Module 7

CYBERCRIMES

Summary Modules on Litigating Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

Published by Media Defence: www.mediadefence.org
This module was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Originally published in December 2020
Revised in November 2022

This work is licenced under the Creative Commons Attribution-NonCommercial 4.0 International License. This means that you are free to share and adapt this work so long as you give appropriate credit, provide a link to the license, and indicate if changes were made. Any such sharing or adaptation must be for non-commercial purposes and must be made available under the same “share alike” terms. Full licence terms can be found at https://creativecommons.org/licenses/by-ncsa/4.0/legalcode.

TABLE OF CONTENTS

MODULE 7

CYBERCRIMES

- **As access to the internet continues to grow rapidly in Africa, cybercrimes are becoming ever more prevalent and dangerous.**
- **However, laws which regulate criminal activity on the internet are increasingly providing tools for States to suppress dissent and the media.**
- **The African Union (AU) has encouraged a harmonised, continent-wide approach to tackling cybercrimes in Africa, but the AU Convention on Cyber Security and Personal Data (Malabo Convention) has not yet achieved widespread adoption, limiting its efficacy.**
- **Despite the limited adoption of the Malabo Convention, data privacy is starting to attract more widespread attention across the continent, with many countries recently passing new data protection legislation.**
- **Concerningly, many cybercrimes have a particularly gendered nature, such as cyberstalking and the non-consensual sharing of intimate images (NCII).**
- **There are, however, various practical steps that can be taken to address cybercrimes, and ensure that fundamental rights are equally protected both off- and online.**

INTRODUCTION

The increase in internet access in the recent past has created a number of new legal challenges. The internet is transnational, amorphous, and difficult to define, and as such the new landscape created by the digital world has often confounded the law when it comes to protecting fundamental rights in the digital age. Old definitions about what constitutes a publisher or a journalist are increasingly complicated; overcoming the anonymity afforded by many internet platforms can be a difficult, if not impossible, endeavour; and there are serious questions about who is liable for content shared online that may affect multiple parties in different jurisdictions.

Regulating and legislating crimes that occur on, or relate to, the internet has been a difficult undertaking for states and international bodies. It is estimated that African economies are

losing $4 billion annually due to cybercrimes,[1] roughly 10% of the continent's GDP,[2] and Africa now has the third highest number of cybercrime victims in the world.[3] Without adequate regulatory frameworks and protections, the growth of internet access, e-commerce, and economic development is likely to lead to increased instances of cybercrimes.

In Africa, where the number of new internet users continues to grow at a rapid rate, the increase in access to the internet and information and communications technologies (ICTs) has also led to increased violations of users' rights. Laws to regulate criminal activity on the internet are increasingly providing tools for the state to suppress dissent or to punish critics and independent media because of their often vague and overly broad nature.

As far back as 2011, the United Nations (UN) Special Rapporteur on freedom of expression warned that:

> "[L]egitimate online expression is being criminalized in contravention of States' international human rights obligations, whether it is through the application of existing criminal laws to online expression, or through the creation of new laws specifically designed to criminalize expression on the internet. Such laws are often justified on the basis of protecting an individual's reputation, national security or countering terrorism, but in practice are used to censor content that the Government and other powerful entities do not like or agree with."[4]

Unfortunately, little has changed in the intervening period.

WHAT IS A CYBERCRIME?

Definition

There is no precise, universal definition of the term 'cybercrime.' In general terms, it refers to a crime that is committed using a computer network or the internet.[5] This can cover a wide range of activities, including terrorist activities and espionage conducted with the help of the internet and illegal hacking into computer systems, content-related offences, theft and manipulation of data, and cyberstalking.[6]

---

[1] World Economic Forum, 'Africa must act now to address cybersecurity threats. Here's why,' (2022) (accessible at: https://www.weforum.org/agenda/2022/08/africa-must-act-to-address-cybersecurity-threats/#:~:text=African%20businesses%20not%20prioritizing%20cybersecurity&text=According%20to%20Techcabal%2C%20Africa%20is,damage%20to%20brand%20and%20reputation).

