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/

Table of Contents

Introduction 1

The Right to Access Information 2

Internet shutdowns 2

Social media taxes 3

Registration of bloggers 4

Blocking and filtering of content 5

Increased access and the need for digital literacy and safeguards 6

The interplay between net neutrality and zero-rated content 7

The rise in cybercrimes and cyber attacks 8

The Right to Privacy 9

Data Privacy 9

Surveillance 11

The collection of biometric data and the use of facial recognition technologies 12

Anonymity and encryption 13

The Right to Freedom of Expression 14

Efforts to address disinformation 14

Efforts to address hate speech 17

Harassment of journalists, bloggers and other professionals 18

Conclusion 19

MODULE 1

General Overview of Trends in Digital Rights Globally and Expected Developments

- **To provide an overview of global trends in digital rights.**
- **To set out trends and expected developments in the context of the right of access to information, particularly trends that pose a threat to access to information.**
- **To set out trends and expected developments relating to privacy rights, including current and potential threats.**
- **To set out trends and expected developments regarding 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 January 2020, the digital population consists of 4.54 billion users.[1] In Africa, the number of internet users grew from 110.9 million to 522.81 million between 2010 and 2019.[2] The internet has undeniably revolutionised the free flow of information between individuals by offering anyone with an internet connection the ability to gather and share information and ideas.[3] This has had a profound effect on the exercise and the protection of the triad of information rights, which includes the right to privacy, the right to freedom of expression and the right to access information. The 2016 Resolution of United Nations Human Rights Council (**UNHRC**) 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. When these rights are advanced and exercised online, they deserve the same protections as when they are advanced offline.

Unfortunately, and despite the capabilities of the internet to provide opportunities and fulfil an essential role as a tool for democratic empowerment, it is regularly undermined by authoritarian ideals. Clear trends have emerged globally, with all internet users facing, to varying degrees, similar opportunities, challenges, threats and human rights violations.

The tensions between human rights and freedoms, and the rise in restrictions of access to online spaces, will continue. With increased political polarisation and the seemingly limitless powers of non-state actors, it will be a challenge to restore the internet to a dynamic

[1] Statista, 'Global digital population as of January 2020' (accessible at https://www.statista.com/statistics/617136/digital-population-worldwide/) and Statista 'Number of internet users worldwide from 2005 to 2019' (accessible at https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/).
[2] Statista, 'Number of internet users worldwide from 2009 to 2019, 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/).

environment, which is shaped by innovation and where there are lasting possibilities for realising human potential and capacity. Ultimately, the goal is the protection and development of online spaces where human rights can be protected, respected and promoted. Fortunately, there are, in many instances, effective responses to oppressive regulations, 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 it 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. Internet shutdowns, blocking and filtering of content, social media taxes, censorship and distributed denial of service (**DDoS**) attacks have been some of the common dangers facing internet users.

Internet shutdowns

Several countries have been affected by internet shutdowns in the past ten years. Myanmar, Zimbabwe and India 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 Myanmar Posts and Telecommunications insisted that the internet shutdowns were for the benefit of the people.[4] The start of 2020 saw another spate of internet shutdowns in two of Myanmar's conflict-ridden states.[5]

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.[6] India had nearly 100 internet shutdowns during 2019, including the most protracted recorded shutdown in history in Kashmir.[7] During the last quarter of 2019, the Supreme Court in India ruled that indefinite internet shutdowns violated freedom of speech and expression. Resultantly, the government was ordered to in future publish reasons, including the duration of the shutdown each time it wishes to implement this action.[8]

At the rate at which the internet shutdown trend is growing, there is a possibility that this may be something that governments will continue to implement in the future, especially at times of civil unrest or around election periods. However, the recent jurisprudential developments in

[4] 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/).
[5] 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).
[6] 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/).
[7] BBC, 'Why India shuts down the internet more than any other democracy' (2019) (accessible at https://www.bbc.com/news/world-asia-india-50819905).
[8] Time, 'India's Supreme Court Orders a Review of Internet Shutdown in Kashmir. But For Now, It Continues' (2020) (accessible at https://time.com/5762751/internet-kashmir-supreme-court/).

