p 7.
[8] Accessible at https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Thirteen of the required fifteen states have ratified the Convention as of October 2022: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf.

In respect of cross-border data transfers, article 14(6)(a) provides that: "The data controller shall not transfer personal data to a non-Member State of the African Union unless such a State ensures an adequate level of protection of the privacy, freedoms and fundamental rights of the persons whose data are being or are likely to be processed". Sub-article (b) goes on to provide that the prohibition does not apply if the data controller has requested authorisation for the transfer from the relevant data protection authority before the data has been transferred.

**Processing for journalistic, research, artistic or literary purposes**

Source: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Article 14(3) of the Malabo Convention provides for a specific exemption that applies to the processing of personal data for journalistic, research, artistic or literary purposes. It provides that: "Personal data processing for journalistic purposes or for the purposes of research or artistic or literary expression shall be acceptable where the processing is solely for literary or artistic expression or for professional exercise of journalistic or research activity, in accordance with the code of conduct of these professions."

Article 14(4) goes on to provide that the provisions of the Convention "shall not preclude the application of national legislations with regard to the print media or the audio-visual sector, as well as the provisions of the criminal code which provide for the conditions for exercise of the right of reply, and which prevent, limit, compensate for and, where necessary, repress breaches of privacy and damage to personal reputation."

*Extra-territorial application of data protection frameworks in Europe*

There are two key European instruments in respect of data protection that have extra-territorial application for African states: **Convention 108** and the **GDPR**.

The Convention for the Protection of Individuals with regard to the Processing of Personal Data[9] – commonly referred to as Convention 108 – is an instrument of the Council of Europe (**COE**). Convention 108 opened for signature in 1981 and was the first legally binding instrument in the data protection field.[10] The purpose of Convention 108 is to "protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy".[11] Convention 108 provides for the free flow of personal data between states parties to the Convention.

[9] Accessible at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
[10] COE, 'Convention 108 and protocols: Background', (accessible at https://www.coe.int/en/web/data-protection/convention108/background).
[11] Article 1 of Convention 108.

A key feature of Convention 108 is that, in addition to the members of the COE, it also provides that non-European states may accede to it. For example, in the African context, Cape Verde, Mauritius, and Senegal have all acceded to it. This is of relevance for several reasons: it is a recognition of the adequacy of their data protection frameworks; it adds an additional bulwark of protection for persons within those states, and; it can serve to facilitate cross-border data transfers between those African states and Europe. Convention 108 remains open for accession to other African states that meet the necessary requirements.

**Modernisation of Convention 108**

Source: https://www.coe.int/en/web/data-protection/convention108/modernised

In May 2018, the COE published Convention 108+, in an effort to update and modernise Convention 108 given that it was opened for signature over 35 year previously. The modernisation effort gives new considerations to automated processing, cross-border data flows, and the need to strengthen the Convention's evaluation and follow-up mechanisms.

The second key instrument, the European Union General Data Protection Regulation 2016/679[12] (**GDPR**), is an effort to harmonise all data protection laws across the European Union and has been applicable to all EU member states since 25 May 2018. As explained in article 1 of the GDPR, its purpose is to lay down rules relating to the protection of natural persons with regard to the processing of personal data, as well as rules relating to the free movement of personal data. In particular, article 1(2) makes clear that the GDPR is intended to protect "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".

Chapter II of the GDPR sets out the following principles:

- Article 5: Principles relating to the processing of personal data.
- Article 6: Lawfulness of processing.
- Article 7: Conditions for consent.
- Article 8: Conditions applicable to a child's consent in relation to information society services.
- Article 9: Processing of special categories of personal data.
- Article 10: Processing of personal data relating to criminal convictions and offences.
- Article 11: Processing which does not require identification.

The conditions for consent bear special emphasis. Importantly, the data controller bears the burden of demonstrating that the data subject has consented to the processing of his or her personal data.[13] Where written consent is sought, the GDPR provides that this request for consent "shall be presented in a manner which is clearly distinguishable from the other

[12] Accessible at https://gdpr-info.eu/.
[13] Article 7(1) of the GDPR.

matters, in an intelligible and easily accessible form, using clear and plain language" in order for it to be binding.[14] The data subject has the right to withdraw consent at any time, and it is required that it be made as easy to withdraw consent as it is to give consent.[15] Added to this, the GDPR provides that when assessing whether consent is freely given, utmost account must be taken of whether the performance of a contract or provision of a service "is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".[16]

A unique and notable inclusion in the GDPR is that, per Article 3, it seeks to apply extra-territorially, to data controllers that are not established in the EU, regardless of whether the processing takes place in the EU or not.

Failure to comply with the GDPR carries significant penalties, including administrative fines of up to €20 000 or 4% of the transgressor's total worldwide turnover of the preceding year, whichever is higher.[17]

**Representation of data subjects in terms of the GDPR**

Source: https://gdpr-info.eu/art-80-gdpr/

Article 80 of the GDPR deals with the representation of data subjects. Article 80(1) provides that a data subject has a right to mandate a not-for-profit body, organisation or association – which has been properly constituted within the law of a member state, has statutory objectives in the public interest and is active in the field of data protection – to exercise the data subject's rights on his or her behalf. This opens the door for class action litigation to be brought as a result of an infringement of a provision of the GDPR.

Article 80(2) further gives member states the option to allow anybody, organisation or association referred to in article 80(1) to lodge a complaint independently of a data subject's mandate, if it appears that there has been an infringement of a right as a result of data processing. However, as explained in recital 142, that body, organisation, or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

*Use of data protection authorities to vindicate the right to privacy*

Data protection frameworks typically provide for the establishment of a data protection authority (**DPA**) to oversee and enforce the relevant framework. Such DPAs are typically given a range of powers, including to be notified in the event of a data breach, to adjudicate complaints, and to impose penalties where a data controller is found to be non-compliant with the data protection framework.

[14] Article 7(2) of the GDPR.
[15] Article 7(3) of the GDPR.
[16] Article 7(4) of the GDPR.
[17] Article 83 of the GDPR.

In states with established DPAs, this may be an avenue to vindicate the right to privacy. In the event of a data breach or another infringement of the data protection framework, data subjects may be assisted with lodging complaints to the relevant DPA. This quasi-judicial forum can present a relatively quick and cost-effective remedy for the data subject.

### Data protection litigation in Africa

Because many data protection laws, and accompanying authorities, are relatively new in Africa, and have often faced implementation challenges, there has been limited data protection litigation on the continent to date. However, cases are beginning to appear from various countries, setting a reassuring precedent for the protection of human rights.

- In Ghana, lawyer Francis Kwarteng Arthur filed a suit challenging the government's collection of personal data from mobile phone subscribers. In August 2021, the High Court ruled that the National Communications Authority (NCA) had to stop collecting personal information from mobile phone subscribers and ordered the government to delete data already collected within fourteen days of the judgement.[18]
- In Kenya, a series of successful legal challenges to a new national biometric identity programme known as the Huduma Namba, led to the courts ordering delays and conditions to the programme's rollout. This Module explores the Huduma Namba programme in further detail here.

## Data Retention

### Report of the UN Human Rights Committee regarding data retention in South Africa

Source: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR/C/ZAF/CO/1&Lang=En

The legally mandated retention of communications data in South Africa has been a contentious issue for courts, digital rights advocates, and human rights bodies.

- Section 30(2) of South Africa's Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (**RICA**) obliges telecommunications service providers to retain all communications data for a period of three years. This means that all details of a person's personal telecommunications, up

[18] Kwarteng v Ghana Telecommunications Company and Others, (2021) (accessible at: https://kasapafmonline.com/wp-content/uploads/2021/07/FRANCIS-KWARTENG-ARTHUR-V.-GHANA-TELECOMMUNICATIONS-COMPANY-LTD..pdf).

to three years past, lie in wait for the state to pry into, if the officials convince a judicial officer to authorise access.

- In 2016, in an assessment of South Africa's compliance with the ICCPR, the UN Human Rights Committee raised concern "about the wide scope of the data retention regime under [RICA]", and recommended that South Africa "should refrain from engaging in mass surveillance of private communications without prior judicial authorization and consider revoking or limiting the requirement for mandatory retention of data by third parties."
- In 2022, South Africa's Constitutional Court declared parts of RICA unconstitutional for failing to provide adequate safeguards for the collection of information for surveillance and ordered that it be reformed. While the applicants in *AmaBhungane* did not succeed in convincing the High Court, in an earlier stage of the case, to make a finding on the long period of storage of communication data, the judgment included an order for Parliament to amend the law to build new safeguards for data once it has been collected. This case will be discussed in further detail here.[19]

Data retention is typically described as "the process through which governments and businesses (especially telecommunication and internet providers) record and store various data (usually related to individuals)."[20] As explained by Privacy International:[21]

> "The practice of data retention involves the gathering and storing of communications data for extended periods for the purpose of future access. Metadata tells the story about your data and answers the who, when, what, and how of a specific communication."

While the specific terms and definitions vary, most legal frameworks on data retention relating to communications provide for two categories of information – the 'content' of the communication itself, and information *about* the communication. This second category, often called communication data or communication metadata, includes a wide range of information which is often deeply revealing, such as the identities or identifiers of those involved, the times and durations of their interactions, locational information, and any technology or services involved. While data retention can be important for criminal investigations, it also gives more power to governments to monitor the public and takes away their rights to online privacy.[22] The practice of mandating the retention of communications data raises significant privacy, transparency and security concerns. In turn, this may affect the ways in which people exercise their rights online and poses a risk of leading to self-censorship.

[19] AmaBhungane Centre For Investigative Journalism NPC v President of the Republic of South Africa CCT385/21, (2021) (accessible at: https://www.concourt.org.za/index.php/judgement/483-amabhungane-centre-for-investigative-journalism-npc-v-president-of-the-republic-of-south-africa-cct385-21).
[20] Cactus, 'What is data retention and how does it affect online privacy?', (2018) (accessible at https://www.cactusvpn.com/beginners-guide-to-online-privacy/what-is-data-retention/).
[21] Privacy International, 'National data retention laws since the CJEU's Tele-2 / Watson judgment: A concerning state of play for the right to privacy in Europe', (2017) (accessible at https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf).
[22] Id.

It has been noted that: "Data retention laws are different from country to country, but they ultimately have the same goal: A better grip on the digital world at the expense of privacy and freedom of speech".[23] Privacy International explains that the mass retention of individuals' communications records, outside the context of any criminal investigation or business purpose, "amounts to the compilation of dossiers on each and every one of us, our friends, family and colleagues".[24] Privacy International goes on to explain that:

> "The potential harms associated with data retention and access are significant. In a context where the gathering and exploitation of data by private companies becomes increasingly privacy intrusive and widespread, data retention poses serious risks to individual privacy and data security. The data opens the door for governments and third parties to make intimate inferences about individuals, to engage in profiling and to otherwise intrude on people's private lives. If the information is not properly protected there is the potential of unauthorised access to troves of information by third parties, including cyber-criminals."

Most data protection frameworks provide that data should only be collected for specified, explicit and legitimate purposes and that such data should, in the ordinary course, be deleted when this is no longer the case. Additionally, data ought not to be kept for longer than it is needed. For example, article 5(1)(e) of the GDPR provides that personal data shall be–

> "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes … subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')".

In general, there are two key factors that determine an appropriate data retention period: (i) the purpose for processing the data; and (ii) any legal or regulatory requirements for retaining it. In respect of the latter, various countries have mandatory data retention laws that require telecommunication and internet service providers to retain certain types of data – such as metadata – for stipulated periods of time.

Importantly, there have been at least two significant judgments of the CJEU – *Digital Rights Ireland*[25] and *Tele2 Sverige AB*[26] – that have reaffirmed the requirement that all data retention

[23] Id.
[24] Privacy International, 'Communications data retention', (accessible at https://privacyinternational.org/topics/communications-data-retention).
[25] Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources et al (C-293/12); Kärntner Landesregierung and Others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014).
[26] Tele2 Sverige AB v Post-Och telestyrelsen (C-203/15); Secretary of State for the Home Department v Tom Watson et al (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (2016).

regimes must comply with the principles of legality, necessity and proportionality.[27] Appropriate safeguards are also needed to protect the data that has been retained.

**Indefinite retention of DNA, fingerprints and photograph held to be in breach of privacy rights**

Source: http://hudoc.echr.coe.int/eng-press?i=003-6638275-8815904

The European Court of Human Rights' (**ECtHR**) 2020 judgment of *Gaughran v United Kingdom* (application no. 45245/15) concerned a complaint about the indefinite retention of data (DNA profile, fingerprints and a photograph) of a man who had a spent conviction for driving with excess alcohol.)

- The ECtHR held that there had been a violation of his privacy rights in terms of article 8 of the European Convention on Human Rights (**European Convention**).
- The ECtHR underlined that it was not the duration of the retention of data that had been decisive, but the absence of certain safeguards. In the applicant's case, his personal data had been retained indefinitely without consideration of the seriousness of his offence, the need for indefinite retention, and without any real possibility of review.
- Noting that the technology being used had been shown to be more sophisticated than that considered by the domestic courts in this case, particularly regarding storage and analysis of photographs, the ECtHR considered that the retention of the applicant's data had failed to strike a fair balance between the competing public and private interests.

## Surveillance

*Government-led digital surveillance*

Communications surveillance encompasses the monitoring, intercepting, collecting, analysing, retention, or similar actions, of a person's communications in the past, present, or future.[28] Online surveillance has been a central issue for human rights activists for years, but the Snowden revelations about the extent and scope of global mass surveillance brought new urgency and awareness to the issue and sparked a wave of policy change and jurisprudence in many jurisdictions.

Surveillance constitutes an obvious interference with the right to privacy. Further, it also infringes on the right to hold opinions without interference and the right to freedom of expression. With particular reference to the right to hold opinions without interference,

[27] Privacy International, above n 21 at p 4.
[28] Necessary and proportionate: International principles on the application of human rights to communications surveillance, 2014 (Necessary and Proportionate Principles) at p 4 (accessible at: https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf).

surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, can create a chilling effect by deterring a person from accessing information, particularly where such surveillance leads to repressive outcomes. The knowledge, or even the perception, of being surveilled can lead to self-censorship. Accordingly, emerging jurisprudence on communications surveillance has also often paid special attention to media freedom considerations:

- In *Big Brother Watch and Others v. the United Kingdom (application nos. 58170/13, 62322/14 and 24969/15)* the Grand Chamber of the ECtHR found *inter alia* that the UK's bulk surveillance regime contravened article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms because it did not adequately protect confidential journalistic material from collection and inspection in the course of bulk monitoring of communications data undertaken by UK intelligence agencies.[29]

- In *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* (discussed in further detail below), the High Court of South Africa found that the need of journalists and their sources for confidential communications required special protections against surveillance abuses, remarking that:

  > "In a country that is as wracked by corruption in both our public institutions and in our private institutions as ours is, and where the unearthing of wrongdoing is significantly the work of investigative journalists, in an otherwise, seemingly, empty field, it is hypocritical to both laud the press and ignore their special needs to be an effective prop of the democratic process."[30]

- The Supreme Court of India, in ordering an independent inquiry into allegations that the government deployed the Pegasus spyware against various journalists, politicians and dissidents, similarly found that the free press's democratic function was at stake, and that "such chilling effect on the freedom of speech is an assault on the vital public watchdog role of the press, which may undermine the ability of the press to provide accurate and reliable information."[31]

It has been noted that many frameworks create a legal distinction between communications information that is deemed to be 'content' and information that is *about* the communication (communication data or metadata). This second category is often subject to fewer legal and social protections than information deemed to be 'content'. Yet communication data may give detailed insights into a person's behaviour, social relationships, private preferences and identity – either when analysed in bulk or in some cases in individual parts.[32] In addition, the

[29] Accessible at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}.
[30] Accessible at: http://www.saflii.org/za/cases/ZAGPPHC/2019/384.html
[31] Accessible at: https://main.sci.gov.in/supremecourt/2021/16884/16884_2021_1_1501_30827_Judgement_27-Oct-2021.pdf.
[32] ACLU of California, 'Metadata: Piecing together a privacy solution,' 2014, at p 5 (accessible at: https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf).

two legal distinctions are arbitrary and ill-suited to many types of communication information in the context of the modern digital age, where certain types of data could fall into either legal category.[33]

**United Nations (UN) Resolution on the Right to Privacy in the Digital Age**

Source: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

The 2016 UN Resolution on the Right to Privacy in the Digital Age calls on states to, among other things:

- Review their procedures, practices, and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.
- Establish or maintain existing independent, effective, adequately resourced, and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception, and the collection of personal data.
- Provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations.
- Develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention, or use of personal data by individuals, governments, business enterprises and private organisations.

General Comment No 16 to the ICCPR provides that "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited".[34] In the digital age, Information and Communications Technologies (ICTs) have enhanced the capacity of governments, corporations and individuals to conduct surveillance, interception, and data collection, and have meant that the effectiveness of conducting such surveillance is no longer limited by scale or duration. Surveillance – both bulk (or mass) collection of data or targeted collection of data – interferes directly with the privacy and security necessary for freedom of opinion and expression. As such, in all its forms surveillance must be considered against the three-part test established in international law to assess the permissibility of a restriction on human rights, namely that the limitation is:

[33] Id., at p 3-4.
[34] General Comment No 16 at para 8.

- Provided by law.
- Pursues a legitimate aim.
- Necessary and proportionate to achieving the aim.

In order to meet the condition of legality, many states have taken steps to reform their surveillance laws to allow for the powers required to conduct surveillance activities. For instance, in the judgment of *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*, the Constitutional Court of South Africa upheld a ruling of the High Court that the exercise of bulk surveillance in South Africa was unlawful because of the absence of any empowering legal framework to authorise such surveillance to take place.[35]

*Necessary and proportionate*

The Necessary and Proportionate Principles are a set of 13 international principles on the application of human rights to communications surveillance, especially in the context of the ever-advancing mass surveillance capabilities shown by states and private-sector operators in the modern digital era.[36] The principles advise among other things that all powers of communications surveillance must be prescribed and regulated by law, be necessary and proportionate and pursue a legitimate aim, and be subject to certain safeguards, including that the powers are subject to a competent judicial authority, and necessary transparency and public oversight measures.

Principle 3 establishes *necessity*, explaining that surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. As such, surveillance should only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification rests on the state.

Principle 5 establishes *proportionality*: surveillance should be regarded as a highly intrusive act, and in order to meet the threshold of proportionality, the state should be required at a minimum to establish the following information to a competent judicial authority prior to conducting any communications surveillance:[37]

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

[35] Accessible at http://www.saflii.org/za/cases/ZACC/2021/3.html.
[36] Accessible at https://necessaryandproportionate.org/principles. The Necessary and Proportionate Principles were drafted by Access Now, the Electronic Freedom Foundation and Privacy International, and launched at the UN Human Rights Council in 2013. It has since been endorsed by more than 400 organisations around the world.
[37] Principle 5 of the Necessary and Proportionate Principles.

- Information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a legitimate aim alleged.
- Any excess information collected will not be retained but instead will be promptly destroyed or returned.
- Information will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.
- The surveillance activities requested, and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.

**African Declaration on Internet Rights and Freedoms**

Source: https://africaninternetrights.org/articles/

Principle 9 of the African Declaration on Internet Rights and Freedoms (**AfDec**) – a civil-society-led initiative that has been endorsed by the African Commission on Human and Peoples' Rights – provides that "[u]nlawful surveillance, monitoring and interception of users' online communications by state or non-state actors fundamentally undermine the security and trustworthiness of the Internet." The AfDec goes on to explain that:

- Mass or indiscriminate surveillance of individuals or the monitoring of their communications, constitutes a disproportionate interference, and thus a violation, of the right to privacy, freedom of expression and other human rights, and shall be prohibited by law.
- The collection, interception and retention of communications data amounts to an interference with the right to privacy and freedom of expression whether or not the data is subsequently examined or used.
- Targeted surveillance of online communications must be governed by clear and transparent laws which comply with the following basic principles:
  - Communications surveillance must be both targeted and based on reasonable suspicion of commission or involvement in the commission of serious crime;
  - Communications surveillance must be judicially authorised and individuals placed under surveillance must be notified that their communications have been monitored as soon as practicable after the conclusion of the surveillance operation
  - The application of surveillance laws must be subject to strong parliamentary oversight to prevent abuse and ensure the accountability of intelligence services and law enforcement agencies.
- Individuals must be protected from unlawful surveillance by other individuals, private entities or institutions, including in their place of work or study and in public internet access points.

*Safeguards and oversight*

Privacy International sets out the following ten safeguards that should be implemented for any government hacking or surveillance regime:[38]

- **Legality**: Government hacking powers must be explicitly prescribed by law and limited to those strictly and demonstrably necessary to achieve a legitimate aim. That law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the interference. It should be subject to periodic review by means of a participatory legislative process.

- **Security and integrity of systems**: Prior to carrying out a hacking measure, government authorities must assess the potential risks and damage to the security and integrity of the target system and systems generally, as well as of data on the target system and systems generally, and how those risks and/or damage will be mitigated or corrected. Government authorities must include this assessment in any application in support of a proposed hacking measure. Government authorities must not compel hardware or software manufacturers or service providers to facilitate government hacking, including by compromising the security and integrity of their products and services.

- **Necessity and proportionality**: Prior to carrying out a hacking measure, government authorities must, at a minimum, establish a high degree of probability that: (i) serious crime or act(s) amounting to a specific, serious threat to national security has been or will be carried out; (ii) the system used by the person suspected of committing the serious crime or act(s) amounting to a specific, serious threat to national security contains evidence relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security interest alleged; and (iii) evidence relevant and material to the serious crime or act(s) amounting to a specific, serious threat to national security alleged will be obtained by hacking the target system.

- **Judicial authorisation**: Prior to carrying out a hacking measure, government authorities must make an application, setting forth the necessity and proportionality of the proposed measure to an impartial and independent judicial authority, who shall determine whether to approve such measure and oversee its implementation. The judicial authority must be able to consult persons with technical expertise in the relevant technologies, who may assist the judicial authority in understanding how the proposed measure will affect the target system and systems generally, as well as data on the target system and systems generally. The judicial authority must also be able to consult persons with expertise in privacy and human rights, who may assist the judicial authority in understanding how the proposed measure will interfere with the rights of the target person and other persons.

[38] Privacy International, 'Government hacking and surveillance: 10 necessary safeguards', (accessible at https://privacyinternational.org/type-resource/necessary-hacking-safeguards).

- **Integrity of information**: Government authorities must not add, alter or delete data on the target system, except to the extent technically necessary to carry out the authorised hacking measure. They must maintain an independently verifiable audit trail to record their hacking activities, including any necessary additions, alterations or deletions. Where government authorities rely on data obtained through an authorised hacking measure, they must disclose the method, extent and duration of the hacking measure and their audit trail so that the target person can understand the nature of the data obtained and investigate additions, alterations or deletions to information or breaches of the chain of custody, as appropriate.

- **Notification**: Government authorities must notify the person(s) whose system(s) have been subject to interference pursuant to an authorised hacking measure, regardless of where the person(s) reside, that the authorities have interfered with such system(s). Government authorities must also notify affected software and hardware manufacturers and service providers, with details regarding the method, extent and duration of the hacking measure, including the specific configurations of the target system. Delay in notification is only justified where notification would seriously jeopardise the purpose for which the hacking measure was authorised or there is an imminent risk of danger to human life and authorisation to delay notification is granted by an impartial and independent judicial authority.

- **Destruction and return of data**: Government authorities must immediately destroy any irrelevant or immaterial data that is obtained pursuant to an authorised hacking measure. That destruction must be recorded in the independently verifiable audit trail of hacking activities. After government authorities have used data obtained through an authorised hacking measure for the purpose for which authorisation was given, they must return this data to the target person and destroy any other copies of the data.

- **Oversight and transparency**: Government authorities must be transparent about the scope and use of their hacking powers and activities and subject those powers and activities to independent oversight. They should regularly publish, at a minimum, information on the number of applications to authorise hacking approved and rejected; the identity of the applying government authorities; the offences specified in the applications; and the method, extent and duration of authorised hacking measures, including the specific configurations of target systems.

- **Extraterritoriality**: When conducting an extraterritorial hacking measure, government authorities must always comply with their international legal obligations, including the principles of sovereignty and non-intervention, which express limitations on the exercise of extraterritorial jurisdiction. Government authorities must not use hacking to circumvent other legal mechanisms – such as mutual legal assistance treaties or other consent-based mechanisms – for obtaining data located outside their territory. These mechanisms must be clearly documented, publicly available, and subject to guarantees of procedural and substantive fairness.

- **Effective remedy**: Persons who have been subject to unlawful government hacking, regardless of where they reside, must have access to an effective remedy.

**Impugned provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (RICA) declared unconstitutional**

Source: http://www.saflii.org/za/cases/ZACC/2021/3.html

In the case of *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*, the Constitutional Court of South Africa considered a challenge to South Africa's interception law, RICA, brought by an investigative journalism outfit whose co-founder had been subject to communications surveillance by the intelligence services. The Court declared various provisions of RICA to be unconstitutional, on the grounds that the law:

- Fails to provide safeguards to ensure the independence of a judge designated to oversee interception requests;
- Fails to provide for "post-surveillance notification" of people whose communications are intercepted.
- Does not adequately provide safeguards to address the fact that interception directions are sought and obtained *ex parte* (i.e. necessarily without the knowledge and participation of the person whose communications would be intercepted);
- Does not detail procedures to ensure that data obtained in the interception of communications is managed lawfully, including steps to be followed for examining, sharing, storing, or destroying the data; and
- Does not provide adequate safeguards where the subject of surveillance is a practising lawyer or journalist. For example, RICA fails to prescribe an appointment mechanism and terms for a designated judge (any judge mandated to oversee interception requests), which ensures the judge's independence.

The Constitutional Court also upheld an order of the High Court that bulk surveillance activities and foreign signals interception undertaken by the South African government were unlawful and invalid, in that they were not subject to any enabling law.

*Covert recordings*

There are various domestic laws and international standards that require that individuals be notified of covert recordings, including video surveillance.[39] However, there is no consistent position on this issue. There are two key recent decisions of the Grand Chamber of the ECtHR that are relevant in this regard:[40]

[39] International Justice Resource Centre, 'European Court holds secret surveillance did not violate employees' privacy', (2019) (accessible at https://ijrcenter.org/2019/10/24/european-court-holds-secret-surveillance-did-not-violate-employees-privacy/).
[40] ECtHR Press Unit, 'Surveillance at workplace', (accessible at https://echr.coe.int/Documents/FS_Workplace_surveillance_ENG.pdf).