[2] Interpol, 'African Cyberthreat Assessment Report,' (2021) at p. 9 (accessible at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwip9NmDu-z6AhUEnVwKHeQgDnYQFnoECAoQAQ&url=https%3A%2F%2Fwww.interpol.int%2Fcontent%2Fdownload%2F16759%2Ffile%2FAfricanCyberthreatAssessment_ENGLISH.pdf&usg=AOvVaw3wl6pEW7imKb0QSn5twzq6).

[3] Caryn Dolley, 'Cyberattacks: South Africa, you've been hacked,' Daily Maverick (2021) (accessible at: https://www.dailymaverick.co.za/article/2021-11-06-cyberattacks-south-africa-youve-been-hacked/).

[4] United Nations General Assembly, Human Rights Council, 17th Session, 'Report of the Special Rapporteur on freedom of expression' at p10 (2011) (accessible at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf).

[5] Article 19, 'Freedom of Expression and ICTs: overview of international standards' at p 25 (2018) (accessible at: https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf).

[6] *Id.*

Cybercrimes and cybersecurity are two issues that cannot be separated in an interconnected digital environment. Cybersecurity, or the management of cybercrimes, refers to the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisational and user's assets, such as computing devices, applications and telecommunication systems.[7]

Cybercrimes in international law

The African Union (AU) has sought to encourage a continent-wide approach to tackling cybercrimes through the Convention on Cyber Security and Personal Data Protection (known as the Malabo Convention).[8] Because of the cross-border and international nature of cybercrimes, the AU argues that "national legislation cannot be drafted in isolation and national governments must seek to harmonize national legislation, regulations, standards and guidelines on Cybersecurity issues."[9] However, even the AU itself was the target of a major cyberattack between 2013 and 2017,[10] and the Malabo Convention has been criticised for using vague language which may be open to abuse by states. An example is the provision that criminalises the use of insulting language.[11]

Article 25 of the Malabo Convention calls on states to adopt legislation and/or regulatory measures to prosecute cybercrimes. Nevertheless, the text is clear that such legislation should not infringe on fundamental rights and freedoms:

> "In adopting legal measures in the area of cybersecurity and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others."[12]

The UN General Assembly Resolution on the Creation of a global culture of cyber security also states that:

> "Security should be implemented in a manner consistent with the values recognised by democratic societies, including the freedom to exchange thoughts and ideas, the free flow

[7] ITU Definition of Cybersecurity, (accessible at: https://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx).
[8] Institute for Security Studies, Karen Allen 'Is Africa cybercrime savvy?' (2019) (accessible at: https://issafrica.org/iss-today/is-africa-cybercrime-savvy).
[9] African Union, 'A global approach on Cybersecurity and Cybercrime in Africa,' (accessible at: https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf).
[10] Le Monde, 'A Addis-Abeba, le siège de l'Union africaine espionné par Pékin' (2018) (accessible at: https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html).
[11] African Union 'Convention on Cyber Security and Personal Data Protection' Article 3(g) (2014) (accessible at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection).
[12] *Id*.

> of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency."[13]

The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention, is the only binding international instrument on cybercrime and serves as a useful guideline for countries developing cybercrime legislation.[14]

Cybercrimes in domestic law

Cybercrime legislation has proliferated across Africa in recent years but, unfortunately, at the time of publication, the Malabo Convention had been ratified by only thirteen of the fifteen states required for it to enter into force.[15]

In order to ensure that cybercrimes laws do not unnecessarily infringe on the fundamental rights to freedom of expression, privacy and access to information, they should meet the following criteria:

- Provide narrow, clear, and adequate definitions of cybercrimes.
- Require proof about the likelihood of harm arising from a given criminal activity.
- Require the nature of the threat to national security resulting from any criminal activity to be identified.
- Provide for a public interest defence in relation to the obtaining and dissemination of information classified as secret.
- As a general principle, not impose prison sentences for expression-related offences, except for those permitted by international legal standards and with adequate safeguards against abuse.[16]

