*Module 1*

# General Overview of Trends in Digital Rights Globally

*Advanced Modules on Digital Rights and Freedom of Expression Online in Sub-Saharan Africa*

MEDIA DEFENCE

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

**Originally published in November 2022**
**Revised in February 2024**

## TABLE OF CONTENTS

# MODULE 1

## GENERAL OVERVIEW OF TRENDS IN DIGITAL RIGHTS GLOBALLY

**This module aims to:**

- **Provide an overview of global trends in digital rights;**
- **Set out various aspects of the right to access information in the digital age, such as the blocking of access to the internet and efforts to preserve net neutrality;**
- **Evaluate the current state of the right to privacy by looking at data protection, surveillance, the collection of biometric information and efforts to subvert privacy by targeting encryption and using artificial intelligence; and**
- **Explore new aspects of the right to freedom of expression online, including growing threats in the form of misinformation, hate speech regulations, and online violence against journalists.**

## INTRODUCTION

Over the last decade, the number of internet users worldwide has more than doubled. As of January 2024, the digital population consists of over 5.3 billion people.[1] In Africa, the number of recorded internet users increased almost four-fold between 2012 and 2022, going from just over 167 million people to over 650 million in only 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 United Nations Human Rights Council's (UNHRC) 2016 Resolution on the promotion, protection and enjoyment of human rights on the internet confirmed that these rights enable a full array of other fundamental rights and deserve the same protection when exercised online as 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

[1] Statista, 'Number of internet and social media users worldwide as of January 2024,' (accessible here).
[2] Statista, 'Number of internet users worldwide from 2009 to 2022, by region,' (accessible here).
[3] ARTICLE 19, 'Digital Rights' (accessible here).

to achieving the full capacity of the internet and digital spaces where human rights can be protected, respected, promoted, and 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 as they relate to the digital realm, and highlights expected developments moving forward.

## THE RIGHT TO ACCESS INFORMATION

There is increasing recognition around the world that access to the internet is a critical component of the right to access information (in addition to others such as the right to education).[4] Access to the internet has increased significantly over the last decade, but, regrettably, so too have new and innovative restrictions on how people access the internet, 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 2022, Access Now and the #KeepItOn coalition documented at least 187 internet shutdowns in 35 countries around the world.[5] Between January and May 2023, Access Now recorded 80 internet shutdowns in 21 countries.[6]

Since experiencing a coup in 2021, internet shutdowns in Myanmar have been and continue to be imposed by the military across many parts of the country.[7] In 2022, the United Nations (UN) condemned the attempt to establish a "digital dictatorship" and the use of internet shutdowns to undermine public opposition. The UN found that since August 2021, 31 townships in the 7 states of Myanmar had reported internet shutdowns and a further 23 townships experienced throttling of internet speeds.[8] The longest nationwide outage has been reported as being for nearly 2.5 months.[9] These internet shutdowns typically coincide with an escalation of military offensives and human rights violations by the military.[10]

Within Africa, Zimbabwe and the Tigray region of Ethiopia have seen some of the most prolonged internet shutdowns in history:

- 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

[4] UNHRC, 'Resolution on the promotion, protection, and enjoyment of human rights on the Internet,' (2016) (accessible here).
[5] Access Now, '#KeepItOn' (accessible here).
[6] Id.
[7] GlobalVoices, 'How internet shutdowns in Myanmar have been endangering lives and affecting humanitarian work since the coup' (2023) (accessible here).
[8] UN, 'Myanmar: UN experts condemn military's "digital dictatorship"' (2022) (accessible here).
[9] Access Now, 'Internet shutdowns in 2021' (2022) (accessible here).
[10] GlobalVoices, 'How internet shutdowns in Myanmar have been endangering lives and affecting humanitarian work since the coup' (2023) (accessible here); and Al Jazeera, 'Myanmar reimposes internet shutdown in Rakhine, Chin states' (2020) (accessible here).

internet was partially restored.[11] Zimbabwe experienced internet shutdowns again in 2022,[12] and there were further reports of the quality of internet access being degraded ahead of the 2023 elections.[13]

- 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 over two and a half years despite a peace agreement between the parties.[14] Furthermore, in mid-2023, the government imposed new restrictions in other parts of the country by blocking access to mobile internet in the Amhara region and restricting mobile data across several major cities in the region.[15] In February 2023, social media platforms including Facebook, TikTok, and Telegram were also shut down.[16]

Shutdowns also occurred in Sudan, Libya, Somaliland, Sierra Leone, Tunisia, and Burkina Faso in 2022, and in Guinea, Mauritania, Uganda, Sudan and Somaliland in 2023.[17] In October 2023, during Mozambique's local government elections, reports recorded internet cuts.[18]

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.[19] As 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 (African Charter). This was further bolstered by the judgment in *SERAP v Federal Republic of Nigeria* (2022) in which the ECOWAS Court held that the government's suspension of Twitter in the country in 2021 also violated the rights to freedom of expression, access to information and the media.[20]

Other regions have seen similar trends. In Colombia, the Constitutional Court held in September 2023 that the government had violated the rights to freedom of expression, association, and assembly due to their failure to provide petitioners with timely, truthful, and

[11] Access Now, 'Zimbabwe orders a three-day, country-wide internet shutdown' (2019) (accessible here).
[12] Access Now, 'Zimbabwe elections 2023: voters need internet access' (2023) (accessible here).
[13] Reliefweb, 'Zimbabwe: Elections marred by arbitrary arrests and fears of internet shutdown" (2023) (accessible here).
[14] Access Now, 'Who is shutting down the internet in 2023? A mid-year update' (2023) (accessible here).
[15] Id.
[16] Id.
[17] Access Now above n 5.
[18] Club of Mozambique, 'CIP Mozambique Elections: Internet cut, counting starts' (2023) (accessible here).
[19] Global Freedom of Expression: Columbia University, '*Amnesty International Togo and Ors v. The Togolese Republic*,' (2020) (accessible here).
[20] Global Freedom of Expression: Columbia University, '*SERAP v. Federal Republic of Nigeria*,' (2022) (accessible here).

complete information about internet shutdowns during public protests that occurred in 2021.[21] The Court ordered the State to respond publicly on these issues.