India may spark necessary civic awareness to ensure the protection of people's right to access information.

#KeepItOn

Access Now's STOP Project, in collaboration with the #KeepItOn coalition, has been monitoring and reporting on internet shutdowns across the globe. The #KeepItOn coalition has been fighting internet shutdowns with various creative approaches, including grassroots advocacy, direct policy-maker 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.

Social media taxes

There has been a growing trend, particularly in Africa, where states have been introducing, or considering introducing, taxes specifically for the use of social media. The 2019 Internet Health Report on Taxing Social Media in Africa found:

> "Governments have imposed these levies to raise public revenues, and also argue that they are protecting the local telecommunications sector from competition from internet companies from abroad. But in practice, the (intended or unintended) consequence has been to push more people offline, increase barriers to getting online, and vastly limit freedom of expression and access to information — as well as access to goods and services that are now online."

The Web Foundation aptly noted that Africa is the continent with the highest financial barriers to internet access. An already largely inaccessible resource will only be compounded further with social media taxes, which will, in turn, deepen the digital divide and hinder people's access.

In Uganda, the government imposed a new tax scheme for the daily use of mobile communications apps such as Facebook, Twitter, Instagram, and LinkedIn, as well as instant messaging and voice communication apps such as WhatsApp, Snapchat and Skype. The consequence of this tax has seen people being pushed offline. These taxes are a relatively new and concerning state practice that increases barriers to online access and severely limits access to information. 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 the space of three months following the imposition of the social media tax scheme.

Uganda is one of many African countries that are considering the imposition of social media taxes. Reporters Without Borders has noted with concern that Zambia and Benin are similarly

seeking to introduce social media taxes. However, despite these growing concerns, there have been notable successes in challenging this emergent threat.

Don't Tax My Megabytes

The citizens of Benin recently 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 "TaxePaMesMo" (Don't Tax My MegaBytes). After a few weeks of concerted digital protest, the government repealed the tax.

Internet Without Borders welcomes this victory and notes:

> "The mobilisation online, around the Hashtag #TaxePamesMo (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 #TaxePaMesMo is indicative of innovative forms of digital protest aimed at challenging the introduction of these taxes.

Registration of bloggers

Bloggers – the 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 in many ways are akin to journalists, and given that a variety of individuals can exercise journalism, there should be legal standards that protect bloggers and journalists alike. The United Nations General Comment 34 to the International Covenant on Civil and Political Rights (**ICCPR**) included bloggers in its assessment of journalism. It stated that any restrictions on the operation of websites, blogs or any other internet-based systems are not compatible with the right to freedom of expression.

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, a potential new trend is that of blogger registration. Freedom House reported that in 2018, Tanzania introduced new laws that require bloggers to pay licensing and registration fees. This is an economically untenable situation given that Tanzania's GDP per capita is approximately $1000 (USD), and the licence fee for bloggers is approximately $900 (USD). Human Rights Watch has criticised the decision that makes blogging without a licence a criminal offence. The licensing fee has introduced a severe barrier to freedom of expression and the dissemination of information. The disproportionately high fees are pushing bloggers offline. Of further concern are the criminal offences now attached to bloggers. In 2019, the Daily Maverick reported that select bloggers in Zimbabwe were repeatedly detained and tortured, with one blogger, in particular, being charged with cybercrime offences but later acquitted.

Growing threats to formal and informal modes of journalism are on the rise, and there is little indication, at this stage, that there are genuine efforts to address it. Imposing burdensome obligations on bloggers and journalists are likely to become a standard practice unless states are compelled to respect and protect their international human rights obligations.

Blocking and filtering of content

Censorship has been on the rise over the past decade. The most prevalent 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.[9] Similar to internet shutdowns, but not as extreme, blocking and filtering may in some instances be 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." Internet shutdowns do however differ slightly from blocking and filtering—the former results in complete loss of access, whereas the latter results in partial and influenced access.

In the last decade, China has emerged with 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.[10] However, China is not alone in this regard. Several African governments have taken to censoring to control the flow of information, especially around critical times like elections 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,

[9] 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).
[10] 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).