TYPES OF CYBERCRIMES

Data privacy violations

The use of data, including the volume of cross-border data flows, is increasing exponentially every year, particularly in relation to personal data. However, there is a lack of adequate regulations over the collection and processing of personal information in Africa. 33 African countries currently have data protection or cybercrime laws in place,[17] but their

[13] UN General Assembly, Fifty-seventh session, 'Resolution on the Creation of a global culture of cyber security, at p 3 (accessible at: https://digitallibrary.un.org/record/482184?ln=en).
[14] Council of Europe, 'Budapest Convention and Related Standards', (accessible at: https://www.coe.int/en/web/cybercrime/the-budapest-convention).
[15] African Union, 'List of countries which have signed, ratified/accede to the African Union Convention on Cybersecurity and Personal Data Protection,' (2022) (accessible at: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf).
[16] Media Defence, 'Training manual on digital rights and freedom of expression online, at pp 62 (2020) (accessible at: https://www.mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf).
[17] United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation

comprehensiveness and effectiveness varies significantly. Some of the most recently passed laws were in Zimbabwe, Zambia, Rwanda, and Eswatini, which passed laws between 2021-2022.[18] Several African countries have successfully set up Data Protection Authorities (DPAs) to enforce data protection regulations and investigate violations, though many such DPAs still suffer from a lack of funding and political support, leading to a lack of proper enforcement.

These developments follow the rapid development of data protection legislation around the world since the entry into force of the European Union's General Data Protection Regulations (**GDPR**) in 2018. The GDPR has set a new standard for the protection of personal data online and has served as a template for numerous other countries' legislation. The California Consumer Privacy Act (**CCPA**) likewise has set sweeping regulations regarding consumers' rights to know what personal information is being collected from them, to request deletion of their data, and to opt out of data collection.[19] Because of its application to the technology sector of Silicon Valley, the CCPA has also been lauded for advancing the state of data protection globally.[20]

The rise of sophisticated surveillance technologies and the use of biometric technologies without proper safeguards are just some of the many threats to the right to privacy across Africa. There have, however, been some encouraging judgments in recent years pointing to the willingness of judiciaries around Africa to protect the right to privacy.

In Kenya, the High Court in Nairobi ruled in 2020 in *Nubian Rights Forum and Others v The Hon. Attorney General and Others*[21] that the government could not implement a new comprehensive digital identity system without an adequate data protection law being in place. On surveillance, the Constitutional Court of South Africa found in the case of *amaBhungane and Another v Minister of Justice and Correctional Services and Others*[22] in 2021 that mass surveillance and the interception of communications by the National Communications Centre were unlawful, and declared certain sections of the Regulation of Interceptions of Communications and Provision of Communication Related Information Act (RICA) unconstitutional.

Criminalisation of online speech

Cybercrime legislation usually seeks to deal with a wide range of illegal or harmful content that is posted online. This may include terrorist propaganda, racist content, hate speech, sexually explicit content such as child sexual abuse material (**CSAM**), blasphemous content, content

Worldwide,' (2021) (accessible at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide).

[18] Zimbabwe, Zambia, Rwanda, and Eswatini.

[19] Forbes, 'California Begins Enforcing Broad Data Privacy Law – Here's What You Should Know' (2020) (accessible at: https://www.forbes.com/sites/siladityaray/2020/07/01/california-begins-enforcing-broad-data-privacy-law---heres-what-you-should-know/?sh=1279e683de5c).

[20] The Guardian, 'California's groundbreaking privacy law takes effect in January. What does it do?' (2019) (accessible at: https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do).

[21] High Court of Kenya in Nairobi, Consolidated petitions no. 56, 58 & 59 of 2019, (2020) (accessible at: http://kenyalaw.org/caselaw/cases/view/189189/).