It has become clear that internet shutdowns are increasingly a tool used by governments to control criticism and protest, especially at times of civil unrest or around election periods, and as military tactics during conflicts. For example, recent internet shutdowns in Ukraine and Gaza demonstrate how access disruptions are used as a tactic of warfare to control information flows:

- Since the invasion of Ukraine by Russia in 2022, internet shutdowns have been routinely used as a part of Russian military tactics to prevent Ukrainians from sharing or receiving news about the war, getting information about humanitarian aid, or fact-checking information.[22]
- Since October 2023, 15 of the 19 internet providers operating in Gaza have faced total shutdowns at the hands of Israeli forces. Internet traffic across Gaza decreased by 80% throughout October 2023 as a result of direct attacks on telecommunications infrastructure, restrictions on access to electricity, and technical disruptions to telecommunications services.[23] Israel's bombing campaign has reportedly specifically targeted network installations and disabled much of the communications infrastructure linking Gaza and the rest of the world.

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 action 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.

[21] Global Freedom of Expression: Columbia University, '*Bejarano v. Ministry of Defense*' (2023) (accessible here).
[22] Access Now, 'Who is shutting down the internet is Ukraine' (2023) (accessible here).
[23] Access Now, 'Palestine unplugged: how Israel disrupts Gaza's internet' (2023) (accessible here).

*Blocking and filtering of content*

In addition to full-scale blackouts, censorship of online content has also been on the rise over the past decade around the world. An increasingly prevalent form is 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 to sieve through content, blocking individual pages that display specific characteristics.[24] Although considered less extreme than internet shutdowns or other measures that fully limit access, such mechanisms are also deeply concerning 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 than 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."[25]

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.[26] The COVID-19 pandemic again illustrated how China blocks and filters content around topics that it deems to be harmful, thereby denying its citizens the opportunity to access information.[27]

China is not alone in this regard. Several governments have taken to censorship in order to control the flow of information, especially around critical times like election periods or conflict. In a 2011 Report, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (UNSR on 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."[28]

Unfortunately, in recent years this trend has continued unabated in several African countries. For example, in early 2019 when 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.[29] More recently, in 2023, NetBlocks reported that Gabon had blocked access to social media platforms on the day of presidential and legislative elections.[30]

---

[24] ARTICLE 19, 'Freedom of Expression Unfiltered: How blocking and filtering affect free speech' (2016) (accessible here).
[25] UDHR at Article 19.
[26] Human Rights Watch, 'China's Global Threat to Human Rights' (2019) (accessible here).
[27] Human Rights Watch, 'In China, the Great Firewall Is Changing a Generation' (2020) (accessible here).
[28] UNHRC, 'Report of the UNSR on FreeEx' (2011) (accessible here).
[29] CNN, 'Chadians feel 'anger, revolt' as they struggle without internet for one year' (2019) (accessible here).
[30] Netblocks, 'Internet cut in Gabon on election day'(2023) (accessible here).

Access was restored after 4 days after military officers announced that they had taken power of the country.[31] Similar social media restrictions have occurred in other countries such as Zambia,[32] Uganda,[33] and Cameroon just before or after election periods.[34]

Blocking and filtering of content is also ordered by governments in order to cover up other violations of human rights:

- In 2021, the Eswatini government ordered all operators to suspend access to Facebook, WhatsApp, and Twitter as it claimed that social media was being used to "spread misinformation" contributing to violence around the country.[35] However, this and other internet disruptions at the time were reported to have been ordered instead to quell pro-democracy protests and reports about police brutality.[36]
- 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.[37] As discussed above, the ECOWAS Court held in a foundational case for social media blocking that the seven-month ban was unlawful and violated the freedom of expression of the people of Nigeria.[38]
- In Zimbabwe in 2022, the opposition Citizens' Coalition for Change (CCC) reported the throttling of internet speeds and blocking of access to social media during a political rally held ahead of the national elections.[39]

This phenomenon is a threat not only to the public's right to access information but also to the very core of democracy which relies on the free flow of information to support informed public participation. 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.

*Social media taxes*

In recent years, several 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, increased barriers to accessing the internet, and limits on freedom of expression and access to information — as well as severe economic impacts.[40]

---

[31] Id.
[32] Netblocks, 'Social media and messaging apps restricted in Zambia on election day' (2021) (accessible here).
[33] Netblocks, 'Social media and messaging restricted, internet shut down for Uganda elections' (2021) (accessible here).
[34] Netblocks, 'Facebook and WhatsApp restricted in Cameroon on eve of election results' (2018) (accessible here).
[35] MISA, 'Eswatini shuts down internet as protests rock monarchy' (2021) (accessible here).
[36] Access Now, 'Eswatini authorities shut down internet to quell protests, ask people to email grievances' (2021) (accessible here).
[37] Emmanuel Akinwotu, 'Nigeria lifts Twitter ban seven months after site deleted president's post,' (2022) The Guardian (accessible here).
[38] *SERAP v. Federal Republic of Nigeria*, ECW/CCJ/JUD/40/22, 2022 (accessible here).
[39] Zimbabwe Independent, 'Cyberspace the new Zim political battlefield,' (2022) (accessible here).
[40] Mozilla Foundation, 'Internet Health Report, 2019,' (2019) (accessible here).

The Web Foundation has noted that Africa is the continent with the highest financial barriers to internet access.[41] Social media taxes add yet another barrier to a resource that is already inaccessible to many, a phenomenon which serves to deepen the digital divide and hinder people's rights.