> 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, 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 the recommendation to amend the Constitution to allow the President to remain in power until 2033.[11]

This phenomenon is a threat not only to the public's right to access information, but also the very core of democracy. It is expected that with increases in the number of people with access to the internet, resultant increases in censorship may be seen.

Increased access and the need for digital literacy and safeguards

Information and Communication Technologies (**ICTs**) in many ways fulfil the ever-important role of 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.

Trends indicate an increase in access to ICTs. In 2017, the World Bank reported that Africa was "primed to continue its momentum in the ICT sector", which would lead to increased industrialisation of the ICT sector and economic growth. Statista recorded that Africa has taken great strides over the last decade, with steady and sizeable growth resulting in an increase from 110 million internet users in 2010 to 522.81 million users in 2019, placing Africa as the region with the third-highest number of interest users. Statista further recorded that as of January 2020, the Republic of Congo and the Democratic Republic of Congo have ranked as the top two fastest growing online populations based on relative year-on-year user growth.

Along with shifting digital frontiers, there is a corresponding and urgent need to ensure that digital literacy remains a priority. Digital literacy is critical to ensuring that the full potential of human and digital development is realised.

Digital literacy in Africa

UNICEF's report on Raising Learning Outcomes: the opportunities and challenges of ICT for learning notes that Burkina Faso has recognised that ICTs play an increasingly important role in access to knowledge. However, due to weak infrastructure, low maintenance capacity and insufficient means to acquire devices, the digital literacy rates are not where they should be.

[11] 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).

The report further notes that due to limited finances in Namibia, "essential services in education" do not include ICTs. In Ghana, there is a growing market for technology-based products, even though these products are more accessible to private educational institutions.

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.[12]

While there are pockets of progress, the access, demand and literacy rate in Africa needs to be aligned, and there should be concerted efforts to ensure that the full spectrum of ICT opportunities is available to everyone. Access to the internet will undoubtedly continue to grow. Without appropriate digital literacy, 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 – the principle that seeks to ensure that access to content is open, free-flowing, fair, and equal – has the potential to be under threat by the principle of zero-rating, which aims to direct internet traffic. 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 our information society. In contrast, zero-rating has the potential to distort content consumption, as well as access to the market. There are levels to this debate, with some, such as multinational corporations, arguing that zero-rating can be a tool to facilitate universal access to the internet. 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.

The debate regarding net neutrality and zero-rating ebbs and flows depending on which states are for or against it at any point in time. During 2015 and 2016, the India-Facebook-Airtel controversy took centre stage, with Facebook and Airtel offering differential pricing for access to certain content and no-fee access to other content. Following public outcry and a rejection of Facebook's alleged plan to provide universal access to the internet, 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.[13]

[12] 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).

[13] 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).

The United States has recently engaged this issue, which resulted in the 2019 Federal Communications Commission decision to repeal net neutrality laws.[14] While the repeal was upheld by the Federal Appeals Court in 2020, digital rights activists suggest that this might not be the end of the road for the net neutrality debate in the United States.[15]

This debate is likely to continue with states changing course and multinational corporations finding new ways to provide access, on their terms. Developing and transitioning economies will remain at risk of zero-rating with pressure to accept some access rather than no access. This is an unfortunate trend that undermines the potential of developing and transitioning economies. Hopefully, the Indian example will shine a light on the need to have access that is not controlled by service providers who may have particular agendas or may use development as a guise to control access for people who are most in need of it.

The rise in cybercrimes and cyber attacks

Cybercrimes are becoming more sophisticated, more dangerous, and are in many ways developing more rapidly than their response mechanisms. Attacks on individual users, businesses, CSOs and states are becoming commonplace. It has been reported that 4.1 billion records were exposed to data breaches in the first half of 2019. Hackers are estimated to attack every 39 seconds, averaging over 2200 attacks per day. Further to this, there is a substantial economic concern with the rise of cybercrime costing an estimated $3 trillion (USD) by 2020.