- *Antović and Mirković v Montenegro:*[41] This case concerned an invasion of privacy complaint by two professors at the University of Montenegro's School of Mathematics after video surveillance had been installed in areas where they taught. They stated that they had no effective control over the information collected and that the surveillance had been unlawful. The domestic courts rejected a compensation claim, finding that the question of private life had not been at issue as the auditoriums where the applicants taught were public areas. The ECtHR made the following findings:
    - It held that there had been a violation of article 8 of the European Convention, finding that the camera surveillance had not been in accordance with the law.
    - The ECtHR rejected the government's argument that the case was inadmissible because no privacy issue had been at stake as the area under surveillance had been a public, working area, noting that it had previously found that private life might include professional activities and considered this to apply to the applicants' situation. Article 8 of the European Convention was therefore applicable.
    - On the merits of the case, the ECtHR found that the camera surveillance had amounted to an interference with the applicants' right to privacy and that the evidence showed that the surveillance had violated the provisions of domestic law. According to the ECtHR, the domestic courts had not considered any legal justification for the surveillance because they had decided from the outset that there had been no invasion of privacy.

- *Ribalda and Others v Spain:*[42] This case concerned covert video surveillance of a group of employees at a supermarket, which led to their dismissal. The applicants complained about the covert video surveillance and about the Spanish courts' use of the footage to find that their dismissals had been fair. Several applicants who had signed settlement agreements also complained that the agreements had been made under duress owing to the video material and should not have been accepted as evidence that their dismissals had been fair. The Grand Chamber made the following findings:
    - It held that there had been no violation of article 8 of the European Convention in respect of the five applicants. It found in particular that the Spanish courts had carefully balanced the rights of the applicants – who had been suspected of theft by their employer – and those of the employer and thoroughly examined the justification for the video surveillance.
    - A key argument by the applicants was that they had not been given prior notice of the surveillance, despite such a legal requirement, but the ECtHR found that the measure was justified owing to a reasonable suspicion of serious misconduct and to the losses involved, taking account of the extent and the consequences of the measure.
    - The ECtHR concluded that, in the present case, the domestic courts had not exceeded their power of discretion or margin of appreciation in finding that the covert video surveillance was proportionate and legitimate.

In respect of the media, considerations of public interest and the public status of individuals are key in determining whether information should be published. This was affirmed, for

[41] Application No. 70838/13, (2017) (accessible at http://hudoc.echr.coe.int/eng?i=001-178904).
[42] Application Nos. 1874/13 and 8567/13, (2019) (accessible at http://hudoc.echr.coe.int/fre?i=001-197098).

instance, in *Radio Twist v Slovakia*,[43] where the ECtHR had cause to consider the unlawful recording of a telephone call that had been broadcast on the radio. The recording was of a conversation among several senior government officials about the privatisation of an insurance company. The recording had been shared anonymously with the radio station. The ECtHR had particular regard to the context and content of the conversation being clearly political in nature, and the subject matter of the conversation being of general interest.[44] As to whether the recording was illegal, the ECtHR stated that it was not convinced that the mere fact that the recording had been obtained by a third party contrary to the law justified the applicant's being deprived of its right to freedom of expression.[45] The ECtHR, therefore, held that the radio station had not violated the rights of the persons who were recorded.

Principle 12(a) of the Global Principles lists the following factors to consider in balancing the rights to freedom of expression and privacy, in situations concerning the publication of personal information:

- The extent to which the publication contributes to a debate of public interest; the degree of notoriety or vulnerability of the person affected;
- The subject covered by the publication and the extent of the private nature of the information at issue;
- The prior conduct of the person concerned;
- The content, form, and consequences of the publication;
- The way in which the information was obtained;
- The intent of the individual or entity disseminating the information at issue, and in particular whether it was malicious; and
- The extent to which the individual whose privacy is at issue is a public figure.[46]

Furthermore, Principle 12 provides that when dealing with the publication of photographs, video footage, or sound recordings, there should be consideration of whether the recording was made voluntarily and with consent. The use of privacy-invasive techniques, such as hidden cameras or undercover reporting, should only be permitted where there is an overriding public interest in the dissemination of the information sought or discovered which could not have been obtained by less invasive means, and where efforts have been made to address or minimise any privacy implications.[47]

[43] Application No. 62202/00, (2005) (accessible at http://hudoc.echr.coe.int/eng?i=001-71431).
[44] Id. at para 58.
[45] Id. at para 62.
[46] ARTICLE 19, 'Global principles on freedom of expression and privacy: A policy brief', (2017) (accessible at: https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf).
[47] Principle 12(c) of the Global Principles of Freedom of Expression and Privacy.

## Collection of Biometric Data and Facial Recognition

### Collection of biometric data for the National Integrated Identity Management System (NIIMS) in Kenya

Source: Privacy International, 'Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba', accessible at https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma

The collection and retention of biometric data present a unique set of privacy concerns. As biometric data can remain relevant for the course of a person's life, the security of this data is paramount. Biometric data breaches can result in serious harm to people's rights and interests, including identity theft or fraud, financial loss or other damage.

In January 2020, the High Court of Kenya handed down judgment on the validity of the National Integrated Identity Management System (NIIMS), also known as the Huduma Namba, a national identity registration programme which includes the collection of biometric information. The court ruled that the rollout of NIIMS should not continue without further legislation to guarantee the security of biometric data and to ensure that the system is not exclusionary.

In a subsequent ruling in October 2021, the High Court again halted the NIIMS rollout, albeit temporarily, when it ordered that the programme must be subject to a data impact assessment in terms of Kenya's Data Protection Act.

Facial recognition is a form of biometric system that attracts particular concern for its use in surveillance.[48] Facial recognition technology refers to a wide range of software that can be linked to camera networks; the software analyses live or recorded images and footage of people from a camera network and matches these against images in a pre-existing database in order to identify specific people from the footage.[49] As noted by Privacy International, facial recognition cameras are far more intrusive than regular CCTV: they scan distinct, specific features of your face, such as face shape, to create a detailed map of it – "which means that being captured by these cameras is like being fingerprinted, without your knowledge or consent".[50]

[48] American Civil Liberties Union, 'Face recognition technology', (accessible at https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology).
[49] Privacy International 'Facial recognition', (accessible at https://privacyinternational.org/long-read/2726/police-are-increasingly-using-facial-recognition-cameras-public-spy-us).
[50] Id.

**Facial recognition in practice in the United Kingdom**

Source: Privacy International, 'Catt v The United Kingdom', 2016, accessible at https://privacyinternational.org/legal-action/catt-v-united-kingdom

The growing use of facial recognition by police in the United Kingdom has attracted several notable legal challenges.

In 2019, in *Catt v the United Kingdom*, the European Court of Human Rights found that the UK government had violated the right to privacy in the course of monitoring and profiling a peace activist. In a third-party intervention, Privacy International drew the court's attention to the potential digital technology such as facial recognition to increase any such violation of the right to privacy. The Court noted that the potential for such emerging technologies to violate human rights requires examination "where the powers vested in the state are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated".

In *Bridges v CC South Wales & others,* British civil liberties organisation Liberty acted in a legal challenge against the use of facial recognition technology by police in South Wales. In 2020, the UK Court of Appeal overturned an earlier ruling by finding that the police's use of facial recognition technology breaches privacy rights, data protection laws, and equality laws and that there were "fundamental deficiencies" in the legal framework governing its use.[51]

In this regard, unlike many other biometric systems, facial recognition can be used for general surveillance in combination with public video cameras, and it can be used in a passive way that doesn't require the knowledge, consent, or participation of the subject.[52] As noted by the American Civil Liberties Union, this creates the risk for the technology to be used for general surveillance of a population that is not suspected of any specific wrongdoing. For example, most motor vehicle agencies have high-quality photographs of large numbers of people, which can be a natural source for facial recognition programmes and could easily be combined with public or private surveillance camera networks to create a comprehensive system of identification and tracking. Law enforcement agencies also regularly use photographs scraped from social media sites as well.

Interpol has described computerised facial recognition as a relatively new technology which was introduced by law enforcement agencies around the world to identify persons of interest, including criminals, fugitives and missing persons.[53] The Interpol Facial Recognition System

[51] Liberty, 'Liberty Wins Ground-Breaking Victory Against Facial Recognition Tech,' (2020) (accessible at: https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/).
[52] American Civil Liberties Union, 'Face recognition technology', (accessible at https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology).
[53] Interpol, 'Facial recognition', (accessible at https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition).

contains facial images received from more than 160 countries, and coupled with an automatic biometric software application, the system is capable of identifying or verifying a person by comparing and analysing patterns, shapes and proportions of their facial features.[54] Unlike fingerprints and DNA, which do not change during a person's life, facial recognition has to take into account different factors, such as ageing, plastic surgery, cosmetics, the effects of drug abuse or smoking, and the physical pose of the subject.[55]

However, facial recognition technology has also been linked to inaccuracies and biases which raise serious discrimination concerns. A study commissioned by a public agency in the United States found "empirical evidence" that most widely used facial recognition algorithms exhibit "demographic differentials that can worsen their accuracy based on a person's age, gender, or race.[56] Some of the specific findings included the following:[57]

- Facial-recognition systems misidentified people of colour more often than white people. Asian and African American people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search.
- The faces of African American women were falsely identified more often in the kinds of searches used by police investigators, where an image is compared to thousands or millions of others in hopes of identifying a suspect.
- Women were more likely to be falsely identified than men, and the elderly and children were more likely to be misidentified than those in other age groups.

Privacy International notes that the use of facial recognition technology impacts the exercise of at least the following rights:[58]

- **Privacy**: According to Privacy International, "[t]he use of facial recognition in public spaces makes a mockery of our privacy rights". It is a disproportionate crime-fighting technique, as it scans the face of every person who passes by the camera, whether or not they are suspected of any wrongdoing. The biometric data that it collects can be as uniquely identifying as DNA or a fingerprint and is typically done without the consent or knowledge of the data subject.

- **Freedom of expression**: Being watched and identified in public spaces is likely to lead us to change our behaviour, limiting where we go, what we do and with whom we engage. For example, persons might be unwilling to participate in a particular protest action if facial recognition is being used in the area.

[54] Id.
[55] Id.
[56] Washington Post, 'Federal study confirms racial bias of many facial recognition systems, casts doubts on their expanding use', (2019) (accessible at https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/).
[57] Id.
[58] Privacy International 'Facial recognition', (accessible at https://privacyinternational.org/long-read/2726/police-are-increasingly-using-facial-recognition-cameras-public-spy-us).

- **Equality and non-discrimination**: It has been found that facial recognition software is more likely to misidentify women and black people. There are also concerns that the police use facial recognition to target particular communities.

The roll-out of facial recognition technology is often done without any empowering legal framework to authorise it and is arguably a disproportionate limitation on the right to privacy and other associated rights. In this regard, potential litigation to challenge the use of facial recognition technology may seek to show that it does not meet the threshold of the three-part test for a justifiable limitation, even when used for security purposes.

## Encryption and Anonymity on the Internet

*The interplay between encryption and anonymity*

Encryption and anonymity are necessary tools for the full enjoyment of digital rights and enjoy protection by virtue of their critical role in securing the rights to freedom of expression and privacy. As described by the United Nations Special Rapporteur (**UNSR**) on Freedom of Expression:[59]

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

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

[59] Report of the UNSR on Freedom of Expression, 'Report on anonymity, encryption and the human rights framework', A/HRC/29/32, 22 May 2015 (**UNSR Report on Anonymity and Encryption**) at para 12 (accessible at http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx).

According to the UNSR on Freedom of Expression, while encryption and anonymity may frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public justification to support any relevant restrictions or to identify situations where the restriction has been necessary to achieve a legitimate goal.[60] The UNSR on Freedom of Expression has therefore called on states to promote strong encryption and anonymity and noted that decryption orders should only be permissible when they result from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (not to a mass of people), and subject to a judicial warrant and the protection of due process rights.[61]

*Encryption*

Encryption refers to a mathematical process of converting messages, information or data into a form unreadable by anyone except the intended recipient, which in doing so protects the confidentiality and integrity of content against third-party access or manipulation.[62] With "public key encryption" – the dominant form of end-to-end security for data in transit – the sender uses the recipient's public key to encrypt the message and its attachments, and the recipient uses her or his own private key to decrypt them.[63] It is also possible to encrypt data at rest that is stored on one's device, such as a laptop or hard drive.[64]

Outright prohibitions on the individual use of encryption technology disproportionately restrict the right to freedom of expression as it deprives all online users in a particular jurisdiction of the right to carve out a safe space for opinion and expression.[65] Likewise, state regulation of encryption may be tantamount to a ban, for example through requiring licences for encryption use, setting weak technical standards for encryption or controlling the import and export of encryption tools.[66]

[60] Id at para 36.
[61] Id. at paras 59-60.
[62] Id at para 7.
[63] Id.
[64] Id.
[65] Id at para 40.
[66] Id at para 41.

**Requirements for cryptography providers in terms of the Electronic Communications and Transactions Act, 2002**

Source: https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf

Chapter V of the South African Electronic Communications and Transactions Act, 2002 (ECTA) sets out the requirements for cryptography providers. Section 29 of ECTA provides for the establishment and maintenance of a register of cryptography providers, as well as the particulars that must be recorded in the register, including the name and address of the cryptography provider, as well as a description of the type of cryptography service or product being provided. Section 29(3) provides that a cryptography provider "is not required to disclose confidential information or trade secrets in respect of its cryptography products or services."

It should further be noted that some states have implemented – or proposed implementing – so-called 'back door access' in commercially available products, forcing developers to install weaknesses that allow government authorities access to encrypted communications. While the states supporting such measures typically claim that such a framework is necessary to intercept the content of encrypted communications, the UNSR on Freedom of Expression notes that such states have failed to demonstrate that criminal or terrorist use of encryption serves an insuperable barrier to law enforcement objectives.[67] Creating an intentional mechanism to allow a state to bypass security measures would inevitably undermine the security of all users online, with respect to both state and non-state actors.[68]

Further, there is a key role for encryption to play in data protection. It has been noted that companies can reduce both the probability and the harm of a data breach, and thus reduce the risk of fines in the future if they choose to encrypt any personal data in their possession.[69]

**Encryption and the GDPR**

Source: Intersoft Consulting, 'GDPR: Encryption', accessible at https://gdpr-info.eu/issues/encryption/

The GDPR, and many of the data protection laws which follow its model, place responsibility on data controllers and processors to ensure adequate security and protection when processing personal data, which speaks to the role of encryption in data protection. As outlined in an industry advisory:

> "The GDPR deliberately does not define which specific technical and organisational measures are considered suitable in each case, in order to

[67] Id at para 42.
[68] Id.
[69] Intersoft Consulting, 'GDPR: Encryption', (accessible at https://gdpr-info.eu/issues/encryption/).

> accommodate individual factors. However, it gives the controller a catalogue of criteria to be considered when choosing methods to secure personal data. Those are the state of the art, implementation costs and the nature, scope, context and purposes of the processing. In addition to these criteria, one always has to consider the severity of the risks to the rights and freedoms of the data subject and how likely those risks could manifest. This basically boils down to the following: The higher the risks involved in the data processing and the more likely these are to manifest, the stronger the taken security measures have to be and the more measures must be taken. Encryption as a concept is explicitly mentioned as one possible technical and organisational measure to secure data in the list of Art. 32(1) of the GDPR, which is not exhaustive. Again, the GDPR does not mention explicit encryption methods to accommodate for the fast-paced technological progress."

Encryption of personal data has additional benefits for controllers or processors; for example, the loss of a state-of-the-art encrypted mobile storage medium which holds personal data may not necessarily be considered a data breach that must be reported to the DPA.[70] In addition, if there is a data breach, the authorities must positively consider the use of encryption in their decision on whether and what amount of a fine is imposed as per article 83(2)(c) of the GDPR.[71]

In 2018, the DPAs of the EU, represented in the Article 29 Working Party (**WP29**), published a statement framing strong and efficient encryption as a vital tool for upholding data protection and privacy rights,[72] noting three key points:

- **Strong encryption ensures a secure, free flow of data between citizens, businesses and governments:** The WP29 noted that there is a strong public interest in the implementation of encryption, as it is crucial to ensure a reasonable guarantee that everyday activities – like buying goods online, filing taxes, using banking services, sending or receiving emails or making an appointment with a physician – can be done securely. The WP29 described encryption as "absolutely necessary and irreplaceable for guaranteeing strong confidentiality and integrity when data are transferred across open networks like the Internet or stored in mobile devices like smartphones". According to the WP29, encryption should ideally always cover the entire communication, from the device of the sender to that of the recipient, commonly referred to as end-to-end-encryption.

- **Backdoors and master keys deprive encryption of its utility:** The WP29 countered the argument that law enforcement should be able to access the encrypted data of suspected criminals by requiring technology providers to implement 'back doors' (i.e. security vulnerabilities deliberately built into a particular software) or 'master keys' (i.e. design features to enable the central decryption of all data encrypted with specific

[70] Id.
[71] Id.
[72] WP29, 'Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU', (2018) (accessible at https://www.aepd.es/sites/default/files/2019-09/art29-statement.pdf).

software) in encryption software. The WP29 argued that there is significant historical evidence that master keys and backdoors cannot be kept secure and that there is no way for these technological features to be implemented at any scale without significant risks of compromising people's security. The WP29 also raises concerns that imposing backdoors and master keys on the general population would not be an effective measure against criminals, as criminals would use or adapt to the state-of-the-art encryption to protect their data, which in turn would only harm 'the honest citizen' by making their data vulnerable.

- **Law enforcement agencies already have legal powers and targeted tools to address the challenge of encryption:** According to the WP29, law enforcement agencies can be legally empowered in other ways to obtain access to data otherwise encrypted, including personal data, for investigations in targeted circumstances. While these powers may raise serious privacy concerns in themselves, the WP29 argues that they appear more proportionate and less dangerous than backdoors or master keys.

Based on the above, the WP29 concluded that encryption must remain standardised, strong and efficient, and encryption providers should never be compelled to include master keys and backdoors in their software.

**Advice on how to implement encryption**

Source: Information Commissioner's Office (**ICO**), 'Encryption', accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/

The ICO recommends the following measures when implementing encryption:

- When implementing encryption, it is important to consider four things: choosing the right algorithm, choosing the right key size, choosing the right software, and keeping the key secure.
- Over time, vulnerabilities may be discovered in encryption algorithms that can eventually make them insecure. You should regularly assess whether your encryption method remains appropriate.
- It is important to ensure that the key size is sufficiently large to protect against an attack over the lifetime of the data. You should therefore assess whether your key sizes remain appropriate.
- The encryption software you use is also crucial. You should ensure that any solution you implement meets current standards, such as FIPS 140-2 and FIPS 197.
- Advice on appropriate encryption solutions is available from a number of organisations.

*Anonymity*

In digital contexts, anonymity can be defined either as acting or communicating without using or presenting one's name or identity, as acting or communicating in a way that protects the determination of one's name or identity, or using an invented or assumed name that may not necessarily be associated with one's legal or customary identity.[73] Anonymity may be distinguished from pseudo-anonymity: the former refers to taking no name at all, while the latter refers to taking an assumed name.[74]

Anonymity has been recognised for the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation, and debate. As explained by the American Civil Liberties Union (**ACLU**):[75]

> "The right to remain anonymous is a fundamental component of our right to free speech, and it applies every bit as much in the digital world as it does in the physical one. In the words of the U.S. Supreme Court in *McIntyre v. Ohio Elections Commission*, "Anonymity is a shield from the tyranny of the majority."
>
> Unfortunately, the right to remain anonymous has been under steady attack in the online world. Governments and corporations have attempted to unmask unpopular speakers through subpoenas directed at the websites they visit."

**Anonymity as an enabler of fundamental rights**

Source: Association for Progressive Communications (**APC**), 'The right to freedom of expression and the use of encryption and anonymity in digital communications', February 2015, accessible at https://www.apc.org/sites/default/files/APC%20submission%20to%20SR%20FOEX_20150211_0.pdf

> "Anonymity is also inextricably linked to the right to privacy. An individual cannot have a reasonable expectation that his or her privacy is being protected without the ability to control what information is shared about them and how that information is used. Lack of privacy, or even perceived lack of privacy, is understood to have a chilling effect on freedom of expression, leading to self-censorship.
> …
> Additionally, anonymity is an important enabler of the right to freedom of association and assembly online and the right to be free from discrimination. The relative anonymity that the internet offers enables individuals and minority groups, among others, to associate on sensitive matters such as sexual orientation or

[73] Electronic Frontier Foundation, Anonymity and encryption, (2015) at p 3 (accessible at: http://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf).
[74] Id.
[75] ACLU, 'Online anonymity and identity', (accessible at https://www.aclu.org/issues/free-speech/internet-speech/online-anonymity-and-identity).

> religion. Anonymity provides an enabling environment for people to form relationships and seek support for problems that have a social stigma like drug addiction, illnesses such as HIV/AIDS, or sexual abuse. It also allows people to engage in online association based on identities or beliefs that are illegal in some countries, like LGBT groups, political opposition, or religious minorities".

A number of courts have protected anonymity, both of individual users and of journalistic sources. However, there are also a number of states that prohibit or interfere with anonymity online. In Brazil, for example, anonymity is prohibited by article 5 of the Federal Constitution, which states that "free expression of thought is assured, prohibiting anonymity," without specifying in which situations this should apply.[76] Although this restriction was designed to prevent individuals from offending and causing damage to the honour and image of third parties, without leaving any trace for identification, it has generated confusion and been used to limit the right to privacy and freedom of expression online and offline.[77]

Mandatory SIM card registration is a widespread policy that requires real-name registration for online activity.[78] Mandatory SIM card registration laws typically require that people link their identity to their SIM card in order to activate it, by providing personal information such as a valid identity document, proof of address or biometrics, when purchasing a SIM card for a mobile device.[79] As noted by Privacy International, "[p]repaid SIM card use and mandatory SIM card registration laws are especially widespread in African countries: these two factors can allow for a more pervasive system of mass surveillance of people who can access pre-paid SIM cards, as well as exclusion from important civic spaces, social networks, and education and health care for people who cannot."[80]

Mandatory SIM card registration severely undermines the ability to be anonymous online. It has been explained that: "If almost every mobile device has its SIM card registered to a particular person, and the government can get access to that mobile subscriber information, the people who own and use such devices can be more easily tracked and monitored. Not all people with mobile devices may fall equally under the watchful eye of such surveillance systems: people advocating for change, people who disagree with the government's policies, religious or ethnic minorities, journalists, and human rights defenders are particularly vulnerable."[81]

---

[76] APC, 'The right to freedom of expression and the use of encryption and anonymity in digital communications', (2015) (accessible at https://www.apc.org/sites/default/files/APC%20submission%20to%20SR%20FOEX_20150211_0.pdf) .

[77] Id.

[78] Id at paras 49-52.

[79] Privacy International, 'Africa: SIM card registration only increases monitoring and exclusion', (2019) (accessible at https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion).

[80] Id.

[81] Id.

As of 2022, at least 51 countries in Africa had introduced laws or regulations mandating SIM card registration,[82] with Lesotho and Namibia beginning rollouts in 2022.[83] Among African states, Cabo Verde and Comoros were reported not to be considering SIM registration policies, while the situation in Djibouti was inconclusive.[84]

Anonymity is especially critical in repressive environments in which certain types of protected expression are outlawed, and a lack of anonymity could lead to criminal charges or other consequences.[85] Attempts to ban anonymous speech have particularly been seen during times of protest as a measure aimed at protestors and activists.[86]

Intermediary liability is again of concern in relation to anonymous users, as some states have moved towards imposing responsibilities on internet service providers (ISPs) and media platforms to regulate online comments by anonymous users. For instance, in *Delfi v Estonia*, the ECtHR upheld an Estonian law that imposes liability on a media platform for anonymous defamatory statements posted on its site.[87] However, the ECtHR has also upheld that, while there is no absolute guarantee of online anonymity, the right of freedom of expression should be taken into consideration in decisions to revoke anonymity. This informed the ECtHR's 2021 finding that an Austrian news site should not have been forced to disclose the identity of online commenters who had posted offensive and hateful messages to the platform.[88] In its third-party submissions in that case, Media Defence had previously argued that a court should only order an ISP to disclose user data where:[89]

- An applicant is able to demonstrate to a sufficient degree that a wrongful act has been committed against them, and that the information is sought to enable them to seek redress for that wrongful act;
- The anonymous user has been notified, and has had an opportunity to respond to the application;
- There is no less restrictive means of obtaining the information sought; and
- The applicant's interest in disclosure has been sufficiently balanced against the rights to freedom of expression and privacy.

---

[82] GSMA, 'Access to Mobile Services and Proof of Identity 2021', (2021) (accessible at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf).
[83] BiometricsUpdate.com, 'Lesotho, Namibia join trend of SIM card registration with biometrics' (2022) (accessible at https://www.biometricupdate.com/202207/lesotho-namibia-join-trend-of-sim-card-registration-with-biometrics).
[84] GSMA, above n 82, at p 54.
[85] APC, 'The right to freedom of expression and the use of encryption and anonymity in digital communications', (2015) (accessible at https://www.apc.org/sites/default/files/APC%20submission%20to%20SR%20FOEX_20150211_0.pdf).
[86] Id. at para 53.
[87] Application No. 64569/09. (2015) (accessible at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-155105%22]}).
[88] Application No. 39378/15, (2022) (accessible at https://hudoc.echr.coe.int/eng#{%22appno%22:[%2239378/15%22]}).
[89] See MLDI's third party intervener submissions in Standard Verlagsgesellschaft MbH, Application No. 39378, (accessible at https://www.mediadefence.org/news/mldi-files-intervention-at-european-court-seeking-to-protect-anonymity-of-users-online/).

## Source Protection and the Protection of Journalistic Materials

The confidentiality of journalistic sources is central to journalists' ability to properly investigate stories, and to the protection of individuals and whistleblowers who provide information to them.[90] Efforts to compel the disclosure of sources have a chilling effect on freedom of speech and media freedom and hinder the free flow of information.[91]

In this regard, General Comment No. 34 to the ICCPR provides that states parties "should recognise and respect that element of the right of freedom of expression that embraces the limited journalistic privilege not to disclose sources." Furthermore, the Africa Commission on Human and Peoples' Rights issued the Declaration of Principles on Freedom of Expression in Africa in 2019, which deals with the issue of protection of sources by providing as follows:

> "Journalists and other media practitioners shall not be required to reveal confidential sources of information or to disclose other material held for journalistic purposes except where disclosure has been ordered by a court after a full and fair public hearing."[92]

The Declaration emphasises that this should only take place where the identity of the source is necessary for the investigation or prosecution of a serious crime, where the information can't be obtained from elsewhere, and whether the public interest in disclosure outweighs the harm to freedom of expression.

It is important to note that the protection of sources has acquired new significance in the digital age in the context of the right to privacy of communications,[93] as surveillance technologies whose development is justified in terms of national security can be used to target journalists and their confidential sources.[94] The Secretary-General of the UN has noted that surveillance activities can have a chilling effect on media freedom and make it more difficult for journalists to communicate with sources and share and develop ideas, which may lead to self-censorship.[95] Similarly, a UN General Assembly resolution on the safety of journalists emphasised that journalists in the digital age are particularly vulnerable to becoming targets of unlawful or arbitrary surveillance, in violation of their rights to privacy and freedom of expression.[96] The resolution further noted that encryption and anonymity tools have become vital to journalists to secure their communications and protect the confidentiality of their sources.