[22] Constitutional Court of South Africa, Case No. Case CCT 278/19, (20121) (accessible at: https://www.mediadefence.org/resource-hub/resources/amabhungane-v-minister-of-justice-2021/).

critical of states and their institutions, and content unauthorised by intellectual property rights holders.[23]

This is often the area in which such legislation most conflicts with the right to freedom of expression and the right to information. The UN Special Rapporteur on Freedom of Expression stated in 2011 that the only types of expression that states may prohibit under international law are: (a) child pornography;[24] (b) direct and public incitement to commit genocide; (c) hate speech; (d) defamation; and (e) incitement to discrimination, hostility or violence.[25] Even legislation that does criminalise these forms of expression needs to be precise, have adequate and effective safeguards against abuse or misuse and include oversight and review by an independent and impartial tribunal or regulatory body.[26] In 2018, the Special Rapporteur stated that "[b]roadly worded restrictive laws on "extremism", blasphemy, defamation, "offensive" speech, "false news" and "propaganda" often serve as pretexts for demanding that companies suppress legitimate discourse."[27]

In Zimbabwe, for example, the Cyber Security and Data Protection Act, passed in 2021,[28] was published in the Zimbabwean Government Gazette shortly after extensive public protests had taken place over rising fuel and commodity prices in the country. It is intended to consolidate cyber-related offences and provide for data protection and seeks to "create a technology-driven business environment and encourage technological development and the lawful use of technology."[29] However, the Act has been widely criticised as being a tool for the Zimbabwean government to stifle freedom of expression and access to information, promote interference of private communications and data and use search and seizure powers to access the information of activists in order to quell protests.[30] Before it was passed, MISA-Zimbabwe criticised the Bill for:

> "Criminali[sing] the sending of messages that incite violence or damage to property. In the past, this charge has been used to prosecute organizers of peaceful protests and other forms of public disobedience. The same goes for sections 164A and 164B that criminalize the sending of threatening messages and cyber-bullying and harassment respectively."[31]

---

[23] Article 19, 'Freedom of Expression and ICTs' (2018) (accessible at: https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf).
[24] Although this term is used the report, the preferred terminology is "Child sexual assault material" (CSAM).
[25] United Nationals Special Rapporteur on the Right to Freedom of Opinion and Expression, Frank La Rue, (2011) para 25 (accessible at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf).
[26] *Id* at para. 71.
[27] United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression, (2018) para 13 (accessible at: https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf.)
[28] Zvamaida Murwira, 'Zimbabwe: Milestone Cyber Security Bill Sails Through Parly,' AllAfrica (2021) (accessible at: https://allafrica.com/stories/202109030611.html).
[29] ALT Advisory Africa, 'Zimbabwe gazettes Cyber Security and Data Protection Bill' (2020) (accessible at: https://altadvisory.africa/2020/05/20/zimbabwe-gazettes-cyber-security-and-data-protection-bill/).
[30] Paradigm Initiative, 'On Zimbabwe's Approval of a Cybercrime and Cybersecurity Bill' (2019) (accessible at: https://paradigmhq.org/zimbabwe-cybercrime-bill/).
[31] MISA-Zimbabwe, 'Commentary on Cybersecurity and Data Protection Bill HB 18 of 2019' (2019) (accessible at: https://zimbabwe.misa.org/wp-content/uploads/sites/13/2020/06/Commentary-on-Zimbabwe-Cybersecurity-and-Data-Protection-Bill-2019.pdf).

Prominent journalists and activists have seen been arrested under these provisions, leading to criticism that the Act criminalises digital activism.[32]

For more on the criminalisation of online speech, see Module 3 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online.

Cyberstalking and online harassment

Online harassment is becoming increasingly prevalent with the spread of social media, which can provide especially fertile ground for online harassment. Cyberstalking is undue harassment and intimidation online through text messages, phone calls or social media, and it severely restricts the enjoyment that persons have of their rights online, particularly vulnerable and marginalised groups, including women and members of sexual minorities. Research has shown that online harassment is often focused on personal or physical characteristics, with political views, gender, physical appearance, and race being among the most common.[33] Furthermore, women encounter sexualised forms of online harassment at much higher rates than men.[34] Journalists are also particularly at risk due to their public-facing roles and efforts to stifle independent media: research by UNESCO has found that almost three-quarters of women journalists have experienced online violence.[35]