In Uganda, for example, the government imposed a tax scheme for the daily use of mobile communications apps such as Facebook, Twitter, Instagram, LinkedIn, WhatsApp, Snapchat, and Skype in 2018. 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 scheme's rollout, severely limiting freedom of expression and access to information.[42] Research also found that the tax lowered domestic tax revenue.[43] Uganda subsequently abandoned the over-the-top (OTT) tax but later introduced a new 12% excise tax on internet bundles that is reportedly disproportionately affecting women, exacerbating the gender digital divide.[44]

Tanzania and Zambia have also initiated such schemes, along with attempts in a host of other countries in East and Southern Africa.[45] Some taxes have taken a slightly different form, such as Ghana which implemented a 1.5% levy on electronic money transfers.[46] 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, noting:

> "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

[41] Web Foundation, 'New research explores impact of social media taxes in East and Southern Africa,' (2019) (accessible here).
[42] CIPESA, 'Social Media Tax Cuts Ugandan Internet Users by Five Million, Penetration Down From 47% to 35%,' (2019) (accessible here).
[43] Research ICT Africa, 'COVID-19 exposes the contradictions of social media taxes in Africa,' (2021) (accessible here).
[44] Global Dev, 'Taxation, gender, and internet access: lessons from Uganda,' (2023) (accessible here).
[45] Id.
[46] The Economist, 'African governments hope digital taxes will fill a budget hole,' (2022) (accessible here).

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."[47]

In contrast to the burden of social media taxes placed on internet users on the continent, there is growing support for the notion that international digital platforms, particularly the social media companies, should be taxed in the countries in which they operate and generate revenues, including those in Africa. In 2023, the Organisation for Economic Co-operation and Development (OECD) secured agreement from 138 countries on a landmark initiative that would enable major reform to the international tax system to more fairly tax digital platforms in the jurisdictions in which they earn revenue.[48] This is seen as a more equitable and rational way of boosting tax revenues in countries seeking to benefit from the rise of digital technologies without hindering the expansion of access to the internet to those with limited ability to pay.

*Registration of bloggers, social media users and influencers*

Bloggers are a largely undefined group of people who write online entries, self-publish, might remain anonymous and write either semi-professionally or professionally.[49] In addition to their individual rights to freedom of expression, these types of internet users fulfil an important role in our contemporary society by disseminating information and enabling discussion, and many international standards and guidelines on freedom of expression online provide legal standards that protect bloggers and journalists alike.[50] In recent years, there has been a rising trend of implementing laws and regulations that require these kinds of users to register or obtain licenses in order to continue publishing online:

- In 2018, Tanzania introduced new laws that require bloggers and online television outlets to pay large annual licensing fees (the amounts were subsequently revised in 2021, though are still significant).[51] The law also makes blogging without a license a criminal offence and enables publishers to lose their license for publishing content that "causes annoyance" or "leads to public disorder," drawing 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.[52]

[47] Internet with Borders, 'Bénin: Government Repeals Social Media Tax - Internet Sans Frontières,' (2018) (accessible here).
[48] OECD, '138 countries and jurisdictions agree historic milestone to implement global tax deal,' (2023) (accessible here).
[49] There is some overlap between the formerly popular term of bloggers and the more recent term of influencers or social media users with large-scale followings that publish content in various forms online.
[50] 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. See UNHRC, 'General Comment 34 on Article 19: Freedom of Expression' (2011) (accessible here).
[51] Freedom House, 'The Spread of Anti-NGO Measures in Africa: Freedoms Under Threat,' (2019) (accessible here).
[52] Human Rights Watch, '"As Long as I am Quiet, I am Safe" - Threats to Independent Media and Civil Society in Tanzania,' (2019) (accessible here).

- 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 the sharing of information by licensed persons.[53] The Bill would require the registration of bloggers and allow the Communications Authority to develop a bloggers' code of conduct. As of 2024, the Bill has not yet passed and has since gone through several iterations.
- In 2020, Lesotho proposed the Lesotho Communications Authority (Internet Broadcasting) Rules which sought to require all social media users with over 100 followers to register as "internet broadcasters" and comply with the rules governing broadcast media houses.[54]
- Zambia's Independent Broadcasting Authority likewise issued rules requiring online television stations to obtain a broadcasting license and criminalising online broadcasting without such a license.[55]

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. In order to achieve these benefits, however, access to ICTs must be coupled with digital literacy programmes to enable people to access and make use of the internet safely and meaningfully.

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 570 million African internet users in 2022 — representing exponential growth in the previous decade.[56]

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.

[53] Lex Africa, 'Technology Media & Telecommunications in Africa update' (2023) (accessible here).
[54] CIPESA, 'Towards an Accessible and Affordable Internet in Africa: Key Challenges Ahead' (2021) (accessible here).
[55] Id.
[56] Statista, 'Internet usage in Africa - statistics & facts,' (2024) (accessible here).

**Digital literacy in Africa**

In 2020 Afrobarometer found that 55% of adults in Africa were 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.[57] 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.[58] Africa also falls behind other regions of the world in this regard.[59]

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.[60]

Guidance on the requirements for effective digital literacy programmes is provided under several international instruments. For example, the UN Committee on the Rights of the Child (UNCRC) General Comment 25 on children's rights in relation to the digital environment[61] notes that:

> "State parties should ensure that digital literacy is taught in schools, as part of basic education curricula, from the preschool level and throughout all school years, and that such pedagogies are assessed on the basis of their results. Curricula should include the knowledge and skills to safely handle a wide range of digital tools and resources, including those relating to content, creation, collaboration, participation, socialisation and civic engagement. Curricula should also include critical understanding, guidance on how to find trusted sources of information and to identify misinformation and other forms of biased or false content, including on sexual and reproductive health issues, human rights, including the rights of the child in the digital environment, and available forms of support and remedy. They should promote awareness among children of the possible adverse consequences of exposure to risks relating to content, contact, conduct and contract, including cyberaggression, trafficking, sexual exploitation and abuse and other forms of violence, as well as coping strategies to reduce harm and strategies to protect their personal data and those of others and to build children's social and emotional skills and resilience."[62]

While there are pockets of progress in advancing internet access, improvements in internet access and increases in demand must be 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

[57] Afrobarometer, 'Africa's digital divide and the promise of e-learning,' (2020) (accessible here).
[58] Statista, 'Estimated adoption rate of digital skills in selected African countries in 2019 and 2030,' (accessible here).
[59] Brookings Institute, 'Figures of the week: Digital skills and the future of work in Africa,' (2020) (accessible here).
[60] International Finance Cooperation, 'Digital Skills in Sub-Saharan Africa' (2019) (accessible here).
[61] UN Committee on the Rights of the Child, 'General Comment 25 (2001) on children's rights in relation to the digital environment (accessible here).
[62] Id at para 104. See also paras 54 and 96.