---

[90] UNESCO, 'Legal standards on freedom of expression: Toolkit for the judiciary in Africa', (2018) at p 123 (accessible at https://unesdoc.unesco.org/ark:/48223/pf0000366340).
[91] Id.
[92] ACHPR, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa,' 2019 at Principle 25, (accessible at: https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf).
[93] Id at p 124.
[94] Id at p 124.
[95] Report of the Secretary-General of the UN to the UNGA, 'Report on the safety of journalists and the issue of impunity', A/70/290, (2015) at paras 14-16, (accessible at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/247/06/PDF/N1524706.pdf?OpenElement).
[96] UNGA, 'Resolution on the safety of journalists', A/HRC/33/L.6, (2016) (accessible at: https://www.article19.org/data/files/SoJ_res_Draft.pdf).

**The right to source protection in South Africa**

Source: http://www.saflii.org/za/cases/ZAGPJHC/2012/71.html

In *Bosasa Operations (Pty) Ltd v Basson and Another*, the South Africa High Court established a general proposition that journalists are not required to reveal their sources, subject to certain exceptions. The court stated that:

> "If indeed freedom of the press is fundamental and *sine qua non* for democracy, it is essential that in carrying out this public duty for the public good, the identity of their sources should not be revealed, particularly, when the information so revealed, would not have been publicly known. This essential and critical role of the media, which is more pronounced in our nascent democracy, founded on openness, where corruption has become cancerous, needs to be fostered rather than denuded."[97]

Surveillance activities carried out against journalists run the risk of fundamentally undermining the source protection to which journalists are otherwise entitled. Principle 9 of the Global Principles on the Protection of Freedom of Expression and Privacy provides the following about the protection of sources:

> "9.1. The right to freedom of expression implies that everyone who obtains information from confidential sources with a view to exercising a journalistic activity has, subject to Principles 9.2 (a) and (b), a duty not to disclose the identity of their confidential sources and a right not to be required to do so.
> 9.2. States should provide for the protection of the confidentiality of sources in their legislation and ensure that:
> (a) Any restriction on the right to protection of sources complies with the three-part test under international human rights law…;
> (b) The confidentiality of sources should only be lifted in exceptional circumstances and only by a court order, which complies with the requirements of a legitimate aim, necessity, and proportionality. The same protections should apply to access to journalistic material;
> (c) The right not to disclose the identity of sources and the protection of journalistic material requires that the privacy and security of the communications of anyone engaged in journalistic activity, including access to their communications data and metadata, must be protected. Circumventions, such as secret surveillance or analysis of communications data not authorised by judicial authorities according to clear and narrow legal rules, must not be used to undermine source confidentiality; and
> (d) Any court order under 9.2 (b) and (c) must only be granted after a fair hearing where sufficient notice has been given to the journalist in question, except in genuine emergencies."

[97] Id at para 38.

Further to this, the United Nations Educational, Scientific and Cultural Organization (**UNESCO**) has set out that a robust and comprehensive source protection framework would encompass the need to:[98]

- Recognise the value to the public interest of source protection, with its legal foundation in the right to freedom of expression (including press freedom), and to privacy. These protections should also be embedded within a country's constitution and/or national law.
- Recognise that source protection should extend to all acts of journalism and across all platforms, services and mediums (of data storage and publication), and that it includes digital data and meta-data.
- Recognise that source protection does not entail registration or licensing of practitioners of journalism.
- Recognise the potential detrimental impact on public interest journalism, and on society, of source-related information being caught up in bulk data recording, tracking, storage and collection.
- Affirm that state and corporate actors (including third-party intermediaries), who capture journalistic digital data must treat it confidentially (also acknowledging the desirability of the storage and use of such data being consistent with the general right to privacy).
- Shield acts of journalism from targeted surveillance, data retention and handover of material connected to confidential sources.
- Define exceptions to all the above very narrowly, so as to preserve the principle of source protection as the effective norm and standard.
- Define exceptions as needing to conform to a provision of "necessity" and "proportionality" – in other words, when no alternative to disclosure is possible, when there is a greater public interest in disclosure than in protection, and when the terms and extent of disclosure still preserve confidentiality as much as possible.
- Define a transparent and independent judicial process with appeal potential for authorised exceptions and ensure that law-enforcement agents and judicial actors are educated about the principles involved.
- Criminalise arbitrary, unauthorised and wilful violations of confidentiality of sources by third-party actors.
- Recognise that source protection laws can be strengthened by complementary whistleblower legislation.

UNESCO has further noted that there is a particular gender dimension that arises in respect of source protection in the digital age. Women journalists face additional risks in the course of their work, both on- and offline: in the physical realm, these risks include sexual harassment, physical assault and rape, which may limit their physical mobility; and in the digital sphere, acts of harassment and threats of violence are rampant.[99] Similarly, female sources face increased risks when acting as whistleblowers or confidential informants.[100] As such, women journalists need to be able to rely on secure, non-physical forms of communication with their

[98] UNESCO, 'Protecting journalism sources in the digital age', 2(017) at pp 132-133, (accessible at https://unesdoc.unesco.org/ark:/48223/pf0000248054).
[99] Id at p 134.
[100] Id.

sources, in particular secure digital communications, to be able to engage with their sources.[101]

**Digital safety and security are paramount for both female journalists and sources**

Source: UNESCO, 'Protecting journalism sources in the digital age', 2017, accessible at https://unesdoc.unesco.org/ark:/48223/pf0000248054.

"Women journalists need to be able to rely on secure digital communications to ensure that they are not at increased risk in conflict zones, or when working on dangerous stories, such as those about corruption and crime. The ability to covertly intercept and analyse journalistic communications with sources increases the physical risk to both women journalists and their sources in such contexts. Encrypted communications and other defensive measures are therefore of great importance to ensure that their movements are not tracked and the identity of the source remains confidential.

The risks of exposure for confidential sources are magnified for female whistleblowers. Therefore, they need to be able to have access to secure digital communications methods to ensure that they are at minimum risk of detection and unmasking. They also need to have confidence in the ability to make secure contact with journalists to ensure that stories affecting women are told – secure digital communications can be an enabler for women's participation in public interest journalism. They can also help to avoid magnifying the 'chilling' of investigative journalism dependent upon female confidential sources. Also needed are strong legal protections for confidentiality, which are applied in a gender-sensitive manner - especially in regard to judicial orders compelling disclosure."

## Online Harassment

Harassment, threats, and online violence severely restrict the enjoyment that persons have of their rights online, particularly vulnerable, and marginalised groups, including women and members of sexual minorities.

Social media platforms are especially fertile ground for online harassment, but these behaviours occur in a wide range of online venues.[102] For those who experience online harassment directly, these encounters can have profound real-world consequences, ranging from mental or emotional stress to reputational damage or even fear for one's personal safety.[103] Furthermore, whether one is affected directly or indirectly by it, it can lead to significant self-censorship to avoid incurring such harassment.

[101] Id.
[102] Id.
[103] Id.

While the internet provides a forum for people to seek information about their identities and sexual orientation, and to express themselves on these topics, many people suffer a wide range of attacks in doing so, including attacks on sexuality, exposing personal information, and the manipulation of images that are then used for blackmail and destroying credibility. Furthermore, a common trend amongst children using the internet involves so-called 'cyberbullying'. Research has shown that online harassment is often focused on personal or physical characteristics, with political views, gender, physical appearance, and race being among the most common.[104] Furthermore, women encounter sexualised forms of online harassment at much higher rates than men.[105]

A particular form of online harassment, typically towards women, is that of the non-consensual publication of a person's intimate or sexually explicit photographs or videos. This constitutes a gross violation of a person's privacy, often for the purposes of extortion, blackmail, and/or humiliation. Several recently enacted cybercrime laws in Southern Africa criminalise the non-consensual distribution of private sexual photographs and films – most notably in Botswana and South Africa.[106]

Ongoing harassment and attacks on members of the media have become a particularly worrying trend. As stated in the preamble to the 2011 African Commission Resolution on the Safety of Journalists and Media Practitioners in Africa,[107] freedom of expression, press freedom and access to information can only be enjoyed when journalists and media practitioners are free from intimidation, pressure, and coercion.

**Types of online harassment**

Source: PEN America, 'Defining online harassment: A glossary of terms', accessible at https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

- **Cyberbullying**: An umbrella term (like "online harassment") meant to encompass a number of harassing online behaviours. Like physical bullying, "cyberbullying" is generally aimed at young people and may involve threats, embarrassment, or humiliation in an online setting.

- **Cyber mob attacks**: Cyber-mob attack occurs when a large group gathers online to try to collectively shame, harass, threaten, or discredit a target. Targets overwhelmingly belong to traditionally marginalized groups. "Outrage mobs" or "shaming mobs" are a distinct kind of cyber mob made up of internet users who collectively troll individuals in the hopes of silencing or publicly punishing them. Targets of outrage mobs are often attacked for expressing opinions on politically charged topics or ideas the outrage mob disagrees with and/or has taken out of context in order to promote a particular agenda.

[104] Id.
[105] Id.
[106] MISA Zimbabwe, 'Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights,' (2021) (accessible at https://data.misa.org/api/files/1634498575242w6kap89lsf8.pdf).
[107] Accessible at http://www.achpr.org/sessions/49th/resolutions/185/.

Outrage mobbing can sometimes have severe consequences offline and has even resulted in targets losing their jobs.

- **Cyberstalking**: In a legal context, "cyberstalking" is the prolonged use (a "course of conduct") of online harassment intended to kill, injure, harass, intimidate, or place under surveillance a target. Cyberstalking can comprise a number of harassing behaviours committed repeatedly or with regularity that usually cause a target to suffer fear, anxiety, humiliation, and extreme emotional distress.

- **Denial of service (DoS) or Distributed Denial-of-Service (DDoS) attacks**: A DoS attack is a cyberattack that temporarily or indefinitely disrupts internet service by overwhelming a system with data, resulting in the web server crashing or becoming inoperable. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (such as banking), or other services that rely on the affected computer. In a DDoS attack, an attacker takes control of one user's computer in order to attack a different user's computer. This can force the hijacked computer to send large amounts of data to a particular website or send spam to targeted email addresses.

- **Doxing (or doxxing)**: Doxing involves publishing someone's sensitive personal information online in an attempt to harass, intimidate, extort, stalk, or steal the identity of a target. "Sensitive information" can include social security numbers, phone numbers, home addresses, personal photos, employment information, email addresses, and family members' personal information.

- **Hateful speech and online threats**: By far the most common form of online harassment, hateful speech or threats, both explicit and implicit, can be issued by an ill-intentioned internet user pretty much anywhere on the web. Hateful speech is a form of expression attacking a specific aspect of a person's identity, such as one's race, ethnicity, gender identity, religion, sexual orientation, or disability. Hateful speech online often takes the form of ad hominem attacks, which invoke prejudicial feelings over intellectual arguments in order to avoid discussion of the topic at hand by attacking a person's character or attributes. Threats issued online can be just as frightening as they are offline and are frequently meant to be physically or sexually intimidating.

- **Message bombing**: "Message bombing" is the intentional flooding of a person's or institution's phone or email accounts with messages meant to limit or block a user's access to a device's operating system or platform. Because large numbers of messages sent in a short period of time can typically render a person's account unusable, this is an effective way for a harasser to prevent you from using your devices or accessing your online accounts. Message bombing typically occurs over texting apps, chat apps, or email accounts.

- **Non-consensual, intimate images and videos (such as "revenge porn")**: The dissemination of non-consensual intimate images **(NCII)** – often called "revenge porn" – is the distribution of private, sexual or intimate images or videos of a person without their

consent. This can also fall under the category of "sextortion," i.e. the threat of distributing a nude or sexually explicit image or video in an effort to blackmail an individual.

- **Online impersonation**: "Online impersonation" is a strategy whereby harassers create hoax social media accounts, usually in order to post offensive or inflammatory statements in your name. In most cases, the harasser's intention is to defame or discredit you, often by convincing others to believe the fake quotes attributed to you, which might then incite others to commit additional acts of harassment. Impersonation trolling can also happen when a harasser impersonates someone you know in order to offend or hurt you.

- **Online sexual harassment**: Online sexual harassment – which is targeted at women at a far higher rate than men – encompasses a wide range of sexual misconduct on digital platforms and includes some of the more specific forms of online harassment, such as "revenge porn". It often manifests as hateful speech or online threats. There are four distinct types of online sexual harassment: non-consensual sharing of intimate images and videos; exploitation, coercion and threats; sexualised bullying; and unwanted sexualisation.

- **Trolling**: "Trolling" is one of those terms that's evolved so much over time as to have no single agreed-upon meaning. The term "trolling" is defined here as the repetitive posting of inflammatory or hateful comments online by an individual whose intent is to seek attention, intentionally harm a target, cause trouble and/or controversy, and/or join up with a group of trolls who have already commenced a trolling campaign. There are three subcategories of trolling to be aware of: concern trolling, where harassers pose as fans or supporters of your work with the intention of making harmful or demeaning comments masked as constructive feedback; dogpiling, where a group of trolls works together to overwhelm a target through a barrage of disingenuous questions, threats, slurs, insults, and other tactics meant to shame, silence, discredit, or drive a target offline; and botnet or sock-puppet trolling, which are used for a variety of reasons, from promoting propaganda to amplifying hate or defamation against targeted individuals.

Arguably, one of the key challenges is in getting lawmakers and law enforcement officials to recognise the severity of such harassment and threats, and to treat it with the appropriate levels of concern, recognising that the real and persistent harm suffered applies whether the harassment and threats take place online or offline. Two further challenges that arise that are exacerbated in the online sphere relate to the volume of threats that can be received, given the relative ease with which this can be done via social media platforms, for instance; and the concurrent difficulties in identifying perpetrators who are sometimes able to mask their online identities.

This ties in with the issue of anonymity online. This is because one of the particular challenges with online harassment is that perpetrators may mask their identities, making it difficult for law enforcement officials to apprehend them. This, however, should not be seen as a sufficient

basis to allow for a blanket ban on anonymity or encryption online. The UNSR on Freedom of Expression has responded to this concern and has stated that:[108]

> "The "dark" side of encryption and anonymity is a reflection of the fact that wrongdoing offline takes place online as well. Law enforcement and counter-terrorism officials express concern that terrorists and ordinary criminals use encryption and anonymity to hide their activities, making it difficult for Governments to prevent and conduct investigations into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives. Harassment and cyberbullying may rely on anonymity as a cowardly mask for discrimination, particularly against members of vulnerable groups. At the same time, however, law enforcement often uses the same tools to ensure their own operational security in undercover operations, while members of vulnerable groups may use the tools to ensure their privacy in the face of harassment. Moreover, Governments have at their disposal a broad set of alternative tools, such as wiretapping, geo-location and tracking, data-mining, traditional physical surveillance and many others, which strengthen contemporary law enforcement and counter-terrorism."

Where journalists allege imminent threats to their safety, courts are empowered to grant interdictory relief in appropriate circumstances and subject to the relevant legal requirements. For instance, in the matter of *South African National Editors Forum and Others v Black Land First and* Others,[109] the South African high court granted an interdict in favour of the media broadly, in terms of which the respondents were interdicted from "engaging in any of the following acts directed towards the applicants: Intimidation; Harassment; Assaults; Threats; Coming to their homes; or acting in any manner that would constitute an infringement of their personal liberty", and from "making any threatening or intimidating gestures on social media … that references any violence, harm and threat".[110]

**Protection orders**

Source: South African National Editors' Forum, 'South Africa 2019 elections: Handbook for journalists', 2019, accessible at https://sanef.org.za/elections-2019/

Section 4 of the South African Protection from Harassment Act provides that if a court is satisfied that a protection order must be issued as a result of harassment that has taken place over electronic communications or e-mail, and the identity of the respondent is not known, the court may issue a direction to an electronic communications service provider directing that it furnish the court with the following information on the affidavit:

- The electronic communications identity number from where the harassing electronic communications or electronic mail originated.

[108] UNSR Report on Anonymity and Encryption at para 13.
[109] Accessible at http://www.saflii.org/za/cases/ZAGPJHC/2017/179.html.
[110] Id. at para 29.

- The name, surname, identity number and address of the respondent to whom the electronic communications identity number has been assigned.
- Any information which indicates that electronic communications or electronic mail were or were not sent from the electronic communications identity number of the respondent to the electronic communications identity number of the complainant.

Any other information that is available to an electronic communications service provider that may be of assistance to the court to identify the respondent or the electronic communications service provider which provides a service to the respondent.

As stated in the 2016 UN Resolution on the Safety of Journalists, impunity for attacks against journalists constitutes one of the greatest challenges to the safety of journalists and ensuring accountability for crimes committed against journalists is a key element in preventing future attacks.

Principle 20 of the Declaration of Principles on Freedom of Expression in Africa provides that states must guarantee the safety of journalists and take measures to prevent attacks on them, as well as take effective legal steps to investigate and prosecute attacks against journalists. It further calls on states to take specific measures to ensure the safety of female journalists by addressing gender-specific safety concerns, including sexual and gender-based violence, intimidation, and harassment.[111]

General Comment No. 34 provides that an attack on any person because of the exercise of his or her right to freedom of expression, including forms of attack such as arbitrary arrest, torture, threats to life and killing, cannot be justified under article 19 of the ICCPR.[112] It states further that journalists, as well as other persons involved in gathering and analysing information about human rights situations such as lawyers and judges, are frequently subjected to threats, intimidation and attacks because of their activities.[113]

Although it is clear that what is required in the face of online attacks is swift and firm justice, the reality is that many perpetrators commit such with impunity.[114] Impunity perpetuates a cycle of violence: it raises serious concern that such attacks going unpunished sends a public signal that the state and public authorities do not take such attacks seriously.[115]

There is therefore clear guidance under international law that states must take measures to protect persons, including members of the media, against such harassment and attacks. This is so whether the harassment takes place offline or online.

[111] Accessible at: https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf.
[112] General Comment No. 34 at para 23.
[113] General Comment No. 34 at para 23.
[114] South African National Editors' Forum, 'South Africa 2019 elections: Handbook for journalists', (2019) (accessible at https://sanef.org.za/elections-2019/).
[115] Id.

**Tips for digital safety to protect against online harassment and trolling**

Source: Committee for the Protection of Journalists, 'South Africa elections 2019: Journalist safety toolkit, 27 February 2019, accessible at https://cpj.org/2019/02/south-africa-election-journalist-safety-kit.php#harassment

- Create long and strong passwords for your accounts. (Password managers are useful tools to be able to remember the different passwords used for different accounts.)
- Turn on two-factor authentication.
- Review your privacy settings for each account and make sure any personal data, such as phone numbers and date of birth, is removed.
- Look through your accounts and remove any photos or images that could be manipulated and used as a way to discredit you.
- Consider getting your account verified by the social media company.
- Monitor your accounts for signs of increased trolling activity or for indications that a digital threat could become a physical threat.
- Speak with family and friends about online harassment

## Conclusion

The right to privacy has encountered many new challenges in the digital era. The rapid and widespread adoption of data processing has raised concerns for the protection of personal information, leading to a raft of new data protection laws being passed across the world, and efforts to engender accountability for government and private-sector-led surveillance based on invasive new technologies including facial recognition.

It has also resulted in a need to find the appropriate balance between protecting freedom of expression by enabling anonymity and encryption online while ensuring accountability for crimes committed in the digital sphere. Generally, wholesale prohibitions on anonymity and encryption are seen as disproportionate infringements on the right to freedom of expression, and in recent years international law guidance for states and private actors on these issues has become robust.

These digital rights challenges have particular resonance for journalists who operate online and often bear the brunt of efforts to surveil or intrude in their private communications, including facing high levels of online abuse and harassment. Women journalists are particularly targeted in this regard. It is vital that states take steps to protect journalists in the online sphere and to align their legislative frameworks with the international guidance that exists in order to ensure the protection of freedom of expression in the modern era.

*Module 5*

# Trends in Censorship by Private Actors

*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 5

## Trends in Censorship by Private Actors

**This module aims to:**

- **Give an overview of ways in which non-state actors facilitate online censorship.**
- **Set out the international and regional legal principles that are implicated by online censorship.**
- **Unpack the concept of net neutrality.**
- **Examine the misuse of intermediary liability to curb expression and access.**
- **Explore the right to be forgotten.**
- **Explain the monitoring obligations of search engines and platforms.**

---

## Introduction

It is now well established that "the same rights that people have offline must be protected online".[1] However, there is growing appreciation in international law and human rights that online censorship by non-state actors threatens an array of rights, most notably the right to freedom of expression. Litigators and activists must now contend not only with state abuses of digital rights but also violations by private actors.

According to the 2011 Report of the United Nations Special Rapporteur on Freedom of Expression (**UNSR**), the "framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet." This is particularly true for freedom of expression, as the UNSR explains: the "[i]nternet has become a key means by which individuals can exercise their right to freedom of opinion and expression." The rise of the internet has brought to the fore new, private actors who often wield significant power. Social media platforms and multinational online companies exercise significant control in the facilitation of people's enjoyment of their human rights online. Like many state actors, non-state actors do not always act in accordance with the basic principles of international human rights law.

This module grapples with some of the long-term threats to freedom of expression from non-state actors, as well as emergent threats. Alongside a brief overview of relevant topics, it

[1] UN Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet' A/HRC/RES/20/8, (2012) (accessible at https://daccess-ods.un.org/TMP/9602589.01119232.html). See further UN Human Rights Council 'Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association' A/HRC/41/41, (2019,) (accessible at https://undocs.org/A/HRC/41/41).

provides practical guidance on how to ensure that fundamental rights and freedoms are respected, protected, and promoted online.

## Net Neutrality

*An overview of net neutrality*

The UNSR's 2017 Report focused on the Information and communications technology (**ICT**) sector and explained that net neutrality requires that internet data is treated equally without undue interference.[2] In principle, net neutrality protections are designed to safeguard freedom of expression and access to information online by ensuring that such freedoms are not determined by market forces or curtailed by network providers.[3] Essentially, this means that internet service providers (**ISPs**) must remain neutral and impartial when providing internet access. In this regard, ISPs cannot alter competition, or unduly interfere with or diminish opportunities for content providers. Additionally, as explained by the Center for Technology and Democracy in a report on the Importance of Internet Neutrality to Protecting Human Rights Online, service providers cannot discriminate against or manipulate internet traffic on the basis of source, destination, content or associated application. For example, an ISP cannot block, slow down or alter access to service A or make it faster and easier to access service B.

Net neutrality fulfils an important role in ensuring that people can freely access information and impart ideas across our information society. It promotes diversity, pluralism, and innovation. The Steering Committee on Media and Information Society of the Council of Europe, in its report on Protecting Human Rights through Network Neutrality, explained that net neutrality encourages internet users to freely elect how they use their internet connection. The Center for Technology and Democracy explains that:

> "preserving internet neutrality means preserving the power of individuals to make choices about how they use the Internet – what information to seek, receive, and impart, from which sources, and through which services."

*Net neutrality, development, and human rights*

Given net neutrality's role in the advancement of freedom of expression, it should be viewed through a human rights lens. Some have gone as far as suggesting that it is an emerging international human rights norm.[4] Ensuring network neutrality is seen as central to the protection of fundamental human rights and an enabler of fair competition and innovation, as

[2] See further Media Defence 'Training Manual on Digital Rights and Freedom of Expression Online Litigating digital rights and online freedom of expression in East, West and Southern Africa*'* at 24, (accessible at https://www.mediadefence.org/resources/mldi-training-manual-digital-rights-and-freedom-expression-online).
[3] Carrillo, 'Having Your Cake and Eating It Too? Zero-Rating, Net Neutrality, and International Law' 19 *Stanford Technology Law Review*, (2016) at 367, (accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746447).
[4] Id.

it promotes freedom and enhances network access.[5] In the same 2017 Report, the UNSR noted:

> "In the digital age, the freedom to choose among information sources is meaningful only when Internet content and applications of all kinds are transmitted without undue discrimination or interference by non-State actors, including providers. The State's positive duty to promote freedom of expression argues strongly for network neutrality in order to promote the widest possible non-discriminatory access to information."

Yet despite the demonstrable link between human rights and net neutrality and the clearly defined position of the UNSR, the past decade has seen growing threats to net neutrality. It has been the subject of regulatory debates and radical shifts in regulations across the world. Additionally, norms and standards have started to develop, and, equally, attempts by state and non-state actors to influence net neutrality and individuals' freedom of expression online are on the rise. This will be outlined below.

*Current challenges and debates*

Presently there are two common methods of limiting net neutrality:

- The first entails the **blocking or throttling of content**, either by state or non-state actors. This may include entirely blocking or significantly slowing down access to specific websites, content, or platforms, or restricting access to content in specific geographic regions. It is largely acknowledged that this form of restriction is contrary to international human rights norms. The Net Neutrality Compendium explains that "blocking certain information resources or restricting what information Internet users can impart over their connection would have serious implications for the right to free expression. For example, blocking access to a particular lawful blog because its content is disfavoured by the access provider would raise obvious concerns." The 2017 Report of the UNSR notes that "States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression."

- The second is commonly referred to as **zero-rating**, which involves the differential treatment of content through the provision of certain preferred content with a zero-download cost.[6] This method is less drastic than blocking and throttling of content and is often framed in terms of public benefit. The 2017 Report of the UNSR describes zero-rating as "the practice of not charging for the use of internet data associated with a particular application or service; other services or applications, meanwhile, are subject to metered costs." Zero-rating can have differential effects depending on who implements it and how decisions are made about which content to make freely accessible. In low-income contexts, it can be an effective way to provide widespread access to public good information.

[5] Audibert and Murray, 'A Principled Approach to Network Neutrality' *LSE Research Online,* (2016) at 120, (accessible at http://eprints.lse.ac.uk/67362/7/Murray_Principled%20approach_2016.pdf).
[6] Marsden 'Zero Rating and Mobile Net Neutrality' Belli and De Filippi (ed) *Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet* (2016) at 241.

States have responded differently to net neutrality and zero-rating, with some legislating strong protections for the former and others developing policies to promote zero-rating of certain content as a public service.

Among certain developed states, there is an emergent trend toward complete bans of zero-rating. Canada, Norway, Slovenia, and the Netherlands are some of the states that have prohibited service providers from differentiating between tariffs for internet access services.[7] Developed countries generally have widespread access to the internet, as well as affordable mobile data.

Among developing countries, zero-rating is more likely to be viewed as a policy approach to address challenges such as limited internet access, high data prices and widespread digital divides. Notably, the global COVID-19 pandemic prompted a range of temporary zero-rating initiatives in both developed[8] and developing nations,[9] in which online education, health, and other resources were zero-rated. In many instances, ISPs voluntarily provided zero-rated access to certain resources, such as in Tanzania and Kenya,[10] while in South Africa the government issued regulations which mandated zero-rating of certain resources as a requirement.[11]

While these measures were enacted as once-off exceptions as a result of the unprecedented challenges of a global pandemic, in the long run, zero-rating could be seen to cause complications in relation to net neutrality. Access Now explains:

> "Activists in advanced economies are struggling to communicate the importance of Net Neutrality for free expression, innovation, and competition, in some cases to audiences that are increasingly anti-regulation. Many in developing countries are facing down critics who argue that non-neutral internet access somehow functions as an "on-ramp" for the free and open internet."