A worrying new trend: non-consensual dissemination of intimate images

A particular form of online harassment that has emerged as a concerning new trend is that of private and sexually explicit images, mostly affecting women, being shared publicly online without their permission or consent, often by former partners in retaliation for a break-up or other falling out, or for the purposes of extortion, blackmail or humiliation. However, few countries' cybercrime legislation specifically caters for offences related to the non-consensual dissemination of intimate images (NCII), often leaving victims with little recourse against perpetrators.[36]

South Africa is an exception, having passed the Film and Publications Board Amendment Act[37] in 2019 which, for the first time, explicitly criminalised the practice of non-consensual dissemination of intimate images, stating that:

[32] MISA-Zimbabwe, 'Analysis of the Data Protection Act,' Kubatana (2021) (accessible at: https://kubatana.net/2021/12/06/analysis-of-the-data-protection-act/).
[33] Pew Research Center, 'Online harassment 2017, (2017), (accessible at: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/).
[34] *Id*.
[35] UNESCO, 'Top 26 Preliminary Findings,' (accessible at: https://en.unesco.org/sites/default/files/the-chilling_top26.pdf).
[36] For example, although legislation in both Malawi and Uganda includes anti-pornography and anti-obscenity provisions, neither cater specifically to NCII situations, often leaving victims with little recourse. For more see Chisala-Tempelhoff and Kirya, 'Gender, law and revenge porn in Sub-Saharan Africa: a review of Malawi and Uganda' (2016) (accessible at: https://www.nature.com/articles/palcomms201669).
[37] South Africa Film and Publications Board Amendment Act, 2019 (accessible at: https://static.pmg.org.za/Films_and_Publications_Act.pdf).

> "[A]ny person who knowingly distributes private sexual photographs and films in any medium including through the internet, without prior consent of the individual or individuals and where the individual or individuals in the photographs or films is identified or identifiable in the said photographs and films, shall be guilty of an offence and liable upon conviction."[38]

Practical steps to take if you are a victim of non-consensual dissemination of intimate images:

- Make a record (and copies) of the content posted online, to ensure permanent documentation of the crime. This should include the date the content was posted, where it was posted, and who posted it. Screenshots are a useful way to do this.
- Seek psycho-social and legal assistance. (You may be able to interdict the further dissemination of images or video.)[39]
- File a report with the police. Even if your country does not have a specific provision for the non-consensual dissemination of intimate images, an offence may be located within the existing criminal law.
- File a report with the platform on which the content was posted. It might also help to include a copy of the police report in your report to the platform.[40]

The importance of a name:

The non-consensual dissemination of intimate images is often referred to as 'revenge porn.' However, activists and researchers have universally rejected the term as being misleading.[41] Firstly, the word 'revenge' implies that the victim has committed a harm worth seeking revenge for, and 'porn' conflates the practice with the consensual production of content for mass consumption, which NCII decidedly is not. Secondly, the term "repackages an age-old harm as a new-fangled digital problem," belying the long history that exists of images of women being distributed non-consensually across a range of mediums.[42] Lastly, the term oversimplifies the offence by ignoring a range of aggressors and motivations and invoking a moralist reaction against the victim.[43]

---

[38] *Ibid* at section 24(E).
[39] See Case number A3032-2016 in the High Court of South Africa for reference (2017) (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2017/297.html).
[40] News24, Oberholzer, 'What to do if you're a victim of revenge porn & image-based abuse,' (2020) (accessible at: https://www.sowetanlive.co.za/s-mag/2020-06-29-what-to-do-if-youre-a-victim-of-revenge-porn-image-based-abuse/).
[41] GenderIT, '"Revenge Porn": 5 important reasons why we should not call it by that name' (2019) (accessible at: https://www.genderit.org/articles/5-important-reasons-why-we-should-not-call-it-revenge-porn).
[42] *Id*.
[43] Association for Progressive Communications, 'Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences' (2017) at p.21 (accessible at: https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf)).