The World Economic Forum listed the following as the most pressing cybersecurity issues in 2019, which are expected to be on the rise in 2020:

- **Advanced phishing kits**: Of notable concern is the increase in the availability of phishing kits, allowing people with basic skills to conduct phishing attacks.
- **Remote access attacks**: These types of attacks are becoming more sophisticated, specifically targeting cryptocurrency.
- **Attacks via smartphones**: Unsafe browsing is playing a significant role in the rising online fraud rate, with more than 60% of online fraud committed on mobile platforms.
- **Vulnerabilities in home automation and the Internet of Things**: The Internet of Things industry is expected to grow by 7 billion devices in 2020. There are concerns that insecure designs will create risks for devices, which will become targets not only for data collection but for attackers to launch tools, or DDos attacks.
- **Utilising artificial intelligence (AI)**: Developing AI for malicious purposes is a genuine threat, and can be used to avoid detection, amplify phishing attacks and better facilitate social engineering.

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

[14] 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/).
[15] EFF, 'D.C. Circuit Offers Bad News, Good News on Net Neutrality: FCC Repeal Upheld, But States Can Fill the Gap' (2019)(accessible at https://www.eff.org/deeplinks/2019/10/dc-circuit-offers-bad-news-good-news-net-neutrality-fcc-repeal-upheld-states-can).

Cybersecurity was identified as an emerging global trend in 2014 and has since mushroomed into a booming industry.

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."[16] The intense and often vague legislative measures implemented to counteract cybercrime are arguably doing little to take fundamental human rights and freedoms into account, leaving internet users vulnerable to both the crime and the harsh response. It is expected that cybercrimes will continue to outpace cybersecurity measures. In response, 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 data collection. Since coming into effect, to date, approximately 95 000 complaints have been filed, and 59 000 breaches have been reported, with approximately 60 million euros worth of fines imposed.[17]

The California Consumer Privacy Act (**CCPA**) came into effect in January 2020, seeking to address how private companies are allowed to collect and use 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.[18]

[16] 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/).
[17] 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/).
[18] 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."[19]

Beyond the GDPR and CCPA, other countries have started to data privacy laws which are aimed at protecting people's data. The UN Conference on Trade and Development (**UNCTAD**) has found that of the 107 countries they reviewed (of which 66 were developing or transition economies):

- 57% of countries have data protection legislation.
- 10% of the states have draft legislation.
- 21% of countries have no legislation.
- 12% of countries have no data available.

UNCTAD further found that Africa ranks at the lower end of the spectrum, with ten of the reviewed countries having no legislation and five with draft legislation. The Democratic Republic of Congo was found to have no legislation for electronic transactions or cybercrime, and there was no data on consumer protection and privacy and data protection. Mozambique was found to have draft legislation for electronic transactions, no legislation regarding cybercrime and no data on consumer protection and privacy and data protection. Egypt has electronic transactions and cybercrime legislation and draft legislation for consumer protection, but no legislation relating to privacy and data protection. Kenya recently enacted the 2019 Data Protection Act, which provides for the regulation of the processing of personal data, the rights of data subjects and obligations on data controllers.

While many countries have data protection frameworks in place, there is a significant lack of implementation of these frameworks. A typical example would be South Africa. The Protection of Personal Information Act 4 of 2013 was signed into law in 2013, but the substantive provisions of the legislation are still not in force.[20]

Data Protection in Africa

Data Protection Africa (DPA) is an online tool that provides a full review of data protection laws in 32 African countries. The website 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.

[19] 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).
[20] Privacy International, 'State of Privacy in South Africa' (2019) (accessible at https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa).

- What steps can be taken to remedy such breaches, including the contact information of operational data protection authorities.

The GDPR and the CPAA have hopefully set the tone going forward and there is a high possibility that other states will follow suit. This is not necessarily because other states are eager to endorse the data protection status quo of the GPDR and the CPAA, but rather because cross border transactions and multinational corporations that function across multiple jurisdictions require data protection regulations. It appears that African states are recognising the need to enact data protection laws in light of this trend.

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. Surveillance is a genuine affront to the right to privacy.