The following examples illustrate the complexity of this debate.

[7] Marsden in Net Neutrality Compendium above n 6 at 248.
[8] Body of European Regulators for Electronic Communication, *BEREC Report on COVID-19 crisis – lessons learned regarding communications networks and services for a resilient society,* (2021) (accessible at https://www.berec.europa.eu/sites/default/files/files/document_register_store/2021/6/BoR_(21)_88_Draft_BEREC_Report_on_COVID19_final.pdf).
[9] Bhandari, *Improving internet connectivity during Covid-19,* Digital Pathways at Oxford Paper Series no. 4, (2020) (accessible at https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-09/improving_internet_connectivity_during_covid-19_0.pdf).
[10] GSMA, 'Education for all during COVID-19: Scaling access and impact of EdTech', (2020) (accessible at: https://www.gsma.com/mobilefordevelopment/blog/education-for-all-during-covid-19-scaling-access-and-impact-of-edtech/).
[11] Bhandari, above n 9 at 19.

### The fight for net neutrality in India

The net neutrality debate came to the fore with two zero-rated options being offered to Indian users in 2015 – Facebook's 'Internet.org' and Bharti Airtel's 'Airtel Zero'. In February 2015, Facebook (now Meta) launched Internet.org with the stated intention of providing free basic internet services to people in India, but only to selected online content.[12] At around the same time, Airtel launched Airtel Zero, a platform for zero-rated services, offering access to a range of content. Content providers paid Airtel to be included in this service. By April 2015, Airtel was the largest mobile ISP in India with 226 million customers.[13]

That year, the Telecom Regulatory Authority of India (**TRAI**) called for public comment on its consultation paper on net neutrality. This sparked a national debate on the topic, with many individuals and civil society actors providing comments on the importance of net neutrality. This process led to the TRAI releasing recommendations on the prohibition of discriminatory data services, which essentially prohibited ISPs from offering or charging discriminatory tariffs for data services on the basis of content. It is worth mentioning that amid the upheaval around zero-rating, Meta's founder Mark Zuckerberg stated in a video: "Some may argue for an extreme definition of net neutrality that says that it's somehow wrong to offer any more services to support the unconnected, but a reasonable definition of net neutrality is more inclusive. Access equals opportunity. Net neutrality should not prevent access."

Meta argued that some access is better than no access. This was not well received by digital rights activists, who lobbied to introduce regulations to safeguard net neutrality. Within two years, the net neutrality landscape underwent significant changes:

- In 2016, TRAI released regulations titled "Prohibition of discriminatory tariffs for data services" which, among other things, prohibited any service provider from offering or charging discriminatory tariffs for data services on the basis of content.
- In 2017, TRAI provided the Department of Technology with further recommendations regarding net neutrality.
- In 2018, the Indian Government pledged its commitment to the fundamental principles and concepts of net neutrality.
- In July 2018, India was heralded for adopting the world's strongest net neutrality norms.

[12] Carrillo above n 3 at 367. See further Chaudhry, 'Spotlight on India's Internet: Facebook's Free Basics or Basic Failure' University of Washington Henry M. Jackson School of International Studies, (2016) (accessible at https://jsis.washington.edu/news/spotlight-indias-internet-facebooks-free-basics-basic-failure/).
[13] Marsden in Net Neutrality Compendium at 251.

### The fight regarding net neutrality in the United States

Legislative and policy developments in the United States provide a useful case study into the nuances of the net neutrality principle and illustrate how politics and economics are at a crossroads with human rights. The Harvard Business Review notes that "Despite being a simple idea, net neutrality has proven difficult to translate into US policy. It sits uncomfortably at the intersection of highly technical internet architecture and equally complex principles of administrative law."

In 2015, following a Federal Court of Appeals ruling, the Federal Communications Commission (**FCC**) in the US enacted the historic Open Internet Rules, which prohibited internet providers from engaging with differential pricing for certain content or from giving preferential treatment to certain websites.[14] However, during the Trump presidency, the US government's view on net neutrality changed.

In 2017, the FCC voted to repeal the Open Internet Rules.[15] This decision was viewed as a negative step for many digital rights and free expression activists. Access Now captured some of the responses by open internet advocates and rights organisations:

- "This order brazenly prioritizes the profits of internet middlemen over the health of the internet ecosystem and the freedom of internet users. We're very disappointed to see this abdication by the US of its leadership in internet governance" - Aravind Ravi-Sulekha, Internet Freedom Foundation (India).

- "Today the country with the largest share of the global internet economy has entered into a dangerous experiment. By abolishing the rules that protect the innovation of its startups and the free speech of its citizens, the benefits of mankind's greatest invention – the internet – are put in jeopardy in exchange for short-term gains for a few telecoms companies. We hope this historic mistake will be corrected and eventually pave the way for real legislative protection of Net Neutrality in the United States." – Thomas Lohninger, Executive Director, epicenter.works (Austria).

- "The internet must be free, open, and preserve the rights of all the users, without any kind of discrimination or repression or censorship of their rights. It was never intended as a tool to give power to IAPs or ISPs to be a 'gatekeeper,' privileging certain users or blocking others based on business or governmental interests. Let's safeguard Net Neutrality!"– Houssem Kaabi, President, International Institute of Debate (Tunisia).

[14] See Pouzin, 'Net Neutrality and Quality of Service' in Net Neutrality Compendium above n 6 at 78. See further Access Now 'Net Neutrality matters for human rights across the globe', (2017) (accessible at https://www.accessnow.org/net-neutrality-matters-human-rights-across-globe/).

[15] See Washington Post, 'The FCC just voted to repeal its net neutrality rules, in a sweeping act of deregulation',( 2017) (accessible at https://www.washingtonpost.com/news/the-switch/wp/2017/12/14/the-fcc-is-expected-to-repeal-its-net-neutrality-rules-today-in-a-sweeping-act-of-deregulation/). See further Electronic Frontier Foundation 'Team Internet Is Far From Done: What's Next For Net Neutrality and How You Can Help', (2017) (accessible at https://www.eff.org/deeplinks/2017/12/team-internet-far-done-whats-next-net-neutrality-and-how-you-can-help).

- "The ending of Net Neutrality in the US could be the beginning of the end of the open, interoperable, free internet. It is now a question of how much, not if, freedom of expression online will be undermined around the world as a result of this short-sighted decision to enrich the entrenched near-monopolies who control internet access in the United States." – Quinn McKew, Deputy Executive Director, ARTICLE 19 (United Kingdom).

In 2018, the FCC's repeal of the net neutrality rules became official.[16] Net neutrality advocates challenged this decision, but in 2019 the DC Circuit Court ruled in favour of the FCC and upheld its repeal of the 2015 Rules.[17] In February 2020, despite attempts by various stakeholders, the DC Court of Appeals dismissed an appeal to reverse the repeal of the net neutrality rules.[18]

However, the position was reversed again shortly after President Joe Biden assumed office in 2021 when Biden signed an Executive Order which included a call for the FCC to reinstate net neutrality rules.[19] It is likely that the net neutrality debate will continue in the US, illustrating the stark contrast between those in favour of net neutrality and the economic interests of those who seek to curb it.

*Practically engaging with net neutrality*

As illustrated above, state and non-state actors often seek to depart from the principles of net neutrality and materially change the conditions of people's access to the internet, which impacts the right of freedom of expression and access to information. Overcoming the threats to net neutrality involves two key considerations: the need to ensure adequate safeguards that preserve net neutrality; and the need to understand what limitations are permissible in relation to net neutrality. According to the Net Neutrality Compendium:

> "To an unprecedented degree, the Internet transcends national borders and reduces barriers to the free flow of information, enabling free expression, democratic participation, and the enjoyment of other rights … Establishing rules to preserve net neutrality – or more precisely, Internet neutrality – is one way to prevent the imposition, by those in a position to control access, of structural inequalities that would distort this environment."[20]

[16] New York Times, 'Net Neutrality Has Officially Been Repealed. Here's How That Could Affect You', (2018) (accessible at https://www.nytimes.com/2018/06/11/technology/net-neutrality-repeal.html).
[17] Washington Post, 'Appeals Court Ruling Upholds FCC's Cancelling of Net Neutrality Rules', (2019) (accessible at https://www.washingtonpost.com/technology/2019/10/01/appeals-court-upholds-trump-administrations-cancelling-net-neutrality-rules/).
[18] Endgated, 'US Appeals Court Will Not Rule on Repealing Net Neutrality Laws', (2020) (accessible at https://www.engadget.com/2020/02/07/net-neutrality-us-appeals-court/).
[19] Office of the US Presidency, 'Fact Sheet: Executive Order on Promoting Competition in the American Economy', (2021) (accessible at https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/).
[20] McDiarmid and Shears, 'The Importance of Internet Neutrality to Protecting Human Rights Online' in Net Neutrality Compendium at 31-32.

As discussed above, states should preserve net neutrality to promote the widest possible non-discriminatory access to information. Calling on states to enact laws or regulations to protect net neutrality is an important step in holding states accountable and pushing them to fulfil their responsibilities of protecting freedom of expression.[21]

### Tips for good net neutrality protections

The Net Neutrality Compendium provides five principles to guide the substantive development of net neutrality protections that will ensure that states fulfil their obligations in relation to free expression and other human rights online:[22]

- There should be a clear expectation that internet access services must be provided in a neutral manner, without discrimination based on the content, applications or services subscribers choose to access.
- The scope of the neutrality obligation should be clearly defined and should account for the crucial distinction between internet access services and specialised services.
- The neutrality obligation should apply equally to fixed and mobile internet access services.
- There should be clear guidelines for evaluating exceptions for reasonable network management practices.
- The neutrality obligation should not apply to over-the-top services available on the internet.

### Minimum standards and safeguards for network neutrality regulation:

The Net Neutrality Compendium in its Policy Statement on Network Neutrality further suggests the following safeguards for Network Neutrality regulatory instruments:

- **Principle of network neutrality**: Network neutrality is the principle according to which internet traffic is treated without unreasonable discrimination, restriction, or interference regardless of its sender, recipient, type or content.

- **Reasonable traffic management**: ISPs should act in accordance with the principle of network neutrality. Any deviation from this principle may be considered reasonable traffic management as long as it is necessary and proportionate to:
  - Preserve network security and integrity.
  - Mitigate the effects of temporary and exceptional congestion, primarily by means of protocol-agnostic measures or, when these measures do not prove practicable, by means of protocol-specific measures.
  - Prioritise emergency services in the case of unforeseeable circumstances or force majeure.

[21] Id at 38.
[22] Id 38-41.

- **Law enforcement**: None of the foregoing should prevent ISPs from giving force to a court order or a legal provision in accordance with human rights norms and international law.

- **Transparent traffic management**: ISPs should publish meaningful and transparent information on characteristics and conditions of the internet access services they offer, the connection speeds that are to be provided, and their traffic management practices, notably with regard to how internet access services may be affected by simultaneous usage of other services provided by the ISP.

- **Privacy**: All players in the internet value chain, including governments, shall provide robust and meaningful privacy protections for individuals' data in accordance with human rights norms and international law. In particular, any techniques to inspect or analyse internet traffic shall be in accordance with privacy and data protection obligations and subject to clear legal protections.
- **Implementation:** The competent national authorities should promote independent testing of internet traffic management practices, ensure the availability of internet access, and evaluate the compatibility of internet access policies with the principle of network neutrality, as well as in terms of respect for human rights norms and international law. National authorities should publicly report their findings. Complaint procedures to address network neutrality violations should be available and violations should attract appropriate fines. All individuals and stakeholders should have the possibility to contribute to the detection, reporting and correction of violations of the principle of network neutrality.

While adequate legislative and regulatory provisions are the goal, it is, as with all rights, imperative to know what limitations are permissible. The 2011 Joint Declaration on Freedom of Expression and the Internet by a group of Special Rapporteurs on Freedom of Expression from around the world stated:

> "Freedom of expression applies to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards."

Simply put, limitations to net neutrality should only be permitted when provided by law and where necessary and proportionate to the achievement of a legitimate aim.[23] This three-part test is rooted in article 19(3) of the International Covenant on Civil and Political Rights (**ICCPR**) and must be passed for the legitimate and legal restriction of the right to freedom of expression.

In a 2018 Report, the UNSR made the following notable statements regarding state and company liability that should be kept in mind when litigating issues around net neutrality:

[23] For a detailed outline of the limitation of freedom of expression see Module 2 on Restricting Access and Content at 4 – 5. See also Belli, 'End-to-End, Net Neutrality and Human Rights' in Net Neutrality Compendium at 12.

- **In relation to state responsibility**: Human rights law imposes duties on states to ensure enabling environments for freedom of expression and to protect its exercise. The duty to ensure freedom of expression obligates states to promote, among other things, media diversity, independence, and access to information. Additionally, international and regional bodies have urged states to promote universal internet access. States also have a duty to ensure that private entities do not interfere with the freedoms of opinion and expression. The UN Guiding Principles on Business and Human Rights (**Guiding Principles**), adopted by the Human Rights Council in 2011, emphasise state duties to ensure environments that enable business respect for human rights.

- **In relation to state responsibility**: The Guiding Principles establish a framework according to which companies should, at a minimum, avoid causing or contributing to adverse human rights impacts, and seek to prevent or mitigate such impacts directly linked to their operations, products, or services by their business relationships, even if they have not contributed to those impacts.

*Conclusion*

Developing countries continue to face challenges in relation to net neutrality and the suggestion that some access is better than no access. While there is a need for a nuanced approach to zero-rating to enable access to public interest information, the international human rights framework is clear on the need to protect equal access, and states should not enable infringements on net neutrality to serve as justification for failing to take steps toward full and meaningful internet access for all. It is necessary for civil society actors and human rights litigators to ensure that net neutrality is protected through lobbying states, submitting complaints to regulators, strategic litigation, and public advocacy, in order to achieve the goal of equal opportunity in access.

## Intermediary Liability

*Internet intermediaries – an overview*

An 'internet intermediary' is a broad, constantly developing term. The Council of Europe suggests the term encompasses "a wide, diverse and rapidly evolving range of service providers that facilitate interactions on the internet between natural and legal persons". They fulfil a variety of functions, including connecting users to the internet; hosting web-based services; facilitating the processing of data; gathering information and storing data; assisting searching, and; enabling the sale of goods and services.[24] Examples of internet intermediaries include:

- ISPs and web hosting companies that provide the infrastructure;
- Search engines and social media platforms, that provide content and facilitate communication.[25]

[24] Media Defence above n 2 at 6.
[25] ARTICLE 19, "Internet intermediaries: Dilemma of Liability", 2013, at 3, (accessible at: https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf). See further Li, 'Beyond

Simply put, "internet intermediaries are the pipes through which internet content is transmitted and the storage spaces in which it is stored, and are therefore essential to the functioning of the internet."[26] Internet intermediaries dominate a pivotal role in the current digital climate impacting social, economic and political exchanges. They can influence the dissemination of ideas and have been described as the "custodians of our data and gatekeepers of the world's knowledge".[27]

It is not difficult to create a link between internet intermediaries and the advancement of an array of human rights. As the gatekeepers to the internet, they occupy a unique position in which they can enable the exercise of freedom of expression, access to information and privacy rights. The 2016 Report of the UNSR noted that:

> "The contemporary exercise of freedom of opinion and expression owes much of its strength to private industry, which wields enormous power over digital space, acting as a gateway for information and an intermediary for expression."

*Intermediary liability*

Given the important roles that intermediaries play in society, particularly in relation to the myriad of implicated rights, it is imperative to understand their legal liability. The Association for Progressive Communications (**APC**) explains that intermediary liability refers to the extent that internet intermediaries should be held responsible for illegal or harmful activities performed by users through their services. Where intermediary liability exists, ISPs have an obligation to prevent the occurrence of unlawful or harmful activity by users of their services, and failure to do so may lead to legal consequences such as orders to compel or criminal sanctions.

In a Report on the liability of internet intermediaries in Nigeria, Kenya, South Africa, and Uganda, APC captured the following ways in which intermediary liability can arise:

- Copyright infringement.
- Digital privacy.
- Defamation.
- National and public security.
- Hate speech.
- Child protection.
- Intellectual property disputes.

---

Intermediary Liability: The Future of Information Platforms' Yale Law School *Information Society Project, (*2018) at 9 (accessible at https://law.yale.edu/sites/default/files/area/center/isp/documents/beyond_intermediary_liability_-_workshop_report.pdf).

[26] Id at 6.

[27] Riordan, 'The Liability of Internet Intermediaries' DPhil thesis, Oxford University, (2013,) at 1, (accessible at https://ora.ox.ac.uk/objects/uuid:a593f15c-583f-4acf-a743.62ff0eca7bfe/download_file?file_format=pdf&safe_filename=THESIS02&type_of_work=Thesis).

While intermediary liability can be associated with a legitimate interest, there are growing concerns, as noted by the UNSR in the 2016 Report, about the "appropriate balance between freedom of expression and other human rights" and the misuse of intermediary liability to curb expression and access.[28] The legal liability of intermediaries has a direct impact on users' rights. In this regard, there is a direct correlation between restrictive liability laws – the over-regulation of content – and the increased censorship, monitoring and restrictions of legitimate and lawful online expression.

There are three general approaches to intermediary liability, each with differing considerations and implications: strict liability, the broad immunity model, and the safe-harbour model.

*Strict liability*

In terms of this approach, intermediaries are liable for third-party content. The abovementioned UNESCO report states that the only way to avoid liability is to proactively monitor, filter, and remove content in order to comply with the state's law. Failing to do so places an intermediary at risk of fines, criminal liability, and revocation of business or media licenses. The UNESCO report notes that China and Thailand are governed by strict liability. This approach is largely considered inconsistent with international norms and standards.

**Strict Liability in China**

The Stanford CIS World Intermediary Liability Map documents laws around the world that govern internet intermediaries and shape users' digital rights. It provides both basic and advanced tools to search for and visualise how legislation, decisions and public policies are evolving globally. It has captured the following in relation to China:

- In 2000, China's State Council imposed obligations on "producing, assisting in the production of, issuing, or broadcasting" information that contravened an ambiguous list of principles (for example opposing the basic principles as they are confirmed in the Constitution; disrupting national policies on religion, propagating evil cults and feudal superstitions; and spreading rumours, disturbing social order, or disrupting social stability).

- China has followed through with its strict liability approach and continues to hold internet companies liable if they fail to comply. This has led to wide-scale filtering and monitoring by intermediaries. This level of oversight has resulted in social media companies being the principal censors of their users' content.

[28] A 2014 UNESCO report on fostering freedom online and the role of internet intermediaries provides a comprehensive overview of the above regulatory objectives pursued by the states, which in turn have a direct impact on how, and to what extent, intermediaries are compelled to restrict freedom of expression online.

*Broad immunity model*

On the other end of the spectrum is the broad immunity model, which provides exemptions from liability without distinguishing between intermediary function and content. The UNESCO report cites the Communications Decency Act in the United States as an example of this model, which protects intermediaries from liability for illegal behaviour by users when they do remove content in compliance with private company policy. ARTICLE19 explains that under this model, intermediaries are not responsible for the content they carry, but are responsible for the content they disseminate. The Organisation for Economic Co-operation and Development (**OECD**), in its Council Recommendation on principles for internet policy, makes reference to this as the preferred model, as it conforms with the best practices, discussed below, and gives due regard to the promotion and protection of the global free flow of information online.

*Safe harbour model*

The safe harbour model, otherwise known as *conditional liability,* seemingly adopts a middle-ground approach. This approach gives intermediaries immunity provided they comply with certain requirements. Through this approach, intermediaries are not required to actively monitor and filter content, but rather are expected to remove or disable content upon receipt of notice that the content includes infringing material. Central to this approach is the idea of 'notice and takedown procedures', which can be content- or issue-specific. There are mixed views on this approach; for some, it is a fair middle-ground; for others, it is a necessary evil to guard against increased filtering or a complete change in the intermediary landscape.[29] As noted in the UNESCO report, there are others who express concern about this approach because of its susceptibility to abuse, as it may lend itself to self-censorship, giving the intermediaries quasi-judicial power to evaluate and determine the legality of content.

**Conditional liability in South Africa**

The Freedom of Expression Institute explains the position in South Africa as follows:

Chapter 11 of the South African Electronic Communications Act 25 of 2002 provides for limited liability of internet intermediaries subject to a takedown notice condition. These provisions apply to members of the Internet Service Providers Association. An immediate response to takedown notices is necessary, failing which the immunity from liability is forfeited.

Concerns have been noted regarding South Africa's framework, similar to most concerns around the safe harbour approach: ISPs err on the side of caution and are quick to remove content without providing the content provider with an opportunity to defend the content, and there are no existing appeal mechanisms for content creators or providers. This is concerning given the fact that any individual can submit a take-down notice.[30]

The potential for these mechanisms to be abused became clear in 2019 when an ISP briefly took the South African news portal *mg.co.za* offline in response to a fraudulent takedown request seemingly submitted in retaliation for an investigative report about a convicted fraudster at the centre of a controversial South African oil deal.[31]

[29] Koren, Nahmia and Perel, 'Is It Time to Abolish Safe Harbor? When Rhetoric Clouds Policy Goals' *Stanford Law & Policy Review, Forthcoming*, (2019) at 47, (accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3344213).
[30] See further Comninos, 'Intermediary liability in South Africa', (2012) (accessible at https://www.apc.org/sites/default/files/Intermediary_Liability_in_South_Africa-Comninos_06.12.12.pdf). See also Rens, 'Failure of Due Process in ISP Liability and Takedown Procedures' in Global Censorship, Shifting Modes, Persisting Paradigms, (2015) (accessible at https://law.yale.edu/sites/default/files/area/center/isp/documents/a2k_global-censorship_2.pdf).
[31] Mail & Guardian, 'The digital breadcrumbs behind the M&G's censorship attack', (2019) (accessible at https://mg.co.za/article/2019-10-04-00-the-digital-breadcrumbs-behind-the-mgs-censorship-attack/).

At the core of the debate between the various models is the need to understand the difference between lawful and unlawful content. There is a chilling effect on expression when internet intermediaries are left to their own devices to determine what is good or legal, as it is likely they will tend towards more censorship than less, out of fear of liability.

Keeping in line with a human rights perspective, this guide advocates that "[t]he right to freedom of expression online can only be sufficiently protected if intermediaries are adequately insulated from liability for content generated by others."[32] The following section provides some guidance on applicable international human rights frameworks that can be relied on when advocating for rights in relation to intermediary liability.

**Intermediary liability in the courts**

Intermediary liability has been dealt with at some length in the European Court of Human Rights (ECtHR). The seminal case of *Delfi AS v Estonia* found that an online news portal was liable for offensive comments they allowed to be posted below one of their news articles.

In *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, however, found that imposing objective liability for unlawful comments made by readers on a website placed "excessive and impracticable forethought capable of undermining freedom of the right to impart information on the Internet."

More recently, Media Defence and the Electronic Frontier Foundation (EFF) have intervened in a case at the Grand Chamber of the ECtHR, which concerns online users being held liable for third-party comments. In *Sanchez v France* a French politician was charged with incitement to hatred on religious grounds following comments posted on the 'wall' of his Facebook account by other parties. Because he failed to delete those comments promptly, he was convicted of that offence. The individuals who posted the comments were convicted of the same offence. The Fifth Section of the ECtHR held that his conviction for failing to promptly delete unlawful comments published by third parties on the public wall of his Facebook account did not breach his Article 10 rights despite his apparent lack of knowledge of the comments. The judgment has now been referred to the Grand Chamber of the ECtHR.

*Applicable international human rights standards and current international best practices*

Different interest groups continue to push different agendas in relation to internet intermediaries and their liability. Many countries either have non-existent laws or vague and inconsistent laws that make it difficult to enforce rights. There are, however, applicable international human rights frameworks that guide how laws should be enacted or how restrictions may be imposed. With any rights-based advocacy or litigation, it is necessary to establish the rights invoked. As discussed above, it is clear that internet intermediaries play a vital role in the advancement of an array of rights. Thereafter, the next step is to determine responsibility.

[32] Media Defence above n 2 at 28.

In relation to internet intermediaries, the triad of information rights is clearly invoked. The 2010 UN Framework for Business and Human Rights finds that states are primarily responsible for ensuring that internet intermediaries act in a manner that ensures the respect, protection and promotion of fundamental rights and freedoms of internet users. But at the same time, the intermediaries themselves have a responsibility to respect the recognised rights of their users.

The 2019 Joint Declaration on Challenges to Freedom of Expression in the Next Decade observed that:

> "private companies have responsibilities to respect human rights and remedy violations, and that addressing the challenges outlined above requires multi-stakeholder support and the active engagement of State actors, media outlets, intermediaries, civil society and the general public."

Although there might be complexities regarding the cross-jurisdictional scope of intermediaries' powers and responsibilities, international human rights norms should always be at the fore.

Given the link between internet intermediaries and the fundamental right to freedom of expression, it is best to engage with this topic and test laws, regulations and policies against prescribed human rights standards and understand the restrictions and limitations that may be applicable. As discussed in previous sections, restrictions on the right to freedom of expression have been formulated as a strict, narrow, three-part test – namely, that the restriction must:

- Be provided by law;
- Pursue a legitimate aim; and
- Conform to the strict tests of necessity and proportionality.[33]

Laws and content restriction orders and practices must comply with this test. Practically, the need to assess the compliance of legislative frameworks is most likely to be necessitated in jurisdictions that adopt the strict liability model and the safe-harbour model. The strict liability model can be easily tested and found to be compliant. The safe-harbour model presents a slightly more in-depth engagement in order to determine compliance, with the Kenyan Copyright (Amendment) Bill, 2017, providing a useful example to illustrate the application of the applicable tests.

[33] For a detailed outline of the limitation of freedom of expression see Module 2 on Restricting Access and Content at 4 – 5. See further OSCE, "Media Freedom on the Internet: An OSCE Guidebook", (2016) (accessible at https://www.osce.org/netfreedom-guidebook?download=true).

### Kenyan Copyright (Amendment) Bill

In 2022, Kenya passed into law the Copyright (Amendment) Act. The Act was quite substantially altered during the public participation process and ultimately did not deal substantively with intermediary liability issues. However, in its earlier forms, the Bill provided some interesting proposals regarding intermediary liability in the African context. A key feature of earlier versions of the Bill was the introduction of the safe-harbour approach, providing for "conduit" safe harbours and "caching" safe harbours. The former, per (former) section 35A(1)(a), would have protected intermediaries from liability for copyright infringements if their involvement was limited to "providing access to or transmitting content, routing or storage of content in the ordinary course of business".

