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/).