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.

**Digital literacy, online harms, and gender**

Research has shown that women and other historically marginalised groups bear the brunt of online harms perpetrated through the internet, such as cyber-harassment.[63] This means that a failure to implement comprehensive and effective digital literacy programmes is likely to exacerbate the existing gender digital divide by deterring women's participation online and enabling ongoing violations of the right to equality in the digital domain. As such, it is vital that digital literacy programmes be undertaken in a gender-sensitive and informed manner so as to account for and mitigate the particular harms faced by women online.

*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. 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.[64]

Efforts to control the free flow of information have the potential to distort content consumption by enabling free access to certain content in preference to other content, as well as access to the market. Net neutrality may be under threat by the increasingly popular initiative in Africa 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.

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, however, argue that zero-rating is a means for the new internet gatekeepers to centralise power and control access.

**Net neutrality in contestation – India**

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 of India (TRAI) announced that shaping users' access to the internet would not be allowed. India then

[63] Meta and CHR, 'Understanding gender-based violence in Southern Africa,' (2021) (accessible here).
[64] Electronic Frontier Foundation, 'Zero Rating: What It Is and Why You Should Care ,' (2016) (accessible here).

moved to adopt strong net neutrality regulations.[65] However, in 2023, concern arose again following TRAI signalling its interest in understanding the "feasibility of introducing an authorisation framework, network usage fee, and selective banning of internet-based services."[66] In response, Access Now, the Internet Society, and 22 other civil society organisations and technical experts are engaging with the TRAI noting their concern that "the proposed measures, if implemented, will fragment the internet, undermine people's rights, and stifle innovation."[67]

Ways to implement net neutrality vary across a broad spectrum in practice:

> "Worldwide efforts at net neutrality, or the open Internet, have varied from outright prohibition of discriminatory conduct (Brazil), banning differential pricing based on content (India) and prohibiting the blocking of Internet services, usage of deep-packet inspection to track customer behaviour, and otherwise filtering or manipulating network traffic (the Netherlands). Varying ex ante measures such as price regulation, surcharges and zero-rating have been applied with varying degrees of success in Canada, Singapore and Slovenia."[68]

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.[69] 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.[70] Despite this gain, the process has since stalled with concerns that the Independent Communications Authority of South Africa (ICASA) has failed to enforce the zero-rating of government and public benefit organisations.[71]

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

[65] New York Times, 'Facebook Loses a Battle in India Over Its Free Basics Program' (2016) (accessible here); and BBC 'India adopts 'world's strongest' net neutrality norms' (2018) (accessible here). 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 (accessible here).
[66] Access Now, 'There are no free-riding services on the internet: India must uphold net neutrality' (2023) (accessible here).
[67] Id.
[68] Tech Central, 'Is net neutrality legislation needed in South Africa?,' (2021) (accessible here).
[69] South Africa, 'Directions on Zero-Rating of Websites for Education and Health Issued Under Regulation 4(10) of the Regulations Made Under the Disaster Management Act, 2000' (2020) (accessible here).
[70] Alt Advisory, 'South Africa: Spectrum winners to zero-rate access to public benefit organisations' (2022) (accessible here).
[71] DGMT, 'Zero-rating of public benefit organisations – invitation to urgently sign an open request to ICASA' (2023) (accessible here).

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 programmes by powerful international multinationals. The experience in India has highlighted the need to ensure that 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: in 2023, Africa continued to be one of the world's regions targeted most by cybercrime due to the increased digitisation of organisations without the necessary corresponding cybersecurity practices.[72] In 2021, cybercrime was reported to have reduced GDP within Africa by more than 10%, at a cost of an estimated 4.12 billion USD.[73] Similar reports were made for 2022.[74]

Interpol has identified online scams, digital extortion, business email compromise, ransomware and botnets as the top five cyber threats in Africa at present.[75] In addition, the rise of Artificial Intelligence (AI) technologies, including public access to generative AI, is likely to result in a rapid expansion of more targeted and sophisticated cybercrime in the coming years.[76]

While cybercrime itself poses a serious threat to human rights, the corresponding rise of oppressive and aggressive cybersecurity measures is also jeopardising the realisation of an array of digital rights. The UN Conference on Trade and Development (UNCTAD) reports that 39 out of the 54 countries in Africa analysed (72%) have cybercrime legislation in place.[77]

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."[78] 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.

[72] Interpol, 'African Cyberthreat Assessment Report Cyberthreat Trends' (2023) (accessible here).
[73] INTERPOL, 'INTERPOL report identifies top cyberthreats in Africa,' (2021) (accessible here).
[74] Positive Technologies, 'Cybersecurity threatscape of African countries 2022-2023' (2023) (accessible here).
[75] Id.
[76] Security Info Watch, 'Cybersecurity predictions for 2024 reflect more advanced threats,' (2024) (accessible here).
[77] UNCTAD, 'Cybercrime Legislation Worldwide,' (accessible here).
[78] Open Global Rights, 'Restricting cybersecurity, violating human rights: cybercrime laws in MENA region' (2019) (accessible here). See further Public Knowledge, 'Cybersecurity and Human Rights' (2019) (accessible here).

**Litigating broad and vague cybercrimes legislation**

Several cases in sub-Saharan Africa have sought to challenge the trend of over-broad, vague, and potentially stifling cybercrime provisions, with, unfortunately, little success to date. For example, in Nigeria, two cases in the Court of Appeal in Lagos denied constitutional challenges to sections of the country's Cybercrime Act, 2015 that argued for infringements on the right to freedom of expression.[79]

In Kenya, petitioners initially achieved some success in 2018 in securing the suspension of problematic provisions of the Computer Misuse and Cybercrimes Act, 2018; however, the order was overturned, and the provisions were declared constitutional by the High Court in 2020.[80]

## THE RIGHT TO PRIVACY

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

*Data protection*

2016 saw the coming into force of the General Data Protection Regulation (GDPR) in Europe, with widespread consequences for regions around the world as well. It exposed the increasing need to protect the right to privacy in a rapidly changing technological landscape and prompted rapid legislative change in many countries seeking to maintain trade and data flows with the European region.