Many stalking crimes begin online before moving offline,[44] and cyberstalking can be complicated for many reasons:

> "[Cyberstalking is] online harassment, threats, intimidating messages and subscribing the victim to unwanted online services. From the outset this interaction may be considered an irritation or an annoyance or may give rise to a belief that harm may be caused. The cyber-stalker may however initiate contact in a non-confrontational manner and proceed to woo or groom the victim into a cyber-friendship in order to gain the victim's confidence and to determine personal details such as the person's address. Without the victim's knowledge the same "cyber-friend" could be stalking the victim in person, perhaps even giving the victim advice on how he or she should respond to the stalker. Although cyberstalking which has escalated into stalking the victim in person i.e. "real-time stalking" may result in the commission of a sexual offence, it is not the only outcome."[45]

Because of this complexity, as well as the rapid evolution of technology that makes it difficult for regulation to keep up, the South African Law Reform Commission recommended that specific reference to cyberstalking not be included explicitly in law:

> "In reality, however surreal "cyberstalking" or the use of technical or computerised equipment to stalk a person is it fundamentally amounts to an extension of physical stalking. One is merely dealing with a different medium."[46]

Ongoing harassment and attacks on members of the media have also become a particularly concerning trend.

Online harassment of the media

Where journalists allege imminent threats to their safety, courts are empowered to grant interdictory relief in appropriate circumstances and subject to the relevant legal requirements.

For instance, in the matter of *South African National Editors Forum and Others v Black Land First and Others*,[47] the High Court of South Africa granted an interdict in favour of the media broadly, in terms of which the respondents were interdicted from "engaging in any of the following acts directed towards the applicants: intimidation; harassment; assaults; threats; coming to their homes; or acting in any manner that would constitute an infringement of their personal liberty", and from "making any threatening or intimidating gestures on social media… that references any violence, harm and threat."[48]

[44] South Africa Law Reform Commission, 'Report on Stalking,' (2006) (accessible at: https://www.justice.gov.za/salrc/reports/r_pr130_stalking.pdf).
[45] *Id* at p 182.
[46] *Id* at p 183.
[47] High Court of South Africa in Johannesburg, Case No 23897/17, (2017) (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2017/179.html).
[48] *Ibid* at para. 29.

Cyberbullying

It is also worth noting the crime of cyberbullying, which is the sending of intimidating or threatening messages, often via social media, and which is pervasive among children and young adults.[49] According to the United Nations Children's Fund (UNICEF):

> "[Cyberbullying] can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. Examples include:
>
> - spreading lies about or posting embarrassing photos of someone on social media;
> - sending hurtful messages or threats via messaging platforms;
> - impersonating someone and sending mean messages to others on their behalf.
>
> Face-to-face bullying and cyberbullying can often happen alongside each other. But cyberbullying leaves a digital footprint — a record that can prove useful and provide evidence to help stop the abuse."[50]

The scale of the problem is significant and growing. A study by UNICEF and the UN Special Representative of the Secretary-General (SRSG) on Violence against Children found that one in three young people in 30 countries reported being a victim of online bullying.[51]

David v Goliath: tackling cyberbullying on tech platforms

In South Africa, the family of a teenager who was sent graphic threats through Instagram from an anonymous account was pitted against one of the largest technology companies in the world, Facebook, the former owner of Instagram.[52] The girl, believing the threats were from someone attending her school, feared for her physical safety and therefore attempted to force Facebook to release the identity of the person behind the anonymous account sending the threats. Multiple attempts to do so were futile, forcing the family to turn to the courts for relief. The case is an example of the challenges in holding multi-national companies to account in the digital age and raises questions about how far their responsibility to protect children who use their platforms should go.

[49] News24, above at no. 35. For more on online harassment see pp. 38-44 of Module 4 of Media Defence's Advanced Modules on Digital Rights and Freedom of Expression Online accessible at: https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/).
[50] UNICEF, 'Cyberbullying: What is it and how to stop it' (accessible at: https://www.unicef.org/end-violence/how-to-stop-cyberbullying).
[51] UNICEF, 'UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying' (2019) (accessible at: https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying).
[52] Daily Maverick, 'Anonymously threatened with gang rape and murder, SA teenager takes Facebook Inc to court to disclose perpetrator' (2020) (accessible at: https://www.dailymaverick.co.za/article/2020-07-24-anonymously-threatened-with-gang-rape-and-murder-sa-teenager-takes-facebook-inc-to-court-to-disclose-perpetrator/).