Under these circumstances, the intermediary is not under an obligation to take down or disable content if a takedown notice is received. As per (former) section 35A(1)(b), intermediaries would have been protected if their role was related to content storage that is "automatic, intermediate and temporary". This protection would be conditional upon the removal of content following a take-down notice.[34]

Civil society criticised the lack of clarity and poor notice-and-takedown procedures in the Bill, noting that it fell short of international standards on freedom of expression. ARTICLE 19 listed five problems with the Bill in terms of notice-and-takedown procedures:

- **Lack of proportionality**: criminal sanctions would have been imposed on intermediaries who failed to remove content. As discussed above, this would cause intermediaries to lean toward censorship and blocking, which infringes on freedom of expression.
- **Lack of clarity**: the procedures were vague and did not provide clarity on the issue of counter-notices.
- **Lack of due process**: there was no mention of judicial review or appeal mechanisms. There was also no requirement to notify the content publisher of the alleged infringement. The 48-hour time frame for the removal of content would have been too short to allow for the submission of a counter-notice.
- **Lack of transparency**: there was no obligation to maintain records of takedown requests or provide access to such records.
- **Severe sanctions**: the harsh sanctions for false takedown notices would have been disproportionate to the purpose of deterring such.

It is apparent that the necessity and proportionality legs of the test proved to be the sticking points in relation to this Bill. While the safe harbour method might serve a legitimate aim, if the guiding regulations are not clear, necessary, and proportionate, then there is an unjustifiable limitation on freedom of expression.

[34] For a more detailed discussion on the Bill see Walubengo and Mutemi, 'Treatment of Kenya's Internet Service Providers (ISPs) under the Kenya Copyright (Amendment) Bill, 2017', The African Journal of Information and Communication, (2019) (accessible at https://journals.co.za/docserver/fulltext/afjic_n23_a5.pdf).

Ultimately, these sections of the Bill were removed, and the Act was passed in 2022 without addressing intermediary liability.

In 2015, a group of civil society organisations drafted a framework of baseline safeguards and best practices to protect human rights when intermediaries are asked to restrict online content. Known as the Manila Principles, these were drafted with the intention of being "considered by policymakers and intermediaries when developing, adopting, and reviewing legislation, policies and practices that govern the liability of intermediaries for third-party content." Advocates and litigators should similarly rely on these best practice principles, which are based on international human rights instruments and other international legal frameworks when advancing online rights.

**Manila Principles**

The key tenets of the Manila Principles on Intermediary Liability:

- Intermediaries should be shielded from liability for third-party content.
- Content must not be required to be restricted without an order from a judicial authority.
- Requests for restrictions of content must be clear, unambiguous, and follow due process.
- Laws and content restriction orders and practices must comply with the tests of necessity and proportionality.
- Laws and content restriction policies and practices must respect due process.
- Transparency and accountability must be built into laws and content restriction policies and practices.

These principles have been relied on to test state rules and to gauge whether the legal frameworks regarding intermediary liability are adequate. In 2019, the Centre for Internet and Society in India submitted a report to the Indian government comparing the Manila Principles to the draft Information Technology [Intermediary Guidelines (Amendment) Rules], 2018. These submissions provided useful guidance by highlighting provisions that were unaligned with the Manila Principles and which had the potential to infringe upon the right to freedom of expression.[35] The submission further provided recommendations to assist the Indian government in ensuring the regulations are compliant. The submissions are a useful illustration of the significance of these principles, as well as a useful resource for others who seek to test domestic legislation against international best practices.

*Conclusion*

[35] Note that the 2018 Draft Rules were subsequently replaced by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, (2021) (accessible at: https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021).

Internet intermediaries play a crucial role in the advancement of human rights. Intermediary liability needs to be understood holistically in relation to the prevention of harm, the protection of free speech and access to information, and, encouraging innovation and creativity.[36] While there is a growing trend of online harms and unlawful content:

> "The law must find a way to flexibly address these changes, with an awareness of the ways in which existing and proposed laws may affect the development of information intermediaries, online speech norms, and global democratic values."[37]

## Right To Be Forgotten

*Overview of the right to be forgotten*

The right to be forgotten, which is also described as the right to be delisted, or the right to erasure, involves an entitlement or right to request that search engines remove links to private information taking into account the right to privacy weighed against public interest considerations.[38]

**Case Note: *Google Spain SL v Agencia Española de Protección de Datos***

The right to be forgotten was given prominence following the 2014 Court of Justice of the European Union (CJEU) judgement in what has come to be known as the Google Spain case.[39] This judgement has altered the online privacy landscape and has far-reaching legal implications.

In brief, Mr Gonzalez, a Spanish national, took issue with the fact that when internet users searched his name on Google, the search results revealed a news story from 1998 regarding his debt. He requested that the personal information be removed as the matter had been resolved and was no longer relevant. The findings of the CJEU can briefly be summarised as follows:

- The CJEU held that it has jurisdiction to adjudicate the matter, search engines are data controllers, and the right to be forgotten means that personal information that is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing" must be erased by the search engine.
- The CJEU, however, ruled that the right to be forgotten should not apply to information that is relevant to the public interest.

[36] Keller, 'Build Your Own Intermediary Liability Law: A Kit for Policy Wonks of All Ages' in Li, 'New Controversies in Intermediary Liability Law Essay Collection Yale Law School' *Information Society Project*, (2019) at 20 (accessible at https://law.yale.edu/sites/default/files/area/center/isp/documents/new_controversies_in_intermediary_liability_law.pdf).
[37] Li, "Beyond Intermediary Liability: The Future of Information Platforms" Yale Law School *Information Society Project*, (2018).
[38] See Media Defence above n 2 at 35.
[39]. For a fuller case note see Media Defence above n 2 at 35.

This wide discretion for search engines to balance the competing elements of relevance and the public interest left some digital rights activists concerned. The decision also triggered a debate regarding the tension between the right to privacy and the right to freedom of expression and access to information. Some privacy proponents welcomed the legal development for creating space for people to have some level of control over their personal information, arguing that it "restores the balance between free speech and privacy in the digital world."[40] Others were more circumspect, noting that when information is delisted it affects other fundamental rights, including freedom of expression and the right to receive and impart information and ideas.[41]

*Evolution of the right to be forgotten*

Following from the abovementioned judgment, the right to be forgotten has been recognised in domestic contexts,[42] regional legislation and again by the CJEU. For example, the High Court of Orissa, India held in *Rout v State of Odisha* (2020) that the right to be forgotten is an integral part of the right to privacy. Nevertheless, some countries' courts continue to push back against such a right. In *Curi et al v Globo Comunicação e Participações S/A* (2021), the Brazilian Federal Supreme Court held that a general right to be forgotten is incompatible with the Federal Constitution.

As of 2022, Google's Transparency Report revealed that it had delisted nearly 50% of the URLs requested for removal under these terms, having received over 1.3 million requests from users to be "forgotten" since 2014. The relevance of this new right cannot be disputed; however, its scope, applicability and effects are still being debated.

In May 2018, the European Union (**EU**) elevated the status of the right through article 17 of the General Data Protection Regulation. Article 17 provides data subjects with the right to the erasure of their personal data from search engines. It further obliges search engines to erase personal data without undue delay subject to listed grounds. When erasure is required, article 17(2) stipulates that all reasonable steps must be followed – taking into account the available technology and the cost of implementation – to inform all controllers processing the personal information that any links, copies or replication of the personal data should also be erased. Article 17(3) includes instances when the right to be forgotten does not apply, namely for exercising the right of freedom of expression and information; for compliance with a legal obligation; for reasons of public interest in the area of public health; for archiving purposes in the public interest, scientific or historical research or statistical purposes; or for the establishment, exercise or defence of legal claims.

---

[40] Cook, 'The Right to be Forgotten: A Step in the Right Direction for Cyberspace Law and Policy', 6 Journal of Law, Technology & the Internet, (2015) at 121-123 (accessible at https://scholarlycommons.law.case.edu/jolti/vol6/iss1/8/).

[41] Kulk and Borgesius, 'Freedom of expression and 'right to be forgotten' cases in the Netherlands after Google Spain' 2 European Data Protection Law Review, (2015) at 116 (accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652171). See also ARTICLE 19, 'The "Right to be Forgotten": Remembering Freedom of Expression', (2016) (accessible at https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf).

[42] See Media Defence above n 2.

### Further jurisprudential developments on the right to be forgotten

In September 2019, the CJEU handed down a further ruling in *Google LLC v Commission Nationale de l'Information et des Liberties (CNIL)*. The case dealt with whether a de-listing order made in a member state of the EU meant that the search results had to be removed from all the search engine's domain name extensions globally.

In 2015, the French Data Protection Agency (**CNIL**) had requested Google to globally remove information concerning a data subject. Google refused and limited its removal only to EU member states, resulting in CNIL fining Google. Google appealed this decision. Many interested parties, including Wikimedia, Microsoft, governments of EU member states, and civil society actors made submissions to the CJEU. The CJEU acknowledged that the right to be forgotten is not globally recognised and that the competing interests between the right to privacy and freedom of expression are balanced differently across the world.

Ultimately, the CJEU found that where a search engine operator has granted a de-listing request of a data subject in an EU member state, there is no obligation under EU law for a search engine operator to be ordered to implement the de-listing on all versions of its search engine globally. The CJEU further noted that while EU law does not require de-referencing from all versions of a search engine, such a practice is not prohibited. A judicial authority of a member state remains competent to weigh up – in the light of national standards of protection of fundamental rights – a data subject's right to privacy and the protection of personal data concerning them, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order the operator of that search engine to carry out a de-referencing concerning all versions of that search engine.

Intervening parties such as ARTICLE 19 and the Electronic Frontier Foundation welcomed the ruling of the CJEU:

> "This ruling is a victory for global freedom of expression. Courts or data regulators in the UK, France or Germany should not be able to determine the search results that internet users in America, India or Argentina get to see. The Court is right to state that the balance between privacy and free speech should be taken into account when deciding if websites should be de-listed – and also to recognise that this balance may vary around the world. It is not right that one country's data protection authorities can impose their interpretation on Internet users around the world."

Other cases have also recently been added to the body of case law on this issue. In *Hurbain v Belgium*, the ECtHR held that an order enforcing the right to be forgotten of a person involved in a road accident through anonymisation did not breach the publisher's freedom of expression. In *Biancardi v Italy*, it likewise held that an online publisher's failure to comply with a de-indexing request justified restricting the publisher's freedom of expression by allowing the request.

The careful navigation of balancing privacy rights against freedom of expression will continue to pose challenges as the digital landscape continues to evolve.[43]

*The extra-territorial scope of the right to be forgotten*

In many ways, the CJEU clarified the extra-territorial scope of the right to be forgotten. The CJEU has acknowledged that states are still entitled to develop the content of this right within their respective jurisdictions, and are still at liberty to adopt different approaches when balancing the relevant rights and interests – provided that such an approach is compliant with international human rights norms.

*Opportunities and risks*

The right to be forgotten can provide important protections for privacy and can fulfil an important role in promoting agency and autonomy. State and non-state actors have far-reaching powers when it comes to the online personal information and identity of individuals. Allowing individuals to have some ownership of their personal information gives them a degree of control over their digital identities. Most online personal information has no bearing on public interest considerations and has far more intrinsic value to the individual than to society at large. The current jurisprudential and legislative developments in this regard have been sensitive to this, recognising the difference between what is of value to an individual, what is interesting to the public, and what is in the public interest.

There were concerns that an "overly expansive right to be forgotten will lead to censorship of the Internet because data subjects can force search engines or websites to erase personal data, which may rewrite history."[44] In some instances, it is permissible for individuals not to be indefinitely defined by their past. The *Google Spain* judgment provides some direction on this, where it recognised the need for relevant considerations to take place – such as the nature and sensitivity of the information, the public interest and the role played by the data subject in public life – when finding a fair balance between the right of the data subject and the interests of internet users.

Shortly after the *Google Spain* judgment, Google received an array of requests from people to have articles of their past removed from the search engine. Google's regular Transparency Reports provide some guidance on how it deals with requests, providing examples of some of the outcomes of requests for erasure. In 2017, for example, the report noted some responses to politician's requests stating "[w]e did not delist the URLs given his former status as a public figure", while another stated "[w]e delisted 13 URLs as he did not appear to be currently engaged in political life and was a minor at the time." ARTICLE 19 explains that, from a child's rights perspective, binding children to negative aspects of their past can "impede their development and diminish their sense of self-worth."

[43] For more on the importance of balancing these right see the Written Observations of ARTICLE 19 and Others, (2017) *Google LLC v Commission Nationale de l'Information et des Libertés* (CNIL), (accessible at https://www.article19.org/wp-content/uploads/2017/12/Google-v-CNIL-A19-intervention-EN-11-12-17-FINAL-v2.pdf).

[44] Michael L Rustad & Sanna Kulevska, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*", 28 Harvard Journal of Law and Technology* 349, (2017) at 373 (accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2627383).

There are legitimate benefits that accompany the right to be forgotten; however, there are also risks associated with the right, in particular around the enforcement of rights and the adverse effect this can have on the right to freedom of expression.[45] A lack of cogent regulatory safeguards can result in search engines becoming the "judge, jury, and executioner" of the right to be forgotten.[46] There are risks involved in conferring such a decision-making power on a private entity, particularly given the need to balance competing rights, an exercise traditionally reserved for courts.[47] The Electronic Frontier Foundation expressed concern that the "ambiguous responsibility upon search engines" will censor the internet.

**Ensuring adequate safeguards when implementing the right to be forgotten**

Access Now has provided some guidance on ensuring clear safeguards for the implementation of the right to be forgotten:

- A right to de-list must be limited to the sole purpose of protecting personal data.
- Criteria for de-listing must be clearly defined in comprehensive data protection legislation to avoid interference with human rights.
- Competent judicial authorities should interpret standards for determining what is de-listed.
- The right to de-list must be limited in scope and application.
- Search engines must be transparent about when and how they comply with de-listing requests.
- Users must have easy access to a remedy.

*Conclusion*

The right to be forgotten brings to the fore the tensions between the right to privacy and the right to freedom of expression and given the rapid pace at which digital space is changing, it is likely that these tensions will persist. Provided public interest overrides are prioritised and adequate safeguards are put in place, there can be some degree of consonance.

## Monitoring Obligations of Search Engines and Platforms

*Overview of monitoring obligations of search engines and platforms*

[45] Id.
[46] Forde, 'Implications of the Right to be Forgotten' 17 *Tulane Journal of Technology and Intellectual Property* 83, (2015) at 113 -114 (accessible at https://journals.tulane.edu/TIP/article/view/2652). See further Lindsay 'The 'Right to be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling' 6 *Journal of Media Law,* (2016) 159 at 173 – 174.
[47] Kuczerawy & Ausloos, 'From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain', 14 *Colorado Technology Law Journal* 219, (2016,) (accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2669471).

The internet has been described as "the greatest tool in history for global access to information and expression".[48] But it is also a powerful tool for disinformation and hate speech which have, as captured in the Joint Letter from Special Rapporteurs and experts, "exacerbated societal and racial tensions, inciting attacks with deadly consequences around the world." The increase in the spread of disinformation and the rise of the internet being used for nefarious purposes has put non-state actors in a somewhat precarious position. The UN Human Rights Office of the High Commissioner notes that along with the many opportunities associated with the internet, there are growing threats of unlawful activities online. The ease with which malicious content can spread online has posed a dilemma for states and intermediaries. On the one hand, there is a need to mitigate online harms, but on the other, in order to do so, content must not be moderated in a manner that leads to censorship and free speech violations.[49] Intermediaries are now complying with state laws concerning content regulation and are also, in some instances, acting proactively to monitor content, either of their own volition or in order to escape liability.[50]

The 2018 Report by the UNSPR noted key concerns regarding content regulation:

> "States regularly require companies to restrict manifestly illegal content such as representations of child sexual abuse, direct and credible threats of harm and incitement to violence, presuming they also meet the conditions of legality and necessity. Some [s]tates go much further and rely on censorship and criminalization to shape the online regulatory environment."

Monitoring obligations for search engines and platforms are loosely understood as general obligations imposed on intermediaries to monitor all content and filter unwanted content.[51] Intermediaries faced with these obligations are expected to develop content recognition technologies or other automatic infringement assessment systems and essentially develop and utilise filtering systems.[52] In instances where there are strict monitoring obligations, it is likely that monitoring will become the norm, opening intermediaries to automatic and direct liability.[53] Monitoring obligations raise concerns in respect of intermediary liability. It has been noted that:

> "Monitoring obligations drastically tilt the balance of the intermediary liability rules toward more restriction of speech, may hinder innovation and competition by

[48] APC, 'Reorienting rules for rights: A summary of the report on online content regulation by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', (2018) (accessible at https://www.apc.org/en/pubs/reorienting-rules-rights-summary-report-online-content-regulation-special-rapporteur-promotion).
[49] Langvardt, 'Regulating Online Content Moderation' Georgetown Law Journal 106, (2018) at 1354-1359, (accessible at https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2018/07/Regulating-Online-Content-Moderation.pdf).
[50] APC, 'Content Regulation in the Digital Age Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression', (2018) (accessible at https://www.ohchr.org/Documents/Issues/Opinion/ContentRegulation/APC.pdf).
[51] Frosio, 'From Horizontal to Vertical: an Intermediary Liability Earthquake in Europe' Centre for International Intellectual Property Studies Research Paper, (2017) at 12 (accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3009156).
[52] Id.
[53] Id

> increasing the costs of operating an online platform, and may exacerbate the broadly discussed problem of over-removal of lawful content from the Internet."[54]

Further to the above, there has been a trend, akin to that of the right to be forgotten, where states demand the global removal of content that violates domestic law.[55] Notwithstanding the recent findings of the CJEU, these demands might continue, as predicted by the UNSR in the 2018 Report, to have the chilling effect of allowing censorship across borders.

The imposition of monitoring obligations appears to have primarily been in relation to copyright infringements. However, it is growing at an unprecedented rate, causing grave concern for free expression.[56] Judgments of the European Court of Human Rights (**ECtHR**) provide useful insight into the issues regarding online platforms and liability for users' comments.

*Jurisprudential developments*

The *Delfi v Estonia* matter was the first of the prominent cases to address the issue of content moderation and online media liability. An Estonian newspaper, Delfi, published an article that was critical of a ferry company. The article received 185 comments online, some of which were targeting a board member of the company, L, and were considered threatening and/or offensive. L requested that the comments be immediately taken down and claimed approximately €32,000 in compensation for non-pecuniary damages. Delfi agreed to remove the comments but refused to pay the damages. L approached the Harju County Court, bringing a civil claim against Delfi. The County Court found that the company could not be considered the publisher of the comments, and it did not have an obligation to monitor them. L appealed to the Tallinn Court of Appeal who remitted the matter back to the County Court for reconsideration, concluding that the lower court had erred in its finding in relation to Delfi's liability. The matter eventually reached the Supreme Court, which found that there was a legal obligation to avoid causing damage to other persons and that Delfi should have prevented the clearly unlawful comments from being published. The Supreme Court noted that after the comments had been published, Delfi failed to remove them on its own initiative, although it must have been aware of their unlawfulness. Delfi's failure to act was found to be unlawful.

Delfi applied to the First Section of ECtHR, arguing that the imposition of liability for the comments violated its right to freedom of expression. The ECtHR was faced with the question of whether Delfi's obligation, as established by the domestic judicial authorities, to ensure that comments posted on its internet portal did not infringe the personality rights of third persons was in accordance with the right to freedom of expression. In order to resolve this question, the ECtHR developed a four-stage test:

- The context of the comments.
- The measures applied by Delfi in order to prevent or remove defamatory comments.

[54] Stanford Law, 'Monitoring Obligations', (2017) (accessible at https://wilmap.law.stanford.edu/topics/monitoring-obligations).
[55] See discussion above on the right to be forgotten, particularly the discussion on *Google LLC v Commission Nationale de l'Information et des Liberties (CNIL.*
[56] Frosio, 'The Death of 'No Monitoring Obligations' A Story of Untameable Monsters' *JIPITEC*, (2017) (accessible at https://www.jipitec.eu/issues/jipitec-8-3-2017/4621/JIPITEC_8_3_2017_199_Frosio).

- The liability of the actual authors of the comments as an alternative to the applicant company's liability.
- The impacts of the restrictions imposed on Delfi in a democratic society.

The ECtHR found that the restriction on Delfi's right to freedom of expression was justified and proportionate, taking into consideration the following:

- The insulting and threatening nature of the comments which were posted in reaction to an article published by Delfi;
- The insufficiency of the measures taken by Delfi to avoid damage being caused to other parties' reputations and to ensure a realistic possibility that the authors of the comments will be held liable; and
- The moderate sanction imposed on Delfi.

Following this decision by the First Section, the matter was then referred to the Grand Chamber of the ECtHR. In 2015, the Grand Chamber affirmed the judgment of the First Section. In this regard, in the 2015 *Delfi v Estonia* judgement, the Grand Chamber noted:

> "[W]hile the Court acknowledges that important benefits can be derived from the Internet in the exercise of freedom of expression, it is also mindful that liability for defamatory or other types of unlawful speech must, in principle, be retained and constitute an effective remedy for violations of personality rights."

The Grand Chamber, in determining if freedom of expression had been infringed, considered the restriction was lawful, sought to achieve a legitimate aim and was necessary in a democratic society. Ultimately the Grand Chamber concluded that Delfi was liable for defamation as the publisher of the comments. The Grand Chamber found that "an active intermediary which provides a comments section cannot have absolute liability" and noted that "freedom of expression cannot be turned into an exercise in imposing duties."

While the Grand Chamber found that the liability against Delfi had been a justified and proportionate restriction on the news portal's freedom of expression, it noted, in its appendix that:

> "We trust that this is not the beginning (or the reinforcement and speeding up) of another chapter of silencing and that it will not restrict the democracy-enhancing potential of the new media. New technologies often overcome the most astute and stubborn politically or judicially imposed barriers. But history offers discouraging examples of censorial regulation of intermediaries with lasting effects."

Shortly after the Grand Chamber's *Delfi* judgment, the Fourth Section of the ECtHR considered whether a non-profit, self-regulatory body of intermediaries (MTE) and an internet news portal (Index) were liable for offensive comments posted on their websites in *Magyar Tartalomszolgáltatók Egyesülete v Hungary*. In 2010, the two parties published an article critical of two real estate agents. The article attracted some comments that the estate agents found to be false and offensive and which, they argued, infringed on their right to a

good reputation. MTE and Index were held liable by the Hungarian courts for the comments. MTE and Index approached the ECtHR arguing that their right to freedom of expression had been violated.

The ECtHR noted that interferences with the freedom of expression must be "prescribed by law," have one or more legitimate aims, and be "necessary in a democratic society." The ECtHR applied the same four-stage test as it did in Delfi but differed from its finding in Delfi, concluding that there had been a violation of freedom of expression. The ECtHR found that:

- The comments triggered by the article can be regarded as going to a matter of public interest and while they were vulgar they were not necessarily offensive, noting that style constitutes part of the communication as the form of expression and is protected together with the content of the expression.

- The conduct of MTE and Index in providing a platform for third parties to exercise their freedom of expression by posting comments is a journalistic activity of a particular nature. It was noted that it would be difficult to reconcile MTE and Index's liability with existing case law that cautions against the punishment of a journalist for assisting in the dissemination of statements made by another person.

- MTE and Index took certain general measures to prevent defamatory comments on their portals or to remove them.

The ECtHR found that there had been a violation of freedom of expression and concluded with the following:

> "However, in the case of *Delfi,* the Court found that if accompanied by effective procedures allowing for rapid response, the notice-and-take-down-system could function in many cases as an appropriate tool for balancing the rights and interests of all those involved. The Court sees no reason to hold that such a system could not have provided a viable avenue to protect the commercial reputation of the plaintiff. It is true that, in cases where third-party user comments take the form of hate speech and direct threats to the physical integrity of individuals, the rights and interests of others and of the society as a whole might entitle Contracting States to impose liability on Internet news portals if they failed to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties. However, the present case did not involve such utterances."

It has been noted that there are some inconsistencies in the ECtHR's approach to online liability.[57] However, it does appear that the shift away from the *Delfi* reasoning was a shift in the right direction.[58] Ultimately, these cases have illustrated that even though freedom of

[57] Fahy, 'The Chilling Effect of Liability for Online Reader Comments' European Human Rights Law Review, (2017) (accessible at https://www.ivir.nl/publicaties/download/EHRLR_2017_4.pdf).
[58] Id at 3. See also Media Defence 'European Court clarifies intermediary liability standard' (2016) (accessible at https://www.mediadefence.org/news/european-court-clarifies-intermediary-liability-standard/).

expression is paramount, complete immunity is not always attainable, and there might be instances where intermediaries will be responsible for the moderation of content.[59]

*Efforts to address content moderation at the global level*

The UN Human Rights Office of the High Commissioner has noted:

> "One of the greatest threats to online free speech today is the murkiness of the rules . . . States circumvent human rights obligations by going directly to the companies, asking them to take down content or accounts without going through legal process, while companies often impose rules they have developed without public input and enforced with little clarity. We need to change these dynamics so that individuals have a clear sense of what rules govern and how they are being applied."

Alongside the considerable rights implications for the moderation of online content by intermediaries, there is a glaring lack of adequate rules, guidelines, procedures, and remedies in relation to the current practices of content moderation that are cause for concern.[60] It is clear that a human rights framework ought to guide the principles for company content moderation.

[59] For substantive commentary on the impact of these cases on intermediary liability see Maroni, 'A Court's Gotta Do, What a Court's Gotta Do. An Analysis of the European Court of Human Rights and the Liability of Internet Intermediaries through Systems Theory' EUI Working Paper (2019) (accessible at https://cadmus.eui.eu/bitstream/handle/1814/62005/RSCAS%202019_20.pdf?sequence=1&isAllowed=y).

[60] ARTICLE 19, 'Social Media Councils: Consultation' (2019) (accessible at https://www.article19.org/resources/social-media-councils-consultation/).

**Guidance from the UNSR on ensuring compliance with human rights standards when online content is being moderated**

These guidelines and recommendations are based on the Guiding Principles on Business and Human Rights as well as established international law, norms, and practices. These can be used when engaging with state and non-state actors to ensure compliance with human rights standards when online content is being moderated. Below is an outline of some of the key recommendations:

1. **Human rights by default**: Companies should incorporate directly into their terms of service and community standards relevant principles of human rights law that ensure content-related actions will be guided by the same standards of legality, necessity and legitimacy that bind state regulation of expression.

2. **Legality**: Company rules routinely lack the clarity and specificity that would enable users to predict with reasonable certainty what content places them on the wrong side of the line. Companies should supplement their efforts to explain their rules in more detail with aggregate data illustrating trends in rule enforcement, and examples of actual cases or extensive, detailed hypotheticals that illustrate the nuances of interpretation and application of specific rules.

3. **Necessity and proportionality**: Companies should not only describe contentious and context-specific rules in more detail; they should also disclose data and examples that provide insight into the factors they assess in determining a violation, its severity and the action taken in response.

4. **Non-discrimination**: Meaningful guarantees of non-discrimination require companies to transcend formalistic approaches that treat all protected characteristics as equally vulnerable to abuse, harassment and other forms of censorship.