Comprehensive data protection laws are vital for securing human rights in the digital age, and the GDPR developed, for the first time, some new safeguards that are necessary for the advancement of human rights in the digital age.[81] In particular, it protects people against gratuitous and excessive data collection. In the years since, the sum of fines issued under the GDPR has skyrocketed, reaching a total of over EUR4 billion by the end of 2023.[82] In 2023, the European Data Protection Board reported that the GDPR has strengthened, modernised, and harmonised data protection principles across the EU.[83] Despite this, there have been notable challenges in implementing the GDPR, enforcing fines and rulings made under it, and ensuring compliance with it across the continent, and important interpretative decisions are ongoing.[84]

---

[79] *Okedara v. Attorney General* (2019) (accessible here) and *the Incorporated Trustees of Paradigm Initiative for Information Technology Development v. The Attorney General of The Federation* (2018) (accessible here).
[80] *Bloggers Association of Kenya (BAKE) v Attorney General & 5 others* (2018) and *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another* (Interested Parties) (2020), see here.
[81] Human Rights Watch, 'The EU General Data Protection Regulation,' (2018) (accessible here).
[82] EQS, 'The Biggest GDPR Fines of 2023,' (2024) (accessible here).
[83] European Data Protection Board, 'Contribution of the EDPB to the report on the application of the GDPR under Article 97' (2023) (accessible here).
[84] CMS, 'GDPR Enforcement Tracker Report,' (2023) (accessible here).

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 defines many of the data protection principles that have become in data protection legislation across the world by enabling data subjects 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; and
- Specific inferences that have been made about them based on their personal information.[85]

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. UNCTAD has found that of the 194 countries they reviewed:[86]

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

Progress has also been made in the African context.

**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.

At present, 36 African countries have passed data protection laws, with three further being in the process of considering drafts. Most recently, Tanzania, Uganda and Eswatini passed new data protection laws in 2022 and Nigeria and Somalia in 2023. Kenya also passed new regulations to their data protection law in 2021, in an effort to strengthen their existing law.

Also of significance was the coming into force of the long-awaited African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) in 2023. The Convention aims to create a comprehensive legal framework for electronic commerce, data protection, and cybercrime and cybersecurity on the continent and requires all 55 AU member states to have domestic laws in each of these policy areas which conform to various standards and principles outlined in the Convention.

[85] New York Times, '*How California's New Privacy Law Affects You*' (2020) (accessible here).
[86] UNCTAD, 'Data Protection and Privacy Legislation Worldwide' (2021) (accessible here).

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 or failing to provide these authorities with the independence and resources needed to act effectively.[87] In addition, there have been significant enforcement challenges, with many data protection authorities on the continent struggling with a lack of independence and resources.[88]

Cross-border transactions and multinational corporations that function across multiple jurisdictions require data protection regulations, demonstrating the importance of data 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 enable fundamental rights and ensuring that laws and implemented and enforced. For example, many laws contain exemptions that limit the scope and effectiveness of the law, such as for public or law enforcement agencies,[89] and there may be a need for such laws to be updated to account for the new data protection challenges of artificial intelligence (AI).

*Surveillance*

Mass and targeted surveillance practices are on the rise across Africa, and there is a notable absence of international legal frameworks and strict safeguards in place to prevent human rights abuses. 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. Despite its growing use, mass and targeted surveillance has been challenged in the courts around the world, with some degree of success.

| **United Kingdom** | **South Africa** |
|---|---|
| The European Court of Human Rights (ECHR) 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 | In South Africa, the Constitutional Court in 2021 declared various provisions of the country's 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.[93] The Court ordered a range of amendments to improve transparency, safeguards, and oversight mechanisms for state surveillance operations.[94] |

[87] Accessible at: www.dataprotection.africa.
[88] Access Now, 'Strengthening data protection in Africa: Key issues for implementation,' (2024) (accessible here).
[89] Id.
[93] *AmaBhungane v Minister of Justice and Correctional Services* ZACC 3 (2021) (accessible here).
[94] *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* ZACC 3 (2021) (accessible here).

| | |
|---|---|
| sufficiently protect journalists' confidential communication.[90]<br><br>A new Bill that was introduced in 2023 to amend the country's laws faced public backlash, with commentators arguing that it could threaten technological innovation.[91] The UK has also recently introduced the Online Safety Bill, about which some have expressed concerns regarding clauses which could mandate mass surveillance of private digital communications.[92] | In 2023, South Africa introduced a Bill to amend the unconstitutional law, which has generated much public outcry, with commentators arguing that the Bill falls short of what was demanded by the judgment and fails to address other long-standing issues.[95] Despite this, the Bill has been passed by Parliament and is awaiting signature by the President.[96] |

As ever-more sophisticated technologies are developed, such as biometric surveillance, facial recognition technology, and data analysis using artificial intelligence, the issue of surveillance is only going to grow as a concern for digital rights. Although effective litigation and advocacy can result in important protections and safeguards, it is clear that there is still much to be done by states to put in place more robust legal frameworks and strict safeguards relating to surveillance in the future to avoid such challenges and to protect privacy rights.