Other violations

Given that the Malabo Convention has yet to be tested in practice, a reading of the Budapest Convention on Cybercrime, the first international treaty that seeks to address internet and computer crimes, is instructive.[53] It is increasingly being used in Africa and has served as a guideline or source for more than 80% of states around the world to develop domestic cybercrimes laws.[54] It is also open for any state willing to implement its provisions to join and can be ratified by African countries.[55]

The Budapest Convention defines the following types of cybercrimes:

- Illegal access to a computer system;
- Illegal interception;
- Data interference;
- System interference;
- Misuse of devices;
- Computer-related forgery;
- Computer-related fraud;
- Child pornography;
- Offences related to infringements of copyright and related rights.[56]

Although these definitions date to 2001, much of what constitutes cybercrimes today is still covered by these categories and provisions.

TRENDS IN AFRICA

As the AU has previously noted that:

> "[T]he rapid pace of innovation in the ICT sector can result in gaps in the legislative and regulatory cybersecurity framework since the challenge for the legislator is the delay in the recognition of the new types of offences and the adoption of amendments to the applicable legislation."[57]

As a result, many African governments have been keenly adopting new cybercrime legislation in an attempt to keep pace and to continue to protect against crimes committed online. Currently, at least 39 African states have basic cybercrime legislation either fully or partially in place, though many are missing implementing regulations.[58]

---

[53] Council of Europe, 'The State of Cybercrime Legislation in Africa – an Overview' at p. 2 (2015) (accessible at: https://rm.coe.int/16806b8a79).
[54] Council of Europe, 'The global state of cybercrime legislation 2013 – 2020: A cursory overview,' at page 5 (2020) (accessible at: https://rm.coe.int/3148-1-3-4-cyberleg-global-state-feb2020-v1-public/16809cf9a9).
[55] Council of Europe, 'Chart of signatures and ratifications of Treaty 185' (2020) (accessible at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures).
[56] Council of Europe above n 48 at p 8.
[57] African Union above n 9 at p 3.
[58] UNCTAD above n 17.

However, cybercrime legislation is increasingly being used to unjustly regulate internet content as well, including undesirable criticism or dissent. Access Now notes that one of the main concerns about the plethora of laws that are currently being enacted to regulate cybercrimes — whilst there may be a legitimate aim in doing so — is that many of them lack clear definitions and are susceptible to being used to regulate online content and restrict freedom of expression.[59] This is a growing concern among human rights defenders regarding a wave of arrests and convictions of activists and journalists in what is an escalating assault on freedom of expression by cybercrime laws. Many of the laws are vague and overbroad, lacking clear definitions, leaving them open to arbitrary and subjective interpretation.

For example, Nigeria's Cybercrime Act of 2015 has been widely criticised for being used to suppress dissent and silence the media.[60] The Committee to Protect Journalists states that in just the first year of the law being in force, five bloggers who criticised politicians and businesspeople online and through social media were accused of the crime of cyberstalking under the new law, which carries a fine of up to 7 million naira (USD$22 000) and a maximum jail term of three years. According to Paradigm Initiative Nigeria, it gives law enforcement "extensive powers to hold personal data without corresponding liability" and has "no provision… to seek redress."[61] It also makes the all-too-common error of using vaguely defined "national security" as a justification for outlawing a wide range of online activities.[62] In 2020, the ECOWAS Community Court of Justice (**ECOWAS Court)** ruled that section 24 of the Act — which criminalises the sending of grossly offensive, indecent, or false messages — did not align with Nigeria's obligations under the African Charter and the ICCPR, and ordered Nigeria to repeal or amend the law.[63]