The European Court of Human Rights is currently seized with the matter of *10 Human Rights Organisations v. United Kingdom* in which human rights defenders are challenging several issues relating to the powers of the British government to engage in surveillance. In South Africa, the *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* case is presently challenging issues in relation to the South African surveillance regime, which was found to be unlawful and invalid. The case came before South Africa's Constitutional Court in February 2020 in order for the Court to determine whether to confirm the unconstitutionality of specific provisions of the Regulation of Interception of Communications and Provisions of Communication Related Information Act.

These two developments indicate that the issue of surveillance is one of which the international community is aware. This could mean that states may be obligated to put in place more robust legal frameworks and strict safeguards relating to surveillance in the future.

Further to this, the use of video surveillance and closed-circuit television (**CCTV**) is becoming a common surveillance occurrence across the world. Increased security threats have generated excessive responses by state and non-state actors who justify the widespread use of CCTV. This form of surveillance and monitoring is susceptible to an array of abuses. The American Civil Liberties Union identified the following:

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

CCTV cameras are mostly unregulated and have a chilling effect on public life. The quality and sophistication of video surveillance is becoming more salient, but Privacy International warns that:

> "Such developments in video technology will undoubtedly be applied in contexts that are beneficial. However, the egregious capabilities enabled by the improved technology must be of primary concern before rushing to implementation."

The collection of biometric data and the use of facial recognition technologies

Biometric data collection entails the identification and authentication of a person based on unique biological characteristics. 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, and the use of encryption keys and passwords is declining. The pace at which biometrics are being implemented is a cause for concern. Ford predicts that states may not be equipped to deal with security and data storage challenges; alternatively, countries might be well equipped and are using biometrics for nefarious purposes. There are 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."

The perpetual catch-22 with the rise of technology is equally relevant in relation to biometrics. The 2020 Report by Gemalto on biometric voter registration reveals that value can be gained from biometric technology, particularly in ensuring the improvement of electoral processes. Daily Maverick suggests that biometrics can potentially:

- Improve voter registration and identification.
- Produce a credible electoral register.
- 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.[21]

The use of biometrics for voting is on the rise in Africa. Privacy International reports that Niger is the latest of over 30 African countries to adopt biometric technologies during elections.

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.

European Digital Rights (**EDRi**) explains that facial recognition technology is a type of biometric identification which "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 $3.2 billion (USD) in 2019 to $7 billion (USD) by 2024 in the United States.[22] Facial recognition will likely continue to be used for surveillance, with strong activism needed to ensure that appropriate safeguards are put in place.

Anonymity and encryption

In the 2015 Report of the UNSR on FreeEx, 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 that:

[21] 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).
[22] 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).

> "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."

Forbes predicts that in 2020 "image security and privacy will percolate to become a top cybersecurity concern, driven by anonymity erosion." Forbes quoted the CEO of 1Password, who predicts:

> "In 2020, governments are going to take an even more active role in cybersecurity through encryption regulation. Governments have been clumsy in their attempts to legislate encryption because that technology has been light years ahead of those that are supposed to regulate it. Next year, they'll be playing catch-up."

Bloomberg published an article in February 2020 suggesting that India's new rules on social media require large social media companies to reveal users' identities if requested to do so by the Indian government. Bloomberg reports that the new rules could strip 400 million social media users of the anonymity.

As challenges to privacy rise, so will the need to secure anonymity and promote reliance on encryption technologies. These technologies will most likely continue to develop and become more sophisticated. As they do, the threat of increased state intrusions in the private lives of citizens may also rise.

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. The Council of Europe, in its 2019 Report on threats and attacks against media freedom in Europe, found that journalists, in particular, are facing these challenges. It noted that in Turkey, more than 200 journalists have been arrested or detained on account of their publications.

Efforts to address disinformation

The Independent High-level Group on Fake News and Online Disinformation recorded that spreading of false, inaccurate, or misleading information that is designed to intentionally cause harm or generate profit continues to be one of the 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.

Disinformation continues to poison the digital sphere creating serious risks for freedom of expression as states tighten controls. In 2018 Freedom House reported:

- Global internet freedom has persistently declined since 2010.
- Nearly 20 countries had enacted or proposed legislation that would criminalise the spreading of false news. (The Washington Post reported that Singapore, Nigeria and Ethiopia have recently followed suit.)