**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 across 21 countries been targeted for surveillance by the Pegasus spyware, a system that can be remotely installed on a smartphone enabling complete control over the device.[97] 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

[90] Big Brother Watch v. The United Kingdom (Big Brother I) App nos. 58170/13, 62322/14 and 24960/15 (2018) (accessible here).
[91] techUK, 'Expressing techUK members' concerns regarding the Investigatory Powers (Amendment) Bill' (2023) (accessible here).
[92] Just Security, 'Changes to UK Surveillance Regime May Violate International Law' (2023) (accessible here).
[95] Intelwatch, 'Submission: What's wrong with the RICA bill' (2023) (accessible here).
[96] Parliamentary Monitoring Group, 'Regulation of Interception of Communications and Provision of Communication-related Information Amendment Bill' (2023) (accessible here).
[97] Forbidden Stories, 'Journalists Under Surveillance,' (2021) (accessible here).

press, which may undermine the ability of the press to provide accurate and reliable information."[98]

Africa has unfortunately not been immune to these trends. African activists and journalists were among some of the targets identified in the Pegagus scandal, as were powerful politicians and state officials revealed to be users of the tools. In 2024, Reporters without Borders found spyware traces on the phones of two Togolese journalists while they were on trial for defamation against a government minister.[99]

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 these technologies. This form of surveillance and monitoring is susceptible to an array of abuses, such as:

- Institutional abuse;
- Abuse for personal gain;
- Discretionary targeting;
- Voyeurism; and
- Location monitoring.[100]

Such surveillance is often unregulated or under-regulated and can have a chilling effect on public life, in addition to creating risks of being abused to monitor critics or activists, 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 discrimination and bias.[101]

A 2021 report by Thales (a large producer of surveillance technologies) recorded the following top seven trends of facial recognition:[102]

- 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.

[98] *Sharma v Union of India and Others* 310 of 2021 Supreme Court of India (2021) (accessible (here).
[99] RSF, 'In first for Togo, RSF identifies spyware on phones of two Togolese journalists,' (2024) (accessible here).
[100] ACLU, 'What's Wrong with Public Video Surveillance?' (2002) (accessible here).
[101] European Digital Rights Initiative, 'Facial recognition and fundamental rights 101,' (2019) (accessible here).
[102] Thales, 'Facial recognition: top 7 trends (tech, vendors, use cases)' (2021) (accessible here).

Despite calls for moratoriums on certain uses of these kinds of technology, it is clear that facial recognition technology is here to stay, with expected industry growth of $5.71 billion (USD) in 2024 globally.[103] It is also increasingly being used for surveillance, including across Africa. 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 developments in FRT**

In 2023, the United States introduced the Facial Recognition and Biometric Technology Bill which, if passed, will ban the use of facial recognition by the federal government unless explicitly approved by an Act of Congress. This Bill is a significant step in a nationwide movement to ban government use of face surveillance technology.[104] 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 European Union's GDPR also classifies biometric data as a special type of data and prohibits people from processing it unless the processing thereof falls into one of the lawful categories.[105] In Sweden, a school was fined for taking attendance through FRT, as this processing did not fall into one of the lawful processing categories.[106]

In addition, the new EU AI Act unveiled in 2021, "aims to limit the use of biometric identification systems including facial recognition that could lead to ubiquitous surveillance" by introducing new rules for its use hinging on whether it is defined as "high-risk" or "low risk" usage.[107] However, the proposed provisions have been watered down in subsequent negotiations,[108] as the Act continues to progress through the final stages of approval.[109]

In Brazil, a civil court in São Paulo held that the use of facial recognition technology on a subway line infringed the right to privacy and freedom of expression due to the lack of consent from users, and the subway operator was ordered to stop using the technology.[110]

*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

[103] Statista, 'Facial Recognition- Worldwide' (accessible here).
[104] ACLU, 'The Fight to Stop Face Recognition Technology' (2023) (accessible here).
[105] European Union, 'General Data Protection Regulation' (2018) (accessible here).
[106] Michalsons, 'Biometric laws around the world' (2024) (accessible here).
[107] European Parliament, 'Regulating facial recognition in the EU,' (2021) (accessible here).
[108] Politico, 'EU set to allow draconian use of facial recognition tech, say lawmakers,' (2024) (accessible here).
[109] IAPP, 'EU countries vote unanimously to approve AI Act,' (2024) (accessible here).
[110] The Case of São Paulo Subway Facial Recognition Cameras (2021) (accessible here).

widely used for surveillance purposes. According to a 2023 Review of biometrics by Thales, biometric technologies are most frequently used for the following:[111]

- **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. Civil liberties organisation Liberty has noted that:[112]

> "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. Some advocates argue that biometrics can be particularly useful in electoral settings by potentially:[113]

- Improving voter registration and identification;
- Producing a credible electoral register; and
- Reducing electoral fraud.

**Biometrics and elections in Africa**

Public opinion on the use of biometrics in elections across Africa varies. Biometric technologies have been heralded as having huge potential to curb electoral fraud and ensure that each person can only vote once. However, there are also concerns about implementation challenges, including technological failures and privacy concerns.[114] High

[111] Thales, 'Biometrics: definition, use cases, latest news,' (2023) (accessible here).
[112] Liberty, 'Rights Groups Urge Shops To Reject Facial Recognition,' (accessible here).
[113] Duduetsang Mokoele and Nomaqhawe Moyo, 'Biometric voting has many pitfalls, but it could work in South Africa' (2019) Daily Maverick (accessible here).
[114] Aratek, 'How Biometrics Is Becoming a Norm of Elections in Africa' (2022) (accessible here).

costs, limited data literacy, and ineffective data protection regimes may cause 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.

Despite mixed views, the use of biometrics for voting continues to be on the rise. For example, in 2024 Cameroon's biometric voter registration drive aims to enrol 7.5 million voters ahead of its 2025 general elections.[115] Other African countries such as Ghana, Nigeria and Uganda, amongst others, are similarly implementing or considering implementing biometric systems for elections. CIPESA has documented the deployment of other national biometric technology-based programmes in 16 African countries in recent years.[116]

*Anonymity and encryption*

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."[117] In the 2018, the UNSR on FreeEx stated:

> "the challenges users face [in using these tools] 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."[118]

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 to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection."[119]

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

[115] Biometric Update.com, 'Cameroon launches last full-cycle biometric voter registration before 2025 polls' (2024) (accessible here).
[116] CIPESA, 'State of Internet Freedom in Africa 2022: The Rise of Biometric Surveillance' (2022) (accessible here).
[117] UNHRC, 'UNSR on FreeEx: Report on encryption, anonymity, and the human rights framework' (2015) (accessible here).
[118] UNSR on FreeEx, 'Encryption and Anonymity follow-up report' (2018) (accessible here).
[119] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2015) (accessible here).

security. Many countries in Africa have relatively heavy restrictions on encryption, although Russia and parts of Asia have globally the heaviest restrictions.[120]