**UNSR guidance on the processes for company moderation and related activities**

These guidelines and recommendations provide further guidance on the processes for company moderation and related activities:

1. **Prevention and mitigation**: Companies should adopt and then publicly disclose specific policies that "direct all business units, including local subsidiaries, to resolve any legal ambiguity in favour of respect for freedom of expression, privacy, and other human rights". Companies should also ensure that requests are in writing, cite specific and valid legal bases for restrictions and are issued by a valid government authority in an appropriate format.

2. **Transparency**: Best practices on how to provide such transparency should be developed. Companies should also provide specific examples as often as possible and should preserve records of requests made.

3. **Due diligence**: Companies should develop clear and specific criteria for identifying activities that trigger assessments and assessments should be ongoing and adaptive to changes in circumstances or operating context.

4. **Public input and engagement**: Companies should engage adequately with users and civil society, particularly in the global south, to consider the human rights impact of their activities from diverse perspectives.

5. **Rule-making transparency**: Companies should seek comment on their impact assessments from interested users and experts when introducing products and rule modifications. They should also clearly communicate to the public the rules and processes that produced them.

6. **Automation and human evaluation**: Company responsibilities to prevent and mitigate human rights impacts should take into account the significant limitations of automation and, at a minimum, technology developed to deal with considerations of scale should be rigorously audited and developed with broad user and civil society input.

7. **Notice and appeal**: Companies could work with one another and civil society to explore scalable solutions such as company-specific or industry-wide ombudsman programmes and the promotion of remedies for violations.

8. **Remedy**: Companies should institute robust remediation programmes, which may range from reinstatement and acknowledgement to settlements related to reputational or other harms.

9. **User autonomy**: While content rules in closed groups should be consistent with baseline human rights standards, platforms should encourage such affinity-based groups given their value in protecting opinion, expanding space for vulnerable communities and allowing the testing of controversial or unpopular ideas.

The UNSR goes on to provide specific recommendations, imparting the urgent need for "radical transparency, meaningful accountability and a commitment to remedy in order to protect the ability of individuals to use online platforms as forums for free expression, access to information and engagement in public life".

## Conclusion

The growing power of private actors within the internet and technology sphere raises new questions with regard to the protection of freedom of expression in the modern age. Private actors have gained the ability to filter and control the flow of information to internet users, raising questions about net neutrality, and complex challenges with regard to enabling access to the internet and to information in developing countries, while maintaining the free and unhindered flow of information.

These powerful actors, along with online news publishers and a host of other internet intermediaries, have also become responsible for hosting huge quantities of information created and posted by regular users, raising questions about how responsibility should be apportioned for illegal or damaging content online. In particular, concerns have been raised that apportioning liability to intermediaries risks creating a digital ecosystem in which freedom of expression is routinely and structurally stymied because of fears of being held liable.

The right to privacy and the protection of personal information has come up against the free flow of information in the issue now known as 'the right to be forgotten,' which has begun to be dealt with at length in regional and domestic courts. This issue relates closely to that of the content moderation obligations of private platform providers and search engines, who must make influential decisions on a daily basis as to what content will be allowed and what will be removed, with significant consequences for the right to freedom of expression in the digital age.

As a result, it is vital that mechanisms and processes for greater transparency and accountability over the decisions of these powerful, private actors be put in place in order to ensure alignment with international human rights law and standards on freedom of expression and access to information.

*Module 6*

# Litigating Digital Rights Cases in Africa

*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 6

## Litigating Digital Rights Cases in Africa

**The objectives of this module are:**

- **To provide an overview of key concepts and procedural requirements.**
- **To set out the stages of litigation at the African Commission on Human and Peoples' Rights.**
- **To set out the stages of litigation at the African Court on Human and Peoples' Rights.**
- **To set out the stages of litigation at the East African Court of Justice.**
- **To set out the stages of litigation at the ECOWAS Community Court of Justice.**
- **To examine the current status of the SADC Tribunal.**
- **To identify practical steps to litigating digital rights cases.**

---

## Introduction

Effective litigation can achieve profound systemic change. Although litigation can be a protracted and costly process, under the right circumstances it can contribute meaningfully to the evolution of legal frameworks that truly ensure that human rights are respected, protected, and promoted. Strategic litigation has been instrumental in advancing freedom of expression and digital rights in many jurisdictions, and the myriad contemporary challenges to human rights online call for new and innovative uses of strategic litigation to hold both state and non-state actors accountable.

This module seeks to outline some of the basic principles in litigation and gives an overview of litigating in various courts across the African continent. It concludes with some practical tips on establishing a litigation strategy.

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

- Media Defence Report Mapping digital rights and online freedom of expression in East, West, and Southern Africa.
- Media Defence manual on litigating freedom of expression cases in East Africa.
- Media Defence West Africa Regional Mechanisms Manual.
- Media Defence Digital Rights Litigation Guide.
- Media Defence Summary Module 10: Introduction to Litigating Digital Rights in Africa.

## Overview of Key Concepts

Below is a brief overview of some of the procedural requirements for any litigation strategy. The specific procedures of the various courts will be further detailed in their respective sections below.

*Standing*

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

**Some points to consider when assessing standing:**

- Is an individual, community or civil society organisation best placed to bring the matter to the court or forum?
- Would a combination of different applicants be strategic?
- What are the different interests in the matter?
- What are the different risks of instituting a matter?
- What is in the best interest of the case?
- What are the resources or capacity constraints?

*Jurisdiction*

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

*Admissibility*

Admissibility refers to the process applied by international human rights fora to ensure that only cases that need international adjudication are brought before them. It is, therefore, the essence of the principle of subsidiarity. The principle of admissibility requires that all local remedies are exhausted and that consideration be given to whether there are rules relating to prescription and whether the forum recognises the concept of ongoing harm.

**Some points to consider when assessing admissibility**

- What are the possible local remedies available?
- Are local remedies efficient and reasonable?
- Is there existing case law in the court on the admissibility of cases in relation to exhausting local remedies?
- Is it practical for the domestic forum to be seized with the matter?
- Are there prescribed time frames?
- Is the harm ongoing?
- Have efforts been taken to appeal initial decisions?
- Is there a mechanism for direct access?

*Representation*

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

**Some points to consider when assessing representation**

- Is there a restriction on having legal representation?
- What resources are available for legal representation?
- Who would be best placed to assist with legal representation?

*Amicus curiae*

An *amicus curiae* is a 'friend of the court'. It is not a main party to the litigation but is accepted by the court or forum to join the proceedings to advise and assist it in respect of a question of law or other issues that affect the case in question. Some individuals, communities or organisations might have first-hand or expert knowledge on a particular topic; their involvement could be of assistance to the court or forum. Interested parties usually need to apply to the court or forum requesting permission to intervene in the matter and typically need to prove that they have an interest in it, that their submissions will be of use to the court or forum, and that they will not be repeating the arguments of the main litigants. However, each court or forum may have its own rules on the admission of *amici*. Courts and fora usually have the discretion to grant or refuse an *amicus* application. *Amicus* interventions can be particularly useful when litigating digital rights matters as there is often a need for technical and expert analysis given the rapid pace of change in the digital environment.

**Some points to consider when assessing *amicus curiae***

- Is there something additional and useful that should be brought to the court's or forum's attention?
- Are there individuals, communities or organisations who might have particular knowledge or interest in a matter?
- Would the *amicus* be neutral, or would the *amicus* be supportive of a particular party?

## Litigating at the African Commission on Human and Peoples' Rights

*Overview of the African Commission on Human and Peoples' Rights*

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

- The protection of human and peoples' rights.
- The promotion of human rights.
- The interpretation of the African Charter.

The ACHPR consists of eleven members elected by the African Union Assembly from experts nominated by states which are party to the African Charter. The ACHPR holds two ordinary sessions annually, which vary from 10 to 15 days, depending on needs and finances, and the ACHPR may also meet in extraordinary sessions, if necessary.

**Examples of cases heard by the African Commission on Human and Peoples' Rights**

*Good v. Botswana*

In 2005, the Botswanan government ordered the deportation of an Australian national in response to his co-authoring a publication that criticised the nature of political succession in Botswana. The ACHPR ruled that the order was a violation of the rights to freedom of expression and access to information, as well as of the right to a fair trial. It held that the publication had not been shown to threaten national security, and as such the deportation order was "unnecessary, disproportionate and incompatible with the practices of democratic societies, international human rights norms and the African Charter in particular".[1] This case sheds light in particular on the use of national security justifications for infringements on freedom of expression, and the protection that should be afforded to dissenting views, even those that the government may consider to be offensive.

[1] Global Freedom of Expression at Columbia University, 'Good v Botswana,' (2010) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/good-v-botswana/).

*Scanlen & Holderness v. Zimbabwe*

Several media advocacy groups in Zimbabwe challenged provisions in the country's Access to Information and Protection of Privacy Act (**AIPPA**) that required all journalists to register with the Media and Information Commission and imposed punishments of up to two years imprisonment for "abusing journalistic privilege" which included the publication of false news, on the grounds that they infringed the right to freedom of expression. The ACHPR held that "registration procedures are not in themselves a violation of the right to freedom of expression, provided they are purely technical and administrative in nature and do not involve prohibitive fees, or […] impose onerous conditions", but that the imposition of onerous conditions and the control of journalists by a non-independent body with the aim of controlling rather than regulating the journalism profession did infringe the rights to freedom of expression and to receive information.[2] This decision is instructive with regard to journalism registration schemes, as well as public order justifications for infringements on freedom of expression.

*Zimbabwe Lawyers for Human Rights v. Zimbabwe*

A US citizen living as a permanent resident in Zimbabwe was charged with contravening legal provisions outlawing the publication of falsehoods also in the AIPPA. He was acquitted of those charges but was subsequently deported, despite the AIPPA being declared unconstitutional in a separate case a week before the deportation and the existence of court orders prohibiting his deportation. The ACHPR held that as the deportation "arose from the publication of an article that the Respondent State did not appreciate", it followed that "[the applicant's] ability to express himself as guaranteed under article 9 was violated", recommending that Zimbabwe rescind the deportation order and permit him to return as a permanent resident.[3] This ruling provides insight into how the ACHPR approaches questions related to due process in the context of freedom of expression and provides a strong endorsement of the importance of protecting critical speech.

Beyond the obligation to consider reports submitted by states, and shadow reports submitted by civil society organisations (**CSOs**) regarding states' compliance with the African Charter, the ACHPR is empowered to receive and consider communications. Filing a communication is essentially the same as filing a complaint. Communications are the mechanism through which the ACHPR fulfils its function to protect the rights and freedoms guaranteed in the African Charter. Article 55 of the African Charter empowers the ACHPR to consider communications.

There are several stages involved in the communications process, which are governed by the Communication Procedure. The Rules of Procedure regulate the ACHPR and establish the

[2] Global Freedom of Expression at Columbia University, 'Scanlen & Holderness v. Zimbabwe,' (2009) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/scanlen-holderness-v-zimbabwe/).
[3] Global Freedom of Expression at Columbia University, 'Zimbabwe Lawyers for Human Rights v. Zimbabwe,' (2009) (accessible at: https://globalfreedomofexpression.columbia.edu/cases/zimbabwe-lawyers-human-rights-v-zimbabwe/.)

procedure in accordance with article 42(2) of the African Charter on Human and Peoples' Rights.

### Stage 1: Registering the Communication

This stage is similar to filing a complaint or launching proceedings in a domestic court or forum. The communication must identify the parties and set out the alleged violation. Communications are usually directed to the Secretariat of the ACHPR, which is based in Banjul, The Gambia.

The communication should include:

- Identifying features of the person or organisation filing (e.g. name, nationality, address where correspondence can be received).
- Whether the identifying features should remain anonymous from the state.
- The state alleged to have committed the violation.
- The reason for registering the communication (if being for the public good or on behalf of someone).
- A description of the violation.
- Other steps taken before reaching this point.

Essentially, the communication should include all relevant information that would allow the ACHPR to make a determination as to whether it should engage with the matter.

This stage incorporates important standing considerations. The ACHPR has broad standing provisions. Anyone can register a communication, including CSOs. This includes a state claiming that another state party to the African Charter has violated one or more of the provisions in the African Charter; CSOs (which do not need to be registered with the AU or have observer status); victims of abuses; or interested individuals acting on behalf of victims of abuses. The matter can also be brought for the public good, as class or representative actions, under the *actio popularis* approach.[4]

In *Article 19 v Eritrea*, the ACHPR noted that it—

> "has adopted an *actio popularis* approach where the author of a communication need not know or have any relationship with the victim. This is to enable poor victims of human rights violations on the continent to receive assistance from NGOs and individuals far removed from their locality. All the author needs to do is to comply with the requirements of Article 56. The African Commission has thus allowed many communications from authors acting on behalf of victims of human rights violations. Thus, having decided to act on behalf of the victims, it is incumbent on the author of a communication to take concrete steps to comply

[4] For more on standing see Pedersen, 'Standing and the African Commission on Human and Peoples' Rights' African Human Rights Law Journal (2006) (accessible at https://www.ahrlj.up.ac.za/pedersen-m-p) and Mayer, 'NGO Standing and Influence in Regional Human Rights Courts and Commissions' Notre Dame Law School (2011) (accessible at https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1053&context=law_faculty_scholarship).

with the provisions of Article 56 or to show cause why it is impracticable to do so."

This was reiterated in *Law Society of Zimbabwe and Others v Zimbabwe*, in which the AHCPR noted that although the African Charter does not explicitly define who is eligible to file complaints, the *actio popularis* approach allows the ACHPR to adopt a flexible approach which enables everyone including non-victim individuals, CSOs and pressure groups with an interest in the matter to file a communication, for its consideration.

It is not necessary for cases to be submitted by lawyers, although legal representation can be helpful. The Communication Procedure states that the preparation, submission, and processing of a communication is a relatively straightforward procedure, and that a complainant or author can act on their own without the need for professional assistance – but that legal representation can be useful, particularly for the interpretation of rights violations and the development of arguments in support of such violations.

### Emergency situations

Every communication should indicate if there is an imminent threat to the life, health, or personal integrity of a person. The Rules of Procedure provide guidance on matters of emergency.

#### Rule 79: Decision on matters of emergency

1. The Commission shall treat a situation as a matter of emergency under Article 58(3) of the African Charter, when:
   a. it is one of serious or massive human rights violations;
   b. it presents the danger of irreparable harm or requires urgent action to avoid irreparable damage;
2. When a situation of emergency arises during a session of the Commission, the decision to treat it as such shall be taken by the Commission.
3. When a situation arises during the Commission's inter-session period, the decision to treat it as a matter of emergency shall be taken by the Bureau of the Commission, which shall keep other members of the Commission informed and present a report on the situation at the next session of the Commission.

#### Rule 80: Action on matters of emergency

1. When the Commission has decided to treat a situation as one of emergency, it shall:
   a. Draw the attention of the Chairperson of the Assembly of Heads of State and Government of the African Union to the matter in accordance with Article 58(3) of the Charter;
   b. Draw the attention of the Peace and Security Council to the matter in accordance with Article 19 of the Protocol on Peace and Security Council;
   c. Inform the Executive Council;
   d. Inform the Chairperson of the African Union Commission of the matter.
2. The Commission as well as its subsidiary mechanisms under the Charter and present Rules shall also take any appropriate action, including Urgent Appeals.

## Stage 2: Seizure and admissibility

Once it has been filed, the ACHPR will seize itself of the communication (i.e. it will consider the complaint) if it is satisfied that the communication alleges a *prima facie* violation of the African Charter, and it has been properly submitted.

The Secretariat of the Commission will issue a letter to the complainant acknowledging receipt of the communication. At this stage, a letter is sent to the state party concerned.

Article 55(2) of the African Charter requires that a decision by a simple majority of commissioners is needed for the ACHPR to be seized with a matter. Once the ACHPR has confirmed that it is seized with the matter, it will then proceed to consider whether the communication is admissible. There are seven formal requirements in terms of article 56 of the African Charter that must be met for a communication to be admissible:

- **Article 56(1) – Indicate the authors**: include your name and address and, if you are not the victim yourself, your relationship with the victim, including on what grounds you represent the victim.
- **Article 56(2) – Compatible with the Constitutive Act of the AU or with the African Charter**: the communication needs to explicitly and clearly discuss the specific violation of rights guaranteed in the African Charter.
- **Article 56(3) – Non-insulting language**: the language should not be aimed at undermining the integrity and status of the institution.
- **Article 56(4) – Evidence other than simply news sources**: the communication should not be based exclusively on news disseminated through the mass media. The evidence must be asserted at this stage but can be presented later.
- **Article 56(5) – Exhaustion**: local remedies must be exhausted before submitting the communication.
- **Article 56(6) – Timeliness**: the communication must be submitted within a reasonable period from the time that local remedies are exhausted
- **Article 56(7) – No conflicting settlements**: the ACHPR does not deal with matters which have been settled by another international mechanism similar to the ACHPR.

These requirements are similar to those listed above at stage 1. Accordingly, it is important at stage 1 to ensure that all relevant information is included to ensure that the admissibility threshold at stage 2 will be met.

The exhaustion of local remedies is often a stumbling block for litigants but is important to observe. The reason behind this requirement links to the principle of subsidiarity, and the need to notify a state of its failure and afford it an opportunity to rectify the violation before escalating the matter. It also ensures that the ACHPR does not become a forum of first instance for cases for which an effective domestic remedy exists.

In *Sir Dawda K. Jawara v The Gambia*, the ACHPR explained that a domestic remedy is "considered **available** if the petitioner can pursue it without impediment, it is deemed **effective** if it offers a prospect of success, and it is found **sufficient** if it is capable of redressing the complaint". The ACHPR went on to give examples of when a remedy would not be available:

- Where the jurisdiction of the courts has been ousted by decrees whose validity cannot be challenged or questioned.
- If the applicant cannot turn to the judiciary of his or her country because of a generalised fear for their life.
- A remedy that has no prospect of success does not constitute an effective remedy.

The ACHPR gave further guidance on admissibility and, in particular, the exhaustion of local remedies in the decision in the case of *SERAC* v Nigeria:

- If a local remedy is unduly prolonged it is not an effective remedy.
- If a right is not well provided for in domestic law, there cannot be effective remedies or any remedies at all.

If a communication is declared inadmissible, the ACHPR will provide reasons for the decision, and this will bring the consideration of the communication to a close. Rule 108 of the Rules of Procedure allows for this decision to be reviewed at a later date if the complainant can provide information to the effect that the grounds for inadmissibility no longer exist.

### Stage 3: Proceedings and consideration of the matter

Following a confirmation of admissibility, the ACHPR will give the parties time to present their written arguments. Rule 108 provides for the consideration of the substantive issues of the matter:

- Once a communication has been declared admissible, the ACHPR shall set a period of sixty (60) days for the Complainant to submit observations on the merits. These observations shall be transmitted to the State Party concerned for the submission of its observations within sixty (60) days.
- Any written statements submitted by the State Party concerned shall be communicated, through the Secretary, to the Complainant, who may submit any additional written information or observations within thirty (30) days. This time limit cannot be extended.

This entails examining the allegations made and the defences raised with due regard to the provisions of the African Charter and other international human rights norms. The Communications Procedure explains that the Secretariat will prepare a draft decision on the merits for the guidance of the Commissioners.

Rule 88 of the Rules of Procedure allows for oral hearings. However, the ACHPR tends to prefer deciding matters on the papers. It is advisable to only insist on an oral hearing if there are exceptional circumstances to argue or an argument to make that is new to the ACHPR. If an oral hearing does take place, some states send representatives to contest allegations, while some do not. Where an oral hearing takes place, it is advisable to be thoroughly prepared to respond to questions from the commissioners at the hearing of the matter and to prepare the evidence on the basis that the state will be well-represented. CSOs and other interest parties who have been admitted as an *amicus curiae* can also make representations at this stage.

**Note on *amici curiae***

Rule 99(16) of the Rules of Procedure provides for the ACHPR to receive *amicus curiae* briefs on communications. During the hearing of a communication in which an *amicus curiae* brief has been filed, the Commission, where necessary shall permit the author of the brief or the representative to address the Commission.

When considering the matter, the ACHPR will have regard to certain sources of law. Article 60 provides:

> "The Commission shall draw inspiration from international law on human and peoples' rights, particularly from the provisions of various African instruments on human and peoples' rights, the Charter of the United Nations, the Charter of the Organization of African Unity, the Universal Declaration of Human Rights, other instruments adopted by the United Nations and by African countries in the field of human and peoples' rights as well as from the provisions of various instruments adopted within the Specialized Agencies of the United Nations of which the parties to the present Charter are members."

Article 61 allows the Commission to consider, as a subsidiary measure:

> "[O]ther general or special international conventions, laying down rules expressly recognized by member states of the Organization of African Unity, African practices consistent with international norms on human and people's rights, customs generally accepted as law, general principles of law recognized by African states as well as legal precedents and doctrine."

After an evaluation of the factual and legal arguments put forward, the ACHPR will make a determination on whether there has been a violation of the African Charter or not. If it finds a violation, a recommendation will then be made.

Amicable settlements are also provided for in the Rules of Procedure. Rule 109 allows the ACHPR, on its own initiative or at the request of any of the parties concerned, to offer its offices for an amicable settlement between the parties. When reaching an amicable settlement, the Commission shall ensure that such amicable settlement:

- Complies with or respects the human rights and fundamental freedoms enshrined in the African Charter and other applicable instruments.
- Indicates that the victim of the alleged human rights violation or, his/her successors, as the case may be, have consented to the terms of the settlement and are satisfied with the conditions.
- Includes an undertaking by the parties to implement the terms of the settlement.

## Stage 4: Recommendations

The final determination of the ACHPR is called a recommendation. A recommendation usually includes:

- A decision on admissibility.
- An interpretation of the provisions invoked.
- A discussion on the alleged violation.
- If a violation is found, what the required actions are for the state to remedy the violation.

The recommendations are not legally binding but can become binding if they are adopted by the African Union Assembly of Heads of State and Government, pursuant to article 59 of the African Charter.

Rule 98 provides that remedies can be provisional in nature with the aim of mitigating against irreparable harm to the victims of the alleged violation as urgently as the situation demands. This can take place at any time after the receipt of a communication and before a determination on the merits, at the discretion of the ACHPR or at the request of one of the parties.

Some of the past recommendations included compensation, the repeal of legislation, the return of deportees, the granting of citizenship, and the reform of electoral laws. The ACHPR does not have the discretion to create remedies beyond what has been asked for by the parties.[5] Therefore, it is important to craft remedies in a way that is clear, concise and includes all the relief that is being sought.

## Stage 5: Enforcement

There are no procedures to supervise the implementation of the ACHPR recommendations; however, the Secretariat typically issues correspondence to states that have been found to have violated provisions of the African Charter which calls upon them to honour their obligations.

[5] Media Defence, 'Digital Rights Litigation' (accessible at https://www.mediadefence.org/sites/default/files/resources/files/MLDI%20Digital%20Rights%20Litigation%20Guide.pdf).

### Commentary on the contribution of the ACHPR

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

Manisuli Ssenyonjo has taken the following view in relation to the impact of the ACHPR as well as some of the challenges it faces.

> "While there is much progress still to be made, the African Commission has greatly contributed to the regional protection of human rights in Africa. The Commission has exposed human rights violations in most authoritarian African States. Through its decisions on communications, it has developed human rights jurisprudence in Africa on several aspects consistent with the jurisprudence of other human rights bodies. These include jurisprudence on exhaustion of local remedies, State obligations concerning civil and political rights, economic, social and cultural rights as well as group rights such as indigenous peoples' rights and the right to development. Nevertheless, the African Commission has only received and decided very few communications related to economic, social and cultural rights.
>
> Initially, it was thought the Commission would be unable to hold States accountable for violations of human rights and to provide reparations to victims. However, over the years the Commission has confronted human rights violations through its decisions on communications; adoption of resolutions, principles/guidelines, general comments, model laws and advisory opinions; special rapporteurs and working groups to deal with thematic human rights issues; conducting on-site visits; consideration of State reports and adoption of concluding observations; as well as the referral of communications to the African Court.
>
> Nevertheless, compliance with the Commission's 'requests' for provisional measures/letters of urgent appeals, decisions and recommendations of the Commission, as set out in the Communications and concluding observations on State reports, has been low. The insufficient funding of the Commission from the member States budget and human crisis at the Commission's Secretariat, impedes the Commission's capacity to follow-up on implementation as it prevents the Commission from developing effective follow up of its findings during country visits, and recommendations arising from its findings, resulting in the overall weakening of the effectiveness of the Commission."

*Practicalities of litigating before the ACHPR*

There are some practical considerations that potential litigants should bear in mind when exploring an application to the ACHPR, including[6]:

- **Cost**: The ACHPR is a relatively cost-effective mechanism, given that legal representation is not a requirement, and complainants do not have to travel to the Commission as everything can be addressed through written submissions. Cost implications do, however, arise when there are oral hearings, as this requires being present at the ACHPR.
- **Timing**: The duration of the process from beginning to end varies depending on the nature of the matter. The 60-day and 30-day time periods allocated to the parties are relatively standard, but it can take several years for the final communication to be delivered.
- **Enforcement**: If a state respondent does not comply with the recommendations, it is usually up to the complainant to address enforcement. This can include engaging directly with the state itself or turning to the national parliament or domestic courts.

## Litigating at the African Court on Human and Peoples' Rights

*Overview of the African Court on Human and Peoples' Rights*

The African Court became operational in 2009. Its mandate is to adjudicate matters dealing with states' compliance with the African Charter and other instruments on the protection of human rights ratified by that state.[7] The African Court was established by African countries to ensure the protection of human and peoples' rights in Africa. It complements and reinforces the functions of the ACHPR. The African Court has different procedures to the ACHPR, which are laid out in the African Court Protocol and the Rules of Court.

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

> "Pursuant to Article 2 of the Protocol, the Court is established to complement the protective mandate of the Commission. The African Commission can bring cases to the Court for the latter's consideration. In certain circumstances, the Court may also refer cases to the Commission, and may request the opinion of the latter when dealing with the admissibility of a case. The Court and the Commission have met and harmonised their respective rules of procedure, and institutionalised their relationship. In terms of their Rules, the Commission and

[6] See Egyptian Initiative for Personal Rights, 'Filing a Communication before the African Commission on Human and Peoples' Rights' (2013) (accessible at https://eipr.org/en/press/2016/09/guide-filing-complaints-achpr).
[7] International Federation for Human Rights, 'Practical Guide: The African Court on Human and Peoples' Rights towards the Africa Court of Justice and Human Rights' (2010) (accessible at https://www.fidh.org/IMG/pdf/african_court_guide.pdf).

the Court shall meet at least once a year, to discuss questions relating to their relationship."[8]

### Examples of cases before the African Court on Human and Peoples' Rights

*Ingabire Victoire Umuhoza v. The Republic of Rwanda*

In 2010 the Rwandan authorities charged Ingabire Victoire Umuhoza, a politician, with:

- Spreading the ideology of genocide.
- Aiding and abetting terrorism, sectarianism, and divisionism.
- Undermining the internal security of a state, and spreading of rumours likely to incite the population against political authorities and mount citizens against one another.
- Establishing an armed branch of a rebel movement.
- Attempting recourse to terrorism, force of arms, and such other forms of violence to destabilise established authority and violate constitutional principles.