It is predicted that in the run-up to the upcoming 2020 US elections, disinformation will again reach new heights.[23]

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.[24]

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 will also be monitored, and those who utter such statements will be liable to fines and, possibly, imprisonment.[25]

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.[26]

---

[23] The Atlantic, 'The Billion-Dollar Disinformation Campaign to Re-elect the President: How new technologies and techniques pioneered by dictators will shape the 2020 election' (2020) (accessible at https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530/).

[24] Protection from Online Falsehoods and Manipulation Act, 2019 (accessible at https://sso.agc.gov.sg/Acts-Supp/18-2019/Published/20190625?DocDate=20190625).

[25] 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).

[26] 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).

If the start of 2020 is anything to go by, there are major concerns for the continued spread of disinformation. Reports are emerging that disinformation about the Coronavirus is spreading faster than the virus itself.[27] The spreading of false news around the coronavirus has been labelled as an "infodemic" according to the World Health Organisation.[28] Social media platforms are playing an active role in trying to redirect the spread of the infodemic by encouraging users to visit legitimate sites such as the World Health Organisation.[29]

However, despite the alarming and current rise of disinformation, 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.

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".
- Harvard is assisting people with "4 Tips for Spotting a Fake News Story".
- Infographics are being designed to assist people with disinformation detection.
- 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.

African Court 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, awareness and dialogue. Despite negative forecasts, the rise of digital activism can play a critical role in rerouting the current trajectory.

[27] Washington Post, 'The coronavirus is spreading rapidly. So is misinformation about it' (2020) (accessible at https://www.washingtonpost.com/health/2020/02/10/coronavirus-is-spreading-rapidly-so-is-misinformation-about-it/).
[28] BBC News 'WHO says fake coronavirus claims causing 'infodemic'' (2020) (accessible at https://www.bbc.com/news/technology-51497800).
[29] Id.

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.

Similar justifications and repressive legislation have been seen in response to hate speech. Many of the laws discussed above that target disinformation also target hate speech. The Internet Health Report reported that Germany has recently enacted legislation that seeks to decrease hate speech online. South Africa has been in the process of adopting the Prevention of Combating of Hate Crimes and Hate Speech Bill that aims to prevent and combat hate crimes and hate speech.

There are also growing practices encouraging states to move away from sanctions and prohibitions towards more positive measures. ARTICLE19 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 seeks to ensure effective responses. 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. 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

The UN reported:

> "In just over a decade, more than 1,000 journalists have been killed while carrying out their work. In nine out of 10 cases, no one was held accountable. Last year alone, the UN agency advocating for freedom of the press, UNESCO, reported that at least 99 journalists were killed and thousands more were attacked, harassed, detained or imprisoned on spurious charges, without due process. Women journalists are often at greater risk of being targeted, including through online threats of sexual violence."

Journalists fulfil an important role in any society but are often at risk. UNESCO's 2018 Report on trends in the safety of journalists notes that there has been a marked increase over the last decade in the frequency and regulatory harassment of journalists, bloggers and other professionals. Comprehensive statistics are available which 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 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.

The UN reported that women are facing increased challenges. It has been recognised that "[o]ver the past 15 years there has been 'a marked increase' in cyber harassment, making the safety of women journalists a significant issue for reportage in today's digital era."

The Council of Europe found that within the first two months of 2020, the following alerts have been raised:

- Slovak Columnist Charged with Criminal Defamation for Criticism of Priest.
- Head of the Russian Republic of Chuvashia says Critical Journalists Should be "Wiped Out".
- Threats and Insults against Female Journalists.
- Arson Attack against Newspaper.

The harassment of journalists is a global issue and remains a deeply entrenched problem. 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.

Conclusion

The last decade has seen unprecedented online development. It was a decade of emerging opportunities and threats. It is likely that the next decade will pose many of the same risks and opportunities but will do so at an incomparable rate. The developments in the digital landscape over the next decade are likely to increase exponentially.

Digital divides will hopefully decrease with improved access and increased efforts towards digital literacy. Threats to privacy are likely to magnify in quantity and intensity. Freedom of expression will remain 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.