**Anonymity on social media**

While threats to encryption are frequently seen to be mere fronts for 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 in facilitating safe discussions about sexuality in environments where such discussions might put them at risk.[121]

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. For example:[122]

- Nigeria's Social Media Bill was introduced in 2019 and, as of 2024, has not yet been passed. However, concerns around the bill's impact on encryption and anonymity resurfaced after the Nigerian President announced in 2023 that the bill had been submitted to parliament.[123] This bill will allow government to examine internet traffic to determine its content, by, for example, restricting the use of end-to-end encryption or requiring the content to be decrypted.[124]

- In Zimbabwe, the Interception of Communications Act mandates cryptography services to decrypt data at judicial authorities' request, with non-compliance punishable by fines or imprisonment.[125]

As challenges to privacy rise, so too will the need to secure anonymity and promote the use of encryption technologies, particularly for journalists, lawyers, activists, and others at risk of oppression. 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.

*Artificial intelligence*

The growing prevalence and use of artificial intelligence (AI), particularly publicly available generative AI tools such as ChatGPT and Microsoft Bing, are raising new questions about the

[120] Comparitech, 'Encryption laws: Which governments place the heaviest restrictions on encryption?' (2022) (accessible here).
[121] The Conversation, 'Online abuse: banning anonymous social media accounts is not the answer' (2021) (accessible here).
[122] CIPESA, 'Policy Brief: How African States Are Undermining the Use of Encryption,' (2021) (accessible here).
[123] Africa News, 'Nigeria proposes new social media regulations' (2023) (accessible here).
[124] Internet Society, 'Internet Impact Brief' (2022) (accessible here).
[125] CIPESA, 'How African Governments Undermine the Use of Encryption' (2021) (accessible here).

widespread collection of personal information to both train these systems and to provide responses to user prompts and the resulting risks to data protection and privacy. Many of these tools have reportedly been trained on the entirety of publicly available information on the internet, which would include personal information shared on social media and other sites, without users having given consent for this use.

Efforts to regulate AI are also, as a result, increasing, most notably through the EU's AI Act, which seeks to "regulate artificial intelligence (AI) to ensure better conditions for the development and use of this innovative technology."[126] It also includes limitations on the use of biometric identification systems by law enforcement and seeks to enable data subjects to receive meaningful explanations about the use of these systems.[127] The European Parliament reached a provisional agreement on the Act in December 2023, setting the scene for it to be passed into law in the coming months.

## THE RIGHT TO FREEDOM OF EXPRESSION

Recent trends indicate that the most significant threat to freedom of expression around the world is the criminalisation of online speech. Criminalisation is affected 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, 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. For example, Zimbabwe's Data Protection Act criminalises the spreading of false information online,[128] and Botswana's Penal Code criminalises publishing "alarming information".[129]

*A growing pandemic of mis- and disinformation*

The rise of what has come to be understood as a global crisis of mis- and disinformation has been accompanied by harsh efforts to crack down on this kind of content by governments, with concomitant risks for the right to freedom of expression online. The consequences of disinformation are far-reaching and can cause significant public harm — such as hampering the ability of the public to make informed decisions or putting public health, security, or the environment at risk. The rapid and widespread proliferation of false information relating to the COVID-19 pandemic and climate change are pertinent examples of this.

Disinformation continues to poison the digital sphere creating serious risks for freedom of expression as states tighten controls. In 2023, Freedom House reported that global internet freedom declined for the 13th consecutive year.[130] AI tools have also become increasingly

[126] European Parliament, 'EU AI Act: first regulation on artificial intelligence,' (2023) (accessible here).
[127] European Parliament, 'Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI,' (2023) (accessible here).
[128] MISA-Zimbabwe, 'Analysis of the Data Protection Act,' (2021) (accessible here).
[129] Southern Africa Litigation Centre, 'False news or free speech: Protecting freedom of expression in Botswana' (2023) (accessible here).
[130] Freedom House, 'The Repressive Power of Artificial Intelligence,' (2023) (accessible here).

sophisticated and widely used in this regard, spurring an escalation of disinformation tactics employed by governments to manipulate online discussions in their favour.

The COVID-19 pandemic gave rise to an outbreak of disinformation, often referred to as an infodemic. This led to many countries to implement false information legislation. For example, South Africa implemented disaster management regulations that created content-related offences with respect to publishing statements surrounding COVID-19.[131] However, even prior to the pandemic, the criminalisation of false news has been popular in Africa:

- Zimbabwe's Data Protection Act, which, as of January 2024 has been enacted but is not yet in force, criminalises the spreading of false information online. The Act states that any person who unlawfully and intentionally makes available, broadcasts, or distributes data to any other person concerning an identified or identifiable person knowing it to be false, with intent to cause psychological or economic harm, will be guilty of an offence. Civil society has raised concerns that this provision promotes self-censorship, and unjustifiably infringes on freedom of expression.[132]
- 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.[133]
- In 2020, Ethiopia passed legislation that increases jail sentences and fines for hate speech and the dissemination of disinformation. Similar to other disinformation laws, commentators have raised concerns about the legislation's violation of freedom of expression.[134]

There are also growing concerns that the rise of AI tools is enabling the production and amplification of mis- and disinformation on an unprecedented scale and in ways that make identification and moderation of such content extremely difficult.[135] Freedom House has also documented the use of AI by governments to conduct propaganda and spread disinformation.[136]

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.

---

[131] ARTICLE 19, 'South Africa: Prohibitions of false COVID-19 information must be amended' (2021) (accessible here).
[132] MISA-Zimbabwe, 'Analysis of the Data Protection Act,' (2021) (accessible here).
[133] Al Jazeera 'Nigerians raise alarm over controversial Social Media Bill' (2019) (accessible here).
[134] Al Jazeera, 'Ethiopia passes controversial law curbing 'hate speech' (2020) (accessible here).
[135] Axios, 'How AI will turbocharge misinformation — and what we can do about it,' (2023) (accessible here).
[136] MIT Technology Review, 'How generative AI is boosting the spread of disinformation and propaganda,' (2023) (accessible here).