In 2012, the High Court of Kigali found the applicant guilty. This was appealed to the Rwandan Supreme Court, which in 2018 found Ms Umuhoza guilty of conspiracy to undermine the government and the Constitution through acts of terrorism, war, or other violent means, of downplaying genocide, and of spreading rumours with the intent to incite the population against the existing authorities, and sentenced her to 15 years' imprisonment.

After exhausting all internal remedies, Ms Umuhoza approached the African Court on Human and Peoples' Rights (**African Court**) alleging an array of rights violations, including a violation of her right to freedom of expression.

The domestic charges for minimisation of genocide related to public remarks she made about the Rwandan genocide alleging that crimes against humanity had been committed against the Hutu people, not only the Tutsi. The state respondent argued that the "right to express one's opinion is subject to limitations and that considering the social context, the history of and environment in Rwanda, there was reason to enact laws to penalise the minimisation of genocide". The State Respondent urged the African Court not to view free expression in a vacuum and to give due regard to the context within which the remarks were made.
The African Court recognised the importance of the right to freedom of expression but noted further that this right can be subject to limitations. The Africa Court confirmed that the conviction was a limitation of Ms Umuhoza's free speech and sought to establish if it was a legitimate, necessary, and proportional restriction.

The African Court found that the laws that criminalise certain speech satisfied the legal leg of the test. On legitimacy, the African Court found that the restrictions on Ms Umuhoza's free speech served the legitimate interest of protecting national security and public order.

[8] African Court on Human and People's Rights, 'Frequently Asked Questions' (accessible at https://en.african-court.org/index.php/faqs/frequent-questions).

In terms of necessity and proportionality, the African Court recognised the particular context of the Rwandan genocide, which warranted measures to be adopted by the government to promote social cohesion and concordance among the people. The African Court found that it was "entirely legitimate for the state to have introduced laws on the 'minimisation', 'propagation', or 'negation' of genocide". According to the African Court, statements that "deny or minimise the magnitude or effects of the genocide or that unequivocally insinuate the same fall outside the domain of the legitimate exercise of the right to freedom of expression and should be prohibited by law".

After consideration of these specific remarks, the African Court found that the remarks did not deny or undermine the genocide committed against the Tutsis. Accordingly, Ms Umuhoza's conviction was found to violate her right to freedom of expression, and it was ordered that the respondent state take all necessary measures to restore her rights and submit a report on the measures within 6 months.

Article 5(3) of the African Court Protocol provides that: "The Court may entitle relevant Non-Governmental Organizations (**NGOs**) with observer status before the Commission, and individuals to institute cases directly before it, in accordance with article 34(6) of this Protocol." In November 2018, The Gambia became the ninth country to allow non-governmental organisations and individuals to access the African Court directly.[9] However, in 2019, Tanzania withdrew the right of individuals and NGOs to directly file cases against it.[10]

### Stage 1: Filing a case

For applications by individuals and NGOs, the application must:

- Disclose the identity of the applicant, even where the applicant has requested anonymity.
- Comply with the Constitutive Act of the African Union and the African Charter.
- Not contain any disparaging or insulting language.
- Not be based exclusively on news disseminated through the mass media.
- Be filed after exhausting local remedies, if any, unless it is obvious that this procedure is unduly prolonged.
- Be filed within a reasonable time from the date local remedies were exhausted or from the date set by the Court as being the commencement of the time limit within which it shall be seized with the matter.

[9] African Court on Human and Peoples' Rights 'The Gambia becomes the ninth country to allow NGOs and individuals to access the Court directly' (2018) (accessible at https://www.african-court.org/en/index.php/news/press-releases/item/257-the-gambia-becomes-the-ninth-country-to-allow-ngos-and-individuals-to-access-the-african-court-directly).
[10] Amnesty International, 'Tanzania: Withdrawal of individual rights to African Court will deepen repression' (2019) (accessible at https://www.amnesty.org/en/latest/news/2019/12/tanzania-withdrawal-of-individual-rights-to-african-court-will-deepen-repression/).

- Not raise any matter or issues previously settled by the parties in accordance with the principles of the Charter of the United Nations, the Constitutive Act of the African Union, the provisions of the African Charter or any legal instrument of the African Union.[11]

The Practice Directions Guide to Litigants provides some useful guidance on filing a submission. The submissions must be made in writing and submitted to the seat of the African Court, which is at Arusha, Tanzania, and can be submitted by post, email, fax, or courier. Only one copy needs to be submitted. This copy must be in one of the official languages of the Court (Arabic, English, French and Portuguese). The copy needs to be signed by the applicant or representative and needs to give the details of the parties and indicate the alleged violations as well as the order sought. The submission needs to be accompanied by proof of exhaustion of local remedies. Submissions should be filed within a reasonable time from the date when local remedies were exhausted.

### Stage 2: Standing

Article 5 of the Protocol indicates who can submit a case to the African Court:

- The ACHPR.
- The state party that had lodged a complaint to the ACHPR.
- The state party against which the complaint has been lodged at the ACHPR.
- The state party whose citizen is a victim of human rights violation.
- African intergovernmental organisations.
- A state party with an interest in a case, on submission of a request to the African Court to be permitted to join.
- NGOs with observer status before the ACHPR and individuals, but only against states that have made a declaration accepting the competence of the African Court to receive such cases in accordance with Article 34(6) of the African Court Protocol.

The standing provisions are relatively straightforward save for the complications and challenges presented by article 34(6), which make it difficult for individuals or NGOs to rely on this forum if the state alleged to have committed violations has not made the necessary declaration.

In respect of legal representation, rule 22 provides that "[e]very party to a case shall be entitled to be represented or to be assisted by legal counsel and/or by any other person of the party's choice".

[11] African Court on Human and People's Rights 'What are the conditions for sending an Application? (accessible at https://en.african-court.org/index.php/faqs/frequent-questions#conditions).

## Stage 3: Jurisdiction

### Note on *amici curiae* in the African Court

*Amici curiae* are permitted in the African Court. Rule 45(1) of the African Court Rules provides that the African Court may decide to hear "as a witness or expert or in any other capacity any person whose evidence, assertions or statements it deems likely to assist it in carrying out its task". The African Court is also empowered in terms of rule 45(2) to ask any person or institution to obtain information, express an opinion or submit a report to it at any point. In addition to providing written submissions, *amici curiae* may also be invited to make oral submissions at the hearing of the matter.

The procedure for making a request to act as *amicus curiae* is contained in sections 42 to section 47 of the Practice Directions of the African Court. An individual or organisation wishing to act as *amicus curiae* must submit a request to the African Court, specifying the contribution that they would like to make with regard to the matter. If the African Court decides to grant the request, the person or organisation making the request will be notified by the Registrar and invited to make submissions and provided with all pleadings. The Practice Directions make clear that the decision on whether or not to grant a request to act as *amicus curiae* is at the discretion of the African Court.

At the African Court, jurisdiction needs to be established alongside the determination of admissibility. This is different to the ACHPR. The African Court's jurisdiction is contained in article 3 of the African Court Protocol, which provides as follows:

> "(1) The jurisdiction of the Court shall extend to all cases and disputes submitted to it concerning the interpretation and application of the Charter, this Protocol and any other relevant Human Rights instrument ratified by the States concerned.
> (2) In the event of a dispute as to whether the Court has jurisdiction, the Court shall decide."

Article 26 of the Rules of Court stipulates that the African Court shall have jurisdiction over the following:

- To deal with all cases and all disputes submitted to it concerning the interpretation and application of the Charter, the Protocol and any other relevant human rights instrument ratified by the States concerned.
- To render an advisory opinion on any legal matter relating to the Charter or any other relevant human rights instruments, provided that the subject of the opinion is not related to a matter being examined by the Commission.
- To promote amicable settlement in cases pending before it in accordance with the provisions of the Charter.
- To interpret a judgment rendered by itself.
- To review its own judgment in light of new evidence in conformity with rule 67 of these Rules.

In 2014, the African Court in *Konaté v. Burkina Faso* developed its jurisdictional scope as follows:

- ***Ratione personae***: The African Court must have jurisdiction over both the complainant and the respondent state. This only arises if the case is brought by an entity contemplated in article 5 of the African Court Protocol, or by an African organisation seeking an advisory opinion.

- ***Ratione materiae***: This requires the African Court to consider whether the acts complained of violate the African Charter and other international human rights treaties ratified by the respondent state.

- ***Ratione temporis***: This requires the African Court to consider whether the violation occurred after the state concerned had ratified the African Court Protocol or the human rights treaty that it is claimed to have violated. Importantly, the African Court has expressly recognised that violations may be of a continuous nature, which opens its jurisdiction to cases where violations began before the African Court Protocol came into force for any state.

- ***Ratione loci***: This requires the African Court to consider whether the violations occurred within the territory of a state party.

### Stage 4: Admissibility

Once jurisdiction is established, the African Court will determine if the matter passes the admissibility threshold. The three main admissibility requirements are as follows:

- **Cases brought by the ACHPR**: Rule 118 of the Rules of Procedure of the African Court allows the ACHPR to bring a case to the African Court if it has taken a decision with respect to a communication submitted under articles 48, 49 or 55 of the African Charter and it considers that the state has not complied or is unwilling to comply with its recommendations within 180 days.[12]

- **Cases brought by an individual or NGO**: Rule 40 of the Rules of Procedure sets out that all the requirements for admissibility contained in article 56 of the African Charter must be met in order for a case to be deemed admissible.

- **Cases brought by an African organisation for an advisory opinion**: Article 4 of the African Court Protocol allows any Member State of the AU, the AU itself or any of its organs, or any African organisation recognised by the AU to request the African Court to provide an opinion on any legal matter relating to the African Charter or any other relevant human rights instruments.

[12] See further Rudman, 'The commission as a party before the court - Reflections on the complementarity arrangement' (2016) PER (accessible at http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812016000100011).

## Stage 5: Proceedings

The ordinary sessions of the African Court are held every year in March, June, September, and December, or at any other period as it may deem fit. It may also hold extraordinary sessions. The hearing is conducted by the Presiding Judge, who prescribes the order in which the representatives of the parties are heard. As the African Court live streams its hearings and makes recordings publicly available, prospective litigants can view previous hearings beforehand to get a general sense of how the African Court operates.

The African Court consists of eleven judges, although seven judges is sufficient for there to be a quorum. Rule 47(1) of the African Court Rules provides that the Presiding Judge or any Judge may put questions to the parties' representatives. In practice, each of the main parties is allocated time to present arguments on admissibility and the merits (usually approximately 45 minutes), whereafter each judge has the opportunity to question the legal representatives. The legal representatives are then given the opportunity to prepare overnight and return the next day to respond to the questions posed and reply to the other side's arguments.

Rule 47(1) of the African Court Rules also provides that where there are witnesses, experts, and other persons appearing before the African Court, the judges are permitted to ask them any questions relating to the matter. Further, the representatives of the parties are entitled to examine, cross-examine, and re-examine the witnesses, experts and other persons who appear before the African Court, as the case may be.

## Stage 6: Measures and Remedies

When reaching its decision, the Africa Court will take into account various sources of law. Article 7 of the African Court Protocol provides that the African Court "shall apply the provisions of the [African] Charter and any other relevant human rights instruments ratified by the States concerned". Other sources of law, may, however, also be considered.

Article 28(1) of the African Court Protocol stipulates that the African Court will render its judgment within 90 days of having completed its deliberations. Parties will be notified of when the judgment is expected to be handed down, and judgments are read in open court. The decision is made by a majority of the members of the panel, with the Presiding Judge having a casting vote in the event of a tie. Any member of the panel that heard the case may deliver a separate or dissenting opinion.

Article 27(2) of the African Court Protocol provides that "[i]n cases of extreme gravity and urgency, and when necessary to avoid irreparable harm to persons, the [African] Court shall adopt such provisional measures it deems necessary." The procedure for making a request for interim measures is contained in the Practice Directions. Any request for interim measures must state the reasons and must specify in detail the extreme gravity and urgency, as well as the irreparable harm that is likely to be caused. The request must be accompanied by all supporting documents that could substantiate the applicant's allegations, including any relevant domestic court or other decisions. The Practice Directions provide that requests for interim measures must be filed within a reasonable time.

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

### Reparations at the African Court

In *Norbert Zongo and Others v Burkina Faso*, the African Court found that the respondent state had violated articles 1, 7 and 9(2) of the African Charter but deferred its ruling on the issues of damages, calling on the parties to make submissions on that point.

In June 2015, after consideration of the submissions, the African Court issued its judgment on reparations. In its reasoning, the African Court relied on the trite legal position that states which violate international human rights provisions are required to make full reparation for the damage caused and relied on its remedial powers in terms of article 27(1) of the Protocol – which enjoins the Court to make an appropriate order to remedy the violation, including the payment of fair compensation or reparation.

There is a difference between material damages and moral damages: the former can be addressed in monetary terms, while the latter affects the reputation, sentiment, or affection of a natural person. In this instance, the applicants sought both material and monetary damages. Here are some key observations and findings of the African Court regarding moral prejudice:

- **The notion of victim**: A victim is not necessarily limited to the first-line heirs of a deceased person; other close relatives may also suffer moral prejudice. In this case, the spouses, children, fathers and mothers of the deceased were found to suffer the most. The Court dismissed the claim by stepmothers, uterine sisters and brothers and step-sisters and step-brothers.
- **The type of evidence required to establish victim status**: Marriage and birth certificates as well as attestations of paternity or maternity, or any other equivalent proof should be produced.
- **Proof of the causal link between the wrongful act and the moral prejudice suffered**: Such a link may result from the violation of a human right, as an automatic consequence, without any need to prove otherwise.
- **The amount of reparation**: This determination should be done equitably and on a case-by-case basis.

On material prejudice, the Court considered the expenditure and costs incurred by the beneficiaries, which included the lawyer's fees, and the transport and sojourn expenses.

Ultimately, the Court awarded damages to the family members affected by the violations of the state. The state respondent was ordered to pay 25 million CFA per spouse (approximately 43 500 USD), 15 million CFA per child (approximately 26,000 USD), and 10 million CFA per mother or father (approximately 17,400 USD).

## Stage 7: Enforcement

It is important to remember that the ACHPR can refer matters to the African Court when it considers that a state (who has signed the Protocol) has not complied or is unwilling to comply with its recommendations. Despite the clear need for strong enforcement mechanisms, the African Court Protocol provides that "[t]he State Parties to the present Protocol undertake to comply with the judgment in any case to which they are parties within the time stipulated by the Court and to guarantee its execution". Failures by states to comply with judgments are noted in the African Court's report to the Assembly per article 31 of the Protocol.

### Commentary on the African Court

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

Manisuli Ssenyonjo has taken the following view in relation to the impact of the African Court as well as some of the challenges it faces:

> "First, [there is] limited direct access by individuals and NGOs to the Court due to a limited number of States that have accepted the Court's jurisdiction and allowed individuals and NGOs direct access to the Court. Thus, there is a need for more States to ratify the Court's Protocol and to allow individuals and NGOs direct access to the Court. This will help to consolidate a pan-African judicial system for the protection of human rights which applies to over 1.2 billion people in Africa. In addition, an amendment of Article 34(6) of the African Court Protocol by a decision of the AU Assembly of Heads of State and Government to allow individuals and NGOs direct access to the Court would make the Court more accessible to victims of human rights violations in Africa. Until this is achieved, the African Commission should submit more cases to the Court in accordance with Rule 118 discussed above, particularly those cases in which States have failed to implement the Commission's decisions.
>
> Second, the non-implementation of the Court's decisions, including refusals to implement, failure to inform the Court of what measures have been taken, and the slow pace or 'reluctance' to comply limits the Court's effectiveness. In 2013, for example, the Court adopted an Interim Report noting that 'Libya has failed to comply with a judgment of the Court'. It called on the AU Assembly of Heads of State to take such other measures as it deems appropriate to ensure that Libya fully complies with the Court Order. However, the Assembly did not take any action. This shows that non-compliance and non-enforcement applies to both the Commission's recommendations as well as the Court's orders. Thus, the ability of the AU organs to impose sanctions consistently on non-complying States is necessary in order to strengthen the credibility of the African Court's orders and judgments."

*Practicalities of litigating before the African Court*

Currently, the most notable practical consideration when litigating at the Africa Court is that states are either failing to engage with the declaration required under article 34(6) or withdrawing their declaration.[13] The Centre for Human Rights has noted that this is "gravely hampering access to remedy for many victims of human rights violations across the continent".[14] This is presently a considerable challenge to potential litigants who seek redress and to hold states accountable for human rights violations.

[13] Al Jazeera, 'Africa's human rights court and the limits of justice' (2017) (accessible at https://www.aljazeera.com/programmes/talktojazeera/2017/01/africa-human-rights-court-limits-justice-170107092107153.html).

[14] Centre for Human Rights, 'Press Statement: Centre for Human Rights expresses concern about Tanzania's withdrawal of access to the African Court by individuals and NGOs' (2019) (accessible at https://www.chr.up.ac.za/latest-news/83-news-chr/1916-press-statement-centre-for-human-rights-expresses-concern-about-tanzania-s-withdrawal-of-access-to-the-african-court-by-individuals-and-ngos).

## Litigating at the East African Court of Justice

**Examples of cases before the East African Court of Justice**

*Media Council of Tanzania and Others v Attorney-General of the Republic of Tanzania*

In 2019 the East African Court of Justice (**EACJ**) handed down a judgment in which it declared that certain provisions of Tanzania's Media Services Act violated freedom of expression.

A group of civil society organisations approached the EACJ arguing that "the Act in its current form is an unjustified restriction on the freedom of expression, which is a cornerstone of the principles of democracy, the rule of law, accountability, transparency and good governance which [Tanzania] has committed to abide by, through the Treaty". It was submitted that the Act violated freedom of expression by criminalising the dissemination of disinformation.

The EACJ was critical of the broad wording of the impugned provision that regulated content restrictions. Further, the EACJ found that the provisions relating to fake news and rumours were similarly vague and found them to be in conflict with the EAC Treaty. The EACJ ultimately found that the provisions violated freedom of expression and ordered the Tanzanian government to take measures to bring the Act into compliance with the EAC Treaty.

*Overview of the East African Court of Justice*

The EACJ is a sub-regional court that is mandated to resolve disputes involving the East African Community and its Member States. The EACJ was established by article 9 of the Treaty for the Establishment of the East African Community (**EAC Treaty**) and is tasked with interpreting and enforcing the treaty.[15] The East African Court of Justice Rules of Procedure (**EACJ Rules**) govern its functioning while it seeks to ensure adherence to law in the interpretations and application of, and compliance with, the EAC Treaty. The EACJ serves the East African Community (**EAC**), namely Burundi; the Democratic Republic of Congo; Kenya; Rwanda; South Sudan; the United Republic of Tanzania; and Uganda. It has a First Instance Division and an Appellate Division. The former administers justice and applies relevant law, while the latter confirms, denies, or changes decisions taken by the First Instance Division.

### Stage 1: Statement reference and statement of claim

A statement of reference (similar to a claim or complaint in domestic litigation) should include an allegation of a human rights violation made by a Partner State, the Secretary-General, or a legal or natural person. Article 24 of the EACJ Rules provides for the lodging of a statement of claim. It should be lodged at the court as a statement of reference and should include:

[15] See further International Justice Resource Center 'East African Court of Justice' (accessible at https://ijrcenter.org/regional-communities/east-african-court-of-justice/).

- The designation, name, address, and residence of both the applicant and respondent(s).
- The subject-matter of the reference and a summary of the points of law on which the application is based.
- The nature of any supporting evidence offered.
- The relief sought.

A notice of the reference and a copy of the application must be served on each respondent and on the Secretary-General.

Article 25 provides for the lodging of a statement of claim. This is used where the issue is between the East African Community and its employees and should include:

- The name, designation, address, and, where applicable, residence of the claimant.
- The designation, name, address, and, where applicable, residence of the respondent.
- A concise statement of facts on which a claim is based and of the law applicable.
- The order sought.

The EACJ User Guide explains that once a claim or reference has been filed, the Registrar will issue a notification requiring the respondents to file their statement of defence, accompanied by a copy of the statement.

### Stage 2: Standing

Article 30(1) of the EACJ Rules provides that any legal or natural person who is resident in a partner state has standing to refer a determination to the EACJ; the party must be:

- A legal or natural person.
- A resident of an EAC Partner State.
- Challenging the legality of any Act, regulation, directive, decision, and action of the said Partner State or an institution of the Community.

#### Note on *amici curiae* in the EACJ

*Amici curiae* are allowed to apply to be involved in a matter per article 36 of the EACJ Rules. An application must be made by notice of motion and provide the following information:

- A description of the parties.
- The name and address of the *amicus curiae.*
- A description of the claim or reference.
- The order in respect of which the *amicus curiae* is applying for leave to intervene.
- A statement of the *amicus curiae*'s interest in the result of the case.

Article 37 of the EAC Treaty allows for parties to be represented when they appear before the EACJ. Parties can be represented by an advocate entitled to appear before a superior court of any of the Partner States.

### Stage 3: Jurisdiction

The jurisdictional requirements of the EACJ are set out in articles 27 and 30 of the EAC Treaty. Article 27 states as follows:

> "(1) The Court shall initially have jurisdiction over the interpretation and application of this Treaty: Provided that the Court's jurisdiction to interpret under this paragraph shall not include the application of any such interpretation to jurisdiction conferred by the Treaty on organs of Partner States.
> (2) The Court shall have such other original, appellate, human rights and other jurisdiction as will be determined by the Council at a suitable subsequent date. To this end, the Partner States shall conclude a protocol to operationalise the extended jurisdiction."

Article 30 states further that:

> "(1) Subject to the provisions of Article 27 of this Treaty, any person who is resident in a Partner State may refer for determination by the Court, the legality of any Act, regulation, directive, decision or action of a Partner State or an institution of the Community on the grounds that such Act, regulation, directive, decision or action is unlawful or is an infringement of the provisions of this Treaty.
> (2) The proceedings provided for in this Article shall be instituted within two months of the enactment, publication, directive, decision or action complained of, or in the absence thereof, of the day in which it came to the knowledge of the complainant, as the case may be.
> (3) The Court shall have no jurisdiction under this Article where an Act, regulation, directive, decision or action has been reserved under this Treaty to an institution of a Partner State".

Accordingly, jurisdiction can be exercised in the following ways:

- ***Ratione personae***: Article 30(1) of the EAC Treaty provides that any natural or legal resident in the EAC may bring a case to the EACJ.

- ***Ratione temporis***: Cases could fall within the temporal jurisdiction of the EACJ if they occurred subsequent to the EAC Treaty coming into force. There is a strict two-months rule that guides this exercise of jurisdiction.

- ***Ratione materiae***: Article 30(1) of the EAC Treaty authorises legal and natural persons, resident in a state party to the EAC Treaty, to make a reference (the same as filing a

complaint) to the EACJ on whether an act or omission of a state party is an infringement of the EAC Treaty.

### Jurisdiction over human rights violations

It is necessary to note that the EACJ does not explicitly have jurisdiction over human rights matters. However, articles 6(d) and 7(2) of the EAC Treaty create scope for human rights matters to be brought before the EACJ.

Article 6(d) states:

> "The fundamental principles that shall govern the achievement of the objectives of the Community by the Partner States shall include: good governance including adherence to the principles of democracy, the rule of law, accountability, transparency, social justice, equal opportunities, gender equality, as well as the recognition, promotion and protection of human and peoples' rights in accordance with the provisions of the African Charter on Human and Peoples' Rights".

Article 7(2) states:

> "The Partner States undertake to abide by the principles of good governance, including adherence to the principles of democracy, the rule of law, social justice and the maintenance of universally accepted standards of human rights."

These articles were relied on in *Burundi Journalists' Union v Attorney General of the Republic of Burundi*. In 2013, the Burundi Journalists Union filed a reference with the EACJ alleging that the Press Law enacted in Burundi restricted freedom of the press, which is a cornerstone of the principles of democracy, rule of law, accountability, transparency, and good governance. Before turning to the merits of the matter the EACJ needed to determine whether the reference was properly before it and whether it had jurisdiction to engage it. Finding that it did have jurisdiction, the EACJ reasoned that the interpretation of the question whether articles 6(d) and 7(2) of the EAC Treaty were violated in the enactment of the Press Law is a matter squarely within the ambit of this EACJ's jurisdiction. In essence, the EACJ read freedom of expression into the above articles and held that the violations of freedom are justiciable as violations of the EAC Treaty, accordingly, clothing it with jurisdiction.

Media Defence has noted that "the judgment is strong precedent for future cases as it removes any doubts over whether the EACJ can consider freedom of expression cases despite its lack of explicit human rights jurisdiction. This makes the EACJ a viable forum before which to test the laws of East African states relevant to the media".

### Stage 4: Admissibility

The EACJ does not apply the same admissibility criteria applied by the ACHPR and the African Court. The two key considerations for the EACJ are as follows:

- **Two-month rule*:*** Article 30(2) of the EAC Treaty requires references to be filed with the EACJ within two months of the alleged violation. This time frame is narrow and can be difficult to comply with. In *Attorney General of Uganda and Another v Awadh and Others*, the EACJ held that it would not be flexible on this requirement. It is also necessary to note that there is no provision in the EAC Treaty that recognises the concept of continuing violations.

- **Local remedies**: There is no requirement that all domestic remedies must be exhausted first. In *Democratic Party v Secretary-General and the Attorneys General of the Republics of Uganda, Kenya, Rwanda and Burundi*, the EACJ held that this jurisdiction is not voluntary and that once an applicant can show an alleged violation of the EAC Treaty, the EACJ must exercise jurisdiction. Where it does not have jurisdiction, the EACJ has held that:

> "Jurisdiction is quite different from the specific merits of any case … As it is, it should be noted that one of the issues of agreement as set out by the parties is that there are triable issues based on Articles 6, 7, 27 and 30 of the Treaty. That is correctly so since once a party has invoked certain relevant provisions of the Treaty and alleges infringement thereon, it is incumbent upon the Court to seize the matter and within its jurisdiction under Articles 23, 27 and 30 [to] determine whether the claim has merit or not. But where clearly the Court has no jurisdiction because the issue is not one that it can legitimately make a determination on, then it must down its tools and decline to take one more step."

### Stage 5: Procedure

Chapters VII and XII of the EACJ Rules provide for written and oral proceedings. Rule 54(1) provides that pre-trial proceedings take place after the close of pleading and allow the Principal Judge to determine issues in dispute, the possibility of mediation, the need for evidence and whether argument should be written or oral. Rule 53(3) and (4) provides:

> "If the matter is to proceed to hearing the Division shall fix the date for commencement of hearing.
>
> In any case where there is no need for evidence and all parties opt to present legal arguments in writing, the Division shall prescribe the time within which the parties shall file their respective written legal arguments and may fix the date on which the parties shall appear before a bench of three judges to deal with any other matter the Division thinks necessary".

The User Guide explains the process of oral hearings as follows:

> "One Party, usually the Claimant, first begins [Rule 62]. He states his case and produces his evidence ─ including calling his witness(es) to give evidence. The Respondent questions the Claimant (in cross-examination). If there is anything that is not clear, the Claimant may re-examine the witness further; and/or comment on any new points raised [Rule 63].
>
> As the witnesses give evidence, the judge(s) take down notes. Simultaneously, a full audio recording of the proceedings is made [Rule 65]. If the case is not concluded for each hearing, a new date is set when the hearing will be continued. That process is known as Adjournment. The Court will always fix a specific date when the case will carry on. If any date is fixed at a later stage, then the Court will notify all the parties of the new date".

The above steps take place at the level of the First Instance Divisions. Judgment shall be delivered within sixty (60) days from the conclusion of the hearing except where the EACJ is unable to do so. In some instances, the EACJ might elect to provide a decision at the close of the hearing and provide reasons at a later date.

A decision from the judgment or any order of the First Instance Division can be appealed per article 77 of the Rules of Procedure on:

- Points of law.
- Grounds of lack of jurisdiction.
- Procedural irregularity.

Written notice must be given when doing so which must state the grounds of the appeal.

An intended appellant must lodge a notice of appeal within 30 days from the date of the decision. Parties are also entitled to review a judgment. Article 35 of the EAC Treaty read with article 72 of the EACJ Rules of procedure provides:

> "An application for review of a judgment may be made to the Court only if it is based upon the discovery of some fact which by its nature might have had a decisive influence on the judgment if it had been known to the Court at the time the judgment was given, but which fact, at that time, was unknown to both the Court and the party making the application, and which could not, with reasonable diligence, have been discovered by that party before the judgment was made, or on account of some mistake, fraud or error on the face of the record or because an injustice has been done."

An application for review of a judgment may be made to the EACJ only if it is based upon the discovery of some fact which by its nature might have had a decisive influence on the judgment if it had been known to the Court at the time the judgment was given, but which fact, at that time, was unknown to both the Court and the party making the application, and which could not, with reasonable diligence, have been discovered by that party before the judgment was

made, or on account of some mistake, fraud or error on the face of the record or because an injustice has occurred.

### Stage 6: Measures and Remedies

Article 38(3) of the EACJ Treaty provides that a partner state or the Council shall take the measures required to implement a judgment of the EACJ without delay. Article 39 of the EACJ Treaty allows for the issuance of interim orders when it is considered necessary to do so. Article 69(2) of the EACJ requires all orders of the EACJ to clearly specify the relief granted or other determination of the case.

### Stage 7: Enforcement

Article 44 provides, amongst other things, that the rules of civil procedure applicable in the state in question will govern the execution of a judgment of the EACJ that imposes a pecuniary obligation. Rule 74 provides that a party who wishes to execute an order of the EACJ must make an application in accordance with Form 9 of the Second Schedule to the EACJ Rules.

*Practicalities of litigating before the EACJ*

The time limitations of the EACJ undoubtedly pose practical challenges for litigants. Other challenges that have been noted include administrative challenges, lack of enforcement mechanisms, and funding challenges.[16]

[16] Luambano, 'Litigating Human Rights Through the East African Court of Justice: Overview and Challenges' Journal of Law, Policy and Globalisation (2018) (accessible at https://www.iiste.org/Journals/index.php/JLPG/article/view/41719/42940).

## Litigating at the ECOWAS Community Court of Justice

### Examples of cases before the ECOWAS Community Court of Justice

*Federation of African Journalists and Others v The Republic of The Gambia*

A challenge was brought against The Gambian Criminal Code which created criminal offences for sedition, false news, and criminal defamation. Several journalists had been arrested and charged as a result of the Code. They argued that this limited their freedom of expression. The Federation of African Journalists, as well as three nationals of The Gambia who were living in exile due to fear of persecution as a consequence of their work as journalists, approached the ECOWAS Court seeking the following relief:

- Declaratory relief that The Gambia, in enforcing statutory provisions of the Criminal Code, violated the following rights:
  - The right to freedom of opinion and expression under article 9 of the African Charter and article 19 of the ICCPR.
  - The right of journalists under article 66(2) of the Revised ECOWAS Treaty.
  - The right to liberty and security under article 6 of the African Charter and article 9(1) of the ICCPR.
  - The right of Gambian citizens to return to The Gambia under article 12(2) of the African Charter and Article 12(4) of the ICCPR.

- A declaration that in subjecting the fourth applicant to torture or other cruel, inhuman, or degrading treatment or punishment, and causing him physical harm, and psychological and emotional injury, The Gambia acted in violation of his human rights, the right to freedom from torture and other cruel, inhuman, or degrading treatment or punishment under article 5 of the African Charter and article 7 of the ICCPR.

- A Declaration that in maintaining the statutory provision The Gambia had continued to act in gross violation of the applicants' rights and in breach of their obligations under the Revised ECOWAS Treaty, the African Charter and the ICCPR.

- An order mandating and compelling The Gambia to repeal the relevant statutory provisions immediately or otherwise amend its laws in order to meet its obligations under international law including under the African Charter, the ICCPR and customary international law.

- An order mandating and compelling The Gambia to effectively enact and implement laws, regulations, and safeguards in order to meet its obligations under international law prohibiting torture and other cruel, inhuman, or degrading treatment or punishment including under the African Charter, the ICCPR and customary international law.

- An order for reparations, including physical, psychological, social, and economic rehabilitation in respect of the violations of the second, third and fourth applicant's human rights.

Amnesty International, Canadian Journalists for Freedom of Expression, the Committee to Protect Journalists, Freedom House, Pen International, Reporters without Borders and the Right2Know Campaign brought an application to join the proceeding as *amici curiae*.

In 2018, the ECOWAS Court made a finding that it had jurisdiction to entertain the matter, despite a preliminary objection by The Gambia. In its decision on the merits, the ECOWAS Court found that:

- The enforcement of the impugned statute violated the rights of the applicants under articles 6, 9 and 12(2) of the African Charter, articles 9, 12(4) and 19(2) of the ICCPR, and Article 66(2)(c) of the Revised ECOWAS Treaty.

- Subjecting the applicants to torture, inhuman, and degrading treatment violated their rights under article 5 of the African Charter and article 7 of the ICCPR.

The ECOWAS Court reasoned that the imposed criminal sanctions were disproportionate and not necessary in a democratic society where freedom of speech is a guaranteed right and ordered that the legislation be reviewed. The Criminal Code was found to be overbroad and to "cast excessive burden upon the applicants in particular and all those who would exercise their right of free speech and violates the enshrined rights to freedom of speech and expression under Article 9 of the African Charter, Article 19 of the ICCPR and Article 19 of the UDHR".

The Gambia was ordered immediately repeal and/or amend the Criminal Code in line with its obligations under international law, especially article 1 of the African Charter, the ICCPR and the ECOWAS Revised Treaty. The Gambia was further ordered to pay damages to the applicants for the violation of their rights.

*Overview of the ECOWAS Community Court of Justice*

The ECOWAS Community Court of Justice (**ECOWAS Court**) is the judicial body of the Economic Community of West African States (**ECOWAS**). The ECOWAS Court was established in terms of the Revised Treaty of the ECOWAS (**ECOWAS Revised Treaty**). The mandate of the ECOWAS Court includes ensuring the observance of law and of the principles of equity in the interpretation and application of the provisions of the Revised Treaty and all other subsidiary legal instruments adopted by ECOWAS. It serves the ECOWAS member states: Benin, Burkina Faso, Cape Verde, Cote d'Ivoire, The Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Sierra Leone, Senegal, and Togo. The ECOWAS Protocol, the ECOWAS Supplementary Protocol, and the Rules of the Community Court of Justice (**Rules**) provide guidance on the procedures of the ECOWAS Court.

### Stage 1: Application to the Tribunal

Cases are to be filed before the Court through written applications addressed to the Registry. Article 11 of the ECOWAS Protocol requires that an application addressed to the Registry must set out the subject matter of the dispute, the parties involved, and a summary of the argument. Rule 33 specifically requires:

- The name and address of the applicant.
- The designation of the party against whom the application is made.
- The subject matter of the proceedings and a summary of the pleas in law on which the application is based.
- The form of order sought by the applicant.
- Where appropriate, the nature of any evidence offered in support.

### Stage 2: Standing

The ECOWAS Court has fairly broad standing provisions. Article 10 of the Revised Treaty provides that the following litigants may approach it:

- Member states.
- The Executive Secretary (now the President of the ECOWAS Commission).
- The Council of Ministers.
- Community Institutions.
- Individuals.
- Corporate Bodies.
- Staff of any Community Institution.
- National Courts of ECOWAS Member States.

Despite covering a wide range of potential litigants, adherence to the standing provision is strictly applied by the ECOWAS Court. In *Ocean King v Senegal*, the ECOWAS Court found that "an applicant will lack the requisite standing to bring a claim to the Court for determination if the issue raised does not fall within those over which they have been granted the right of access".

#### Note on *amici curiae* in the ECOWAS Court

The ECOWAS Protocol and the Rules do not explicitly provide for *amici curiae* briefs. However, as discussed above, in *Federation of African Journalists*, interveners were accepted as *amici curiae*. In that matter the Court granted an application in terms of article 89 of the Rules, allowing the NGOs to join the suit as interveners/ amici curiae.

Accordingly, a party interested in being admitted as *amicus curiae* should follow the rules applicable to interveners before the ECOWAS Court per Chapter III of the Rules. Rule 89, in particular, notes that an application to intervene must be made within six weeks of the publication of the notice of an application initiating proceedings. The application must contain:

- The description of the case.
- The description of the parties.
- The name and address of the intervener.
- The intervener's address for service at the place where the ECOWAS Court has its seat.
- The form of order sought, by one or more of the parties, in support of which the intervener is applying for leave to intervene.
- A statement of the circumstances establishing the right to intervene.

The application must be served on the parties. The President will give the parties an opportunity to submit their observations before deciding on the application, whereafter the President will refer the application to the Court to determine if the application to intervene should be granted.

### Stage 3: Jurisdiction

Article 9(4) of the ECOWAS Protocol, as amended by the ECOWAS Supplementary Protocol, formally recognises that the ECOWAS Court "has jurisdiction to determine cases of violation of human rights that occur in any Member State". Article 10(d) of the ECOWAS Supplementary Protocol states that access to the ECOWAS Court is open to "[i]ndividuals on application for relief for violation of their human rights."

The ECOWAS Court can exercise jurisdiction in the following ways:[17]

- ***Ratione personae***: Any individual alleging a violation of human rights committed in any member state may bring a case before the ECOWAS Court. Applications from organisations acting on behalf of a group of people whose rights have been violated can also be accepted.

- ***Ratione temporis***: Human rights cases must be brought within three years of the cause of action arising. In instances where violations are ongoing, it will give rise to a cause of action *die in diem* (day in and out) and postpones the running of time.

- ***Ratione materiae***: The ECOWAS Court has jurisdiction over all human rights violations that occur in the jurisdiction of members of ECOWAS.

### Stage 4: Admissibility

Admissibility at the ECOWAS Court is not as strictly applied as it is in the other courts; however, it is important to note that applications that are brought cannot be pending before another court of similar status. The ECOWAS Court does not require the exhaustion of

[17] For a comprehensive discussion on jurisdiction at the ECOWAS Court see Media Defence 'Training Manual on Litigation of Freedom of Expression in West Africa (accessible at https://10years.mediadefence.org/wp/wp-content/uploads/2018/11/Legal-resources-6-West-Africa-Regional-Mechanisms-Manual.pdf).

domestic remedies but will neither hear matters that have been determined on the merits by domestic courts nor does it hold appellate jurisdiction over domestic courts.

### Stage 5: Proceedings

Rule 35 prescribes that once an application has been filed, the defendant has a month to lodge his or her defence. The ECOWAS Court will then, per rule 39, issue a preliminary report containing recommendations as to whether a preparatory inquiry or any other preparatory step should be undertaken. The ECOWAS Court may, per rule 43, either at its discretion or on application by a party, order that witnesses prove certain facts. Once the ECOWAS Court is satisfied with all the preliminary inquiries the matter will go to oral proceedings.

#### Cases that need to be dealt with as a matter of urgency

Chapter IV of the Rules provides for expedited procedures. Cases can be determined pursuant to an expedited procedure derogating from the provisions of these Rules, where the particular urgency of the case requires the ECOWAS Court to give its ruling with the minimum delay.

An urgent application needs to be lodged in a separate application along with the application initiating proceedings. The ECOWAS Court will provide all parties with an opportunity to present their arguments and will then deliver its ruling.

### Stage 6: Remedies

The ECOWAS Court will issue a judgment once it has finalised the matter, it shall include the grounds for the decision and the operative part of the judgment, including the decision as to costs. This is done in terms of rule 60 of the Rules. The remedies available to the ECOWAS Court are similar to those offered at a domestic level. Remedies can include declarations and mandatory orders. The ECOWAS Court does not have the scope to create remedies and is accordingly limited to base the remedy on what was put before it by the parties.

### Stage 7: Enforcement

The ECOWAS Court's judgments are binding. Member States are required to take immediate steps to comply with the remedy. Despite this, concerns have arisen regarding the legitimacy of the enforceability of the ECOWAS Court. Olisa Agbakoba Legal has noted that:

> "[E]nforcement of judgments of the ECOWAS Court has been a major problem and this relates to the fact that neither the ECOWAS Revised Treaty, Supplementary Protocols or other legal instruments make provisions regarding the means of enforcing the issued writ of execution where Member States fail to voluntarily comply with the terms of the judgments of the Court. However, Article 77 of the ECOWAS Revised Treaty empowers the authority of heads of state and government of ECOWAS to impose certain sanctions on any member state

> who fails to fulfil its obligations to the community through suspension of new community loans or assistance, suspension of disbursement on on-going community projects or assistance programmes, exclusion from presenting candidates for statutory and professional posts and suspension from participating in the activities of the community.
>
> This power is however yet to be exercised by the apex organ of ECOWAS. Thus, unless Member States are compelled to comply with the judgments of the ECOWAS Court, the confidence in the Court will completely be eroded so much so that the Court may be unable to entertain any applications from any person in respect of the violations of the fundamental rights of the citizens of ECOWAS."

*Practicalities of litigating before the ECOWAS Court*

There are two notable challenges that ought to be taken into account by potential litigants:

- Establishing jurisdiction at the ECOWAS Court.
- Competing competencies between the ECOWAS Court and national courts appear to have also caused some concern.

The expanded jurisdiction that accompanied the Supplementary Protocol seems to have created some tension between the ECOWAS Court and its domestic counterparts. Despite seeking to make the ECOWAS Court more accessible, it has to some extent complicated the jurisdictional requirements that ultimately create access.[18]

**Impactful cases on digital rights at the ECOWAS Court**

In recent years, the ECOWAS Court has become more outspoken on issues of digital rights and has made a number of ground-breaking judgments in this area:

*Amnesty International Togo v. The Togolese Republic*

In August 2017, Togo cut off internet access in an effort to disrupt planned protests about the President's seeking a third term in office. A number of NGOs based in Togo, and a local journalist, applied to the ECOWAS Court alleging that the internet shutdown was a violation of the right to freedom of expression contrary to Article 25 of the Togolese Constitution and Article 9 of the African Charter on Human and People's Rights. As described by the Columbia Global Freedom of Expression case law database,

> "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

[18] Ojomo, 'Competing Competences in Adjudication: Reviewing the Relationship between the ECOWAS Court and National Courts' African Journal of Legal Studies (2014) (accessible at https://brill.com/view/journals/ajls/7/1/article-p87_5.xml?language=en).

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 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)".

*SERAP v. Federal Republic of 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 threatening to punish regional secessionists, prompting telecommunications companies to block access to users in Nigeria. The ban was in place for seven months before Twitter agreed to several of the government's demands, including opening a local office in Nigeria.

The ban was 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 access to Twitter is a "derivative right" that is "complementary to the enjoyment of the right to freedom of expression" and, therefore, 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.

## Current Status of the SADC Tribunal

The SADC Tribunal was established in 2005 with the mandate of ensuring adherence to, and proper interpretation of the provisions of, the SADC Treaty and subsidiary instruments. However, following several rulings against the Zimbabwean government, the Tribunal was suspended in 2010. In 2014 a Protocol was adopted that sought to do away with the Tribunal's power to adjudicate individual disputes against a State party.

The Law Society of South Africa challenged the decisions taken by the South African government to support the suspension, and the decision to sign the Protocol. In 2018 the South African Constitutional Court handed down judgment in *Law Society of South Africa and Others v President of the Republic of South Africa and Others* in which the actions of the President in participating in the decision-making process, and his decisions to suspend the operations of the SADC Tribunal were declared to be unconstitutional, unlawful, and irrational. The President was ordered to withdraw his signature from the 2014 SADC Protocol.

In 2019 the Tanzanian High Court in *Tanganyika Law Society v Ministry of Foreign Affairs and International Cooperation of the Republic of Tanzania* ruled that:

> "The suspension of the operations of the SADC Tribunal; and failure or refusal to appoint Judges contrary to the clear Treaty provisions, was inimical to the Rule of law as a foundational principle inherent to the legitimacy of the Community; and as expressly entrenched in the Treaty. Respondents are enjoined pursuant to the respective Treaty obligations; to give effect to the Treaty".

The Tanzania High Court similarly condemned the decision of the Tanzanian President in relation to the suspension of the SADC Tribunal.[19]

While other states in the region are not bound by these domestic decisions, they may nevertheless serve as pressure points for further litigation. However, at the time of writing, the SADC Tribunal remains defunct.

[19] ICJ, 'Tanzanian High Court condemns unlawful stripping of SADC Tribunal's powers rendering the rule of law a "pipe dream"' (2019) (accessible at https://www.icj.org/tanzanian-high-court-condemns-unlawful-stripping-of-sadc-tribunals-powers-rendering-the-rule-of-law-a-pipe-dream/).

## The Practicalities of Litigating Digital Rights

*Determining a strategy*

A holistic litigation strategy is as much about the anticipated outcome as it is about the steps needed to reach that outcome. Developing a strategy can take some time, particularly when there is a long-term vision. However, time is not always available, and strategies sometimes have to be developed very quickly. Whether it is urgent or protracted there are three key tenets for every litigation strategy, and in this regard the tripod analogy is useful. In order for a tripod to be balanced and useable, each leg needs to be of equal length and strength. The same rationale is applicable to a litigation strategy, with the three being:

1. Procedural considerations.
2. Administrative capabilities.
3. Substantive goals.

These considerations are interdependent and need to be given equal consideration. If one is not properly considered, or if one fails, there is the possibility that the entire strategy will fail.

### Procedural requirements

The procedural considerations are those that relate to actual court process and requirements. The considerations listed above will form an important part of developing a strategy. By way of a brief recap, it is important to consider the following:

- Standing.
- Jurisdiction.
- Admissibility.
- Representation.
- *Amicus curiae* involvement.

Other procedural considerations include which parties to cite, court-mandated time frames, procedures regarding interim remedial measures, conflicts of interest, and rules regarding the gathering of information. Another important consideration is that of mandate. It is imperative that lawyers have received the requisite mandate to act, particularly when acting for broader community groups. It is advisable to set out the terms of reference and mandate agreement up front to avoid any procedural mishaps along the way.

### Administrative capacity

Administrative considerations include:

- The financial implications of the litigation from beginning to end, including any unexpected costs and possibilities of appeals or cost orders.
- Capacity to deal with the matter.
- Expertise and skills.

- The setting up of a team and the distribution of roles.
- Internal and external time frames.

Drawing up budgets, developing calendars, and ensuring there are sufficient financial and human resources form an important part of the development of a sustainable strategy.

## Substantive requirements

This component is all about the legal substance. Here, the facts, law and remedy all need to be considered in detail. This includes understanding and mapping out the following:

- The nature of the legal challenge.
- Rights that are implicated.
- The extent to which the facts support the legal challenge.
- Proposed remedy.
- Alternative remedies.
- Applicable legal frameworks.
- Domestic, regional, or international law and jurisprudence.
- Overcoming a limitations / restrictions analysis.
- The issue of costs.
- Reputational development or backlash.
- Safety and security of litigators and clients.
- Forms of research and advocacy that will be of use to the case.
- Parallel and complementary strategies.
- Social, economic, political, and cultural considerations.
- Systemic issues.
- Reliability and legitimacy of the judicial body.

Linking research, advocacy, and litigation is key in the development of a substantive strategy.

*Gathering evidence*

The ordinary rules of evidence apply to digital evidence, which must still meet the minimum standards of relevance and reliability in order to be admitted. Different types of evidence can be useful for proving a case and providing clarification regarding the facts of the case. This can include evidence of the violation, expert evidence, digital evidence, and witness evidence. The rapidly evolving digital landscape is providing both opportunities and challenges in relation to the gathering of evidence. On the one hand, there is a large quantity of available digital information, whereas on the other hand, collecting and analysing the evidence can be challenging and technical.[20]

[20] Human Rights Center UC Berkley School of Law 'Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court' (2014) (accessible at https://www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf).

Unlike traditional evidence, digital evidence can be more complex given the volume of available data, its velocity, its volatility, and its fragility.[21] Courts should consider legal and technical requirements when considering the admissibility of evidence.[22] Legally, courts should consider:

- The legal authorisation to conduct searches and seizures of information and communication technology and related data.
- The relevance, authenticity, integrity, and reliability of digital evidence.

Technically, the courts should consider:

- The digital forensics procedures and tools used to extract, preserve, and analyse digital evidence.
- The digital laboratories whereby analyses are performed and the reports of digital forensic analysts.
- The technical and academic qualifications of digital forensics analysts and expert witnesses.

Fortunately, there is a wealth of resources that can assist lawyers and activists when trying to capture, collect and present evidence of digital rights violations.

**Collecting, preserving, and verifying online evidence of human rights violations**

From a technical perspective, Open Global Rights has listed an array of modules, apps and tools that seek to assist human rights activists with the collection, preservation, and verification of online evidence of human rights violations.

[21] UNODC E4J University Module Series: Cybercrime, 'Module 4: Introduction to Digital Forensics' (2019) (accessible at https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/digital-evidence.html).
[22] UNODC E4J University Module Series, 'Module 6: Practical Aspects of Cybercrime Investigations and Digital Forensics' (2019) (accessible at https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/digital-evidence-admissibility.html).

**Documenting during Internet Shutdowns**

Witness has published a blog series with practical tips on how to overcome the challenges of capturing, storing, and disseminating information during an internet shutdown, including posts on the following:

- Setting up a phone for offline documentation.
- Should I use this documentation app?
- Maintaining verifiable media during an internet shutdown.
- Backing up phone media without internet or a computer.
- File sharing and communication during an internet shutdown.

Creating partnerships with experts and technical organisations can be of great use. Harmonising technology with the law and presenting viable evidence to courts can go a long way in advancing digital rights and freedom of expression.

Not all digital evidence needs to be technical and complicated. Videos or online sources can play a role in proving rights violations, but verification remains key. Widespread dissemination of information can be useful, however, with disinformation on the rise, it is important to verify information – such as videos – before relying on it or using it as evidence. Amnesty International has set up a Digital Verification Corps hub, which uses tools to verify information found in videos posted on YouTube and circulated via WhatsApp.[23] Timing is verified through a comparison between time periods in the videos and reports of the United Nations Human Rights Council, and confirmation of the events is verified by comparing footage to Google Earth and Google Maps. This level of verification can be useful and ensure that accurate information can be put before courts and tribunals.

**Detecting censorship and traffic manipulation**

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:

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

[23] Amnesty International, 'Using digital verification methods to investigate human rights violations in Rwanda' (2019) (accessible at https://www.amnesty.org/en/latest/campaigns/2019/04/using-digital-verification-methods-to-investigate-human-rights-violations-in-rwanda/).

Digital rights and freedom of expression violations often are accompanied by technical terms that many people, including judges, do not fully understand. It is therefore important to be able to simplify the technicalities in a way that captures the rights violation. For example, the legal team may consider engaging with technical partner organisations or *amici curiae* with technical expertise to assist the litigators and the court in better understanding the concepts that are before it.

Litigators should also make use of the plethora of toolkits available that can assist in understanding technical terms. See for example:

- Media Defence Report Mapping digital rights and online freedom of expression in East, West, and Southern Africa
- Media Defence Manual on freedom of expression law
- Media Defence Training Manual on Digital Rights and Freedom of Expression Online
- Media Defence Digital Rights Litigation Guide

### Start a #

Something as simple as creating a hashtag can go a long way. #FeesMustFall, #MeToo and #BlackLivesMatter turned from hashtags into mass movements and challenged systemic issues.

### Learn and teach

Engaging with community-based activists, experts and academics can ensure that everyone is informed of their rights, the issues, and their available remedies. During the early 2000s, the Treatment Action Campaign in South Africa developed a strategy to educate people in South Africa about HIV/AIDS. The education focused on the technical medical component of the disease, as well as a rights-based component that enabled people to be rights-literate. Community healthcare workers, activists, lawyers, and other medical experts worked together to ensure that everyone understood the issues and was empowered to address them.

More recently, Ndifuna Ukwazi, an organisation based in South Africa, has begun developing different techniques to assist community members with addressing access to housing and unlawful evictions. They host regular workshops where people with legal skills explain the law to the community, in an effort to ensure that those persons could then train other members of their community. This has developed into a sustainable model where community members educate each other. The communities began learning how to represent themselves in unlawful eviction matters and became available to assist others who might not have easy access to legal services. This campaign has been effective in ensuring that people have agency and are empowered to solve legal challenges.

Sharing information online, hosting workshops and developing infographics can all assist in ensuring that there is an informed society, an informed judiciary, and an informed government.

### Tell stories not statements

Issues around digital rights and freedom of expression affect people differently, and their different experiences can play an important role in the way others understand the issues and how others relate to the issues. People, including judges, are often more likely to show empathy for an issue that has a human side. Sharing stories about how people have been affected, and letting people tell their own stories, can go a long way in strengthening an advocacy campaign and in turn can support the litigation.

### Meaningful actions

Actions have proven to be an effective means of drawing attention to an issue. Actions can range from protests and disruptions to petitions and submissions to those in power. They can include visual statements such as paintings, posters, or billboards. These should be strategic and impactful and should send the right message.

## Conclusion

Regional and continental legal fora are increasingly becoming high-opportunity targets for litigating rights issues across the continent, including digital rights. They provide an alternative forum in cases where domestic remedies are insufficient and have demonstrated their willingness to defend the principles of information rights against powerful state parties. While enforcement and compliance remain challenges in these courts, progress is being made in raising awareness among the public about their operations and decisions as well as in finding innovative ways to leverage positive judgments beyond enforcement. As digital rights issues become increasingly prominent in Africa, it is important for activists and lawyers to understand how to take advantage of the opportunities posed by regional courts to advance public interest litigation, and how to support such litigation with effective advocacy, capacity-building, and public outreach.