**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 a "Code of Practice on Disinformation."
- InterAction released a toolkit to assist people with preparing for online disinformation threats.
- Global Partners, the Centre for Human Rights at the University of Pretoria, Article 19 West Africa, CIPESA and PROTÉGÉ QV have jointly launched LEXOTA — an interactive tool to help track and analyse government responses to online disinformation across Sub-Saharan Africa.
- The Real 411 is a collaborative initiative between South African CSO Media Monitoring Africa and the country's Independent Electoral Commission (IEC) that enables social media users to report disinformation, hate speech, and other harmful content to be adjudicated by independent experts and submitted to the digital platforms for removal, if appropriate.

**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. In South Africa, the Johannesburg High Court dealt with the tensions between freedom of expression and the right to dignity in the online realm in *Manuel v Economic Freedom Fighters*, in which the Respondents had made untrue statements on Twitter about the Applicant.

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'."[137]

There is undoubtedly a need to counteract the above groundswell. However, states are quickly turning to the criminalisation of online content to address this, rather than targeting 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 related to hate speech 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. As of January 2024, the Bill has been passed by Parliament and is waiting to be signed into law.
- The proposed Prohibition of Hate Speech Bill, 2019 in Nigeria is another relevant example, but it was withdrawn after public outcry.[138]

However, international law standards and guidance are increasingly encouraging states to move away from sanctions and prohibitions towards more positive measures. ARTICLE 19, for example, emphasises that states should engage with the symptomatic causes of hate speech rather than adopting a singularly punitive approach.[139] 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 that UN entities should take, 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; and
- 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 meaningfully and substantively with hate speech and find ways that address hate speech without limiting freedom of expression.

---

[137] UN, 'Strategy and Plan of Action on Hate Speech' (2019) (accessible here).
[138] Mondaq, 'Nigeria: Revisiting Nigeria's Legal Framework On Hate Speech And Fake News Post 2023 General Elections,' (2023) (accessible here).
[139] Article 19, 'Responding to 'hate speech' with positive measures: A case study from six EU countries, (2018) (accessible here).

*Online violence against journalists, bloggers, and other professionals*

In 2023, the UN warned of a concerning trend of the escalation of violence and repression against journalists and other communicators.[140] Harassment of journalists, bloggers, and other professionals is the most extreme form of media censorship and creates a climate of fear which impedes the free circulation of information, opinions, and ideas. In particular, the COVID-19 pandemic and coverage of climate change, biodiversity, and pollution have attracted threats and efforts to silence journalistic outputs.

**Social media is a platform for information dissemination and expression**

Media Defence recently supported plaintiffs in the 2023 landmark case on media freedom at the ECOWAS Court - *Isaac Olamikan & Anor v. Federal Republic of Nigeria*. The journalists faced deregistration due to their online journalistic activities. Nigerian journalists Isaac Olamikan and Edoghogho Ugberease brought their grievances to the regional court after separate arrests while covering news events. Olamikan was accused of operating with an expired media license, while Ugberease, a citizen journalist in southern Nigeria's Edo state, was deemed unqualified for journalistic work.

They argued that strict educational requirements, age limits, and registration procedures discriminated against them and curtailed their freedom of expression. The Court agreed, finding flaws in provisions regarding journalist registration and editor appointment qualifications by the Nigerian Press Council, failing to recognize the public interest served by online and citizen journalists. Emphasizing the evolving media landscape, the Court highlighted the influential role of influencers and content creators in shaping public opinion, noting that social media offers an unrestricted platform for information dissemination and expression. Commentators note:

> "The decision of the ECOWAS Court of Justice plays an imperative role in policies for both online and citizen journalism and in citizens' right to be informed. In this case, amending these rules per the development of online media would ensure protection for journalists but also for activists who deploy their advocacy and raise awareness on social issues on their online platforms."

According to a 2021 UNESCO discussion paper, women journalists are most impacted by threats and attacks, with 73% of women journalists surveyed saying that they have been threatened, intimidated, and insulted online in connection with their work and 30% having responded to online violence by self-censoring on social media.[141]

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. A global survey conducted by the International Centre for Journalists and the Tow Centre for Digital Journalism shows that 20%

[140] UN, 'Violence against journalists, the integrity of elections, and the role of public leadership' (2023) (accessible here).
[141] UNESCO, 'The Chilling: global trends in online violence against women journalists,' (2021) (accessible here).

of respondents describe their experience of online abuse as "much worse than usual" during the COVID-19 pandemic.[142] In the United States, 90% of journalists believe that online harassment is the biggest threat to their profession.[143]

The consequences of these attacks are significant for freedom of expression. A 2017 Reporters without Borders study by the Council of Europe further indicated that:[144]

- 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; and
- 57% of journalists do not report that they have been the targets of online violence.

UNESCO's research 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.[145] Black, Indigenous, Jewish, Arab, and lesbian women journalists participating in the 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.

**ACHPR Joint Declaration on Media Freedom and Democracy**

In 2023, the African Commission on Human and Peoples' Rights (ACHPR), together with other international and regional bodies, issued a joint declaration in the context of growing threats to legal protection of the media, increasing online and physical attacks against journalists, and judicial harassment of media outlets and journalists, which restrict their ability to hold government authorities and powerful actors to account. The Declaration highlights that media freedom is integral to democracy and upholds freedom of expression for a variety of reasons. For example, free and independent media plays a key role in acting as fact-checkers against disinformation and propaganda and so help to repair trust in democratic institutions.

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.

[142] International Centre for Journalists and the Tow Centre for Digital Journalism, 'Journalism & The Pandemic: A Global Snapshot of Impacts' (2020) (accessible here).
[143] CPJ, 'Why newsrooms need a solution to end online harassment of reporters,' (2019) (accessible here).
[144] Reporters Without Borders, 'Online harassment of journalists: Attack of the trolls,' (accessible here).
[145] UNESCO above n 140.

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, for example, 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.[146]

## 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 for human rights, 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 and AI use proliferates. 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.

[146] *Brown v Economic Freedom Fighters* [2019] ZAGP JHC (2019) (accessible here).