Other common problematic clauses in cybercrime legislation include those that criminalise the "creation of sites with a view to disseminating ideas and programmes contrary to public order or morality", "broadcasting information to mislead security forces", "publication of false information," and more.[64] Recently, Zimbabwe, Eswatini, Tanzania, Zambia, Uganda, Rwanda, and Malawi have recently passed cybercrimes legislation.[65] Zambia's Cyber Security and Cyber Crimes Act is currently being challenged at the Constitutional Court by a group of

[59] Access Now, 'When "cybercrime" laws gag free expression: stopping the dangerous trend across MENA' (2018) (accessible at: https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/).
[60] Committee to Protect Journalists, Peter Nkanga 'How Nigeria's cybercrime law is being used to try to muzzle the press' (2016) (accessible at: https://cpj.org/2016/09/how-nigerias-cybercrime-law-is-being-used-to-try-t/).
[61] *Id.*
[62] OrderPaper, 'Tomiwa Ilori, The Nigerian Cybercrimes Act 2015: Is It Uhuru Yet?' (accessible at: http://www.orderpaper.ng/nigerian-cybercrimes-act-2015-uhuru-yet/).
[63] The Incorporated Trustees of Laws and Rights Awareness Initiatives v Nigeria, ECOWAS Court Suit No. ECW/CCJ/APP/53/2018 (2020) (accessible at: http://www.courtecowas.org/wp-content/uploads/2020/09/JUD_ECW_CCJ_JUD_16_20.pdf).
[64] *Id* at p 8.
[65] Media Defence, 'Mapping Digital Rights and Online Freedom of Expression Litigation in East, West and Southern Africa,' (2020) (accessible at: https://www.mediadefence.org/resource-hub/resources/mapping-digital-rights-and-online-freedom-of-expression-litigation-in-east-west-and-southern-africa/).

civil society organisations alleging that it contains provisions that threaten the right to protection of the law and the right to freedom of expression.[66]

In the case of *Andare v Attorney General of Kenya*,[67] the High Court of Kenya emphasised that the state has a duty to demonstrate that cybercrimes laws are permissible in a free and democratic society, to establish the relationship between the limitation and its purpose, and to show that there were no less restrictive means to achieve the purpose intended.[68]

STEPS TO TAKE IN RESPONSE TO ONLINE HARMS

This section lays out practical approaches to dealing with various online harms.

Actions taken by state actors

- **Tell the story and engage in advocacy**. While ensuring that the identity of the victim or survivor is fully protected, identify the online harms committed, brief the press and start an advocacy campaign. Too often, reportage is limited in terms of the perpetration of online harms which enables these practices to grow.
- **Consider domestic legal challenges.** Many cybercrime laws in Africa arguably breach fundamental rights and freedoms, especially in their vagueness and generality. In such cases, recourse to the courts may provide relief, especially in constitutional democracies. In cases where existing legislation does not cater specifically for crimes committed online, there may be an opportunity to apply or develop existing laws, such as criminal laws.
- **Approach regional courts**. In cases where cybercrimes legislation is being used to unjustly violate rights and freedoms and domestic courts are not amenable or domestic avenues have been exhausted, there may be recourse in regional human rights courts such as the ECOWAS Court, the East African Court of Justice, or the African Court on Human and Peoples' Rights, if jurisdiction can be established. These courts have jurisdiction to determine State compliance with regional human rights agreements and related legal instruments.[69]

Actions taken by non-state actors

- **Consider obtaining an interdict or harassment order.** A harassment order can be an inexpensive civil remedy useful in cases where the behaviour may not constitute a crime but may impact negatively on the rights of a person. The order prohibits a person from harassing another person, and breaching it constitutes an offence, which is usually

[66] MISA-Zimbabwe, 'Zambia's newly enacted cybercrime law challenged in court,' (2021) (accessible at: https://zimbabwe.misa.org/2021/04/06/zambias-newly-enacted-cybercrime-law-challenged-in-court/).
[67] High Court of Kenya at Nairobi, Petition No. 149 of 2015 (2015) (accessible at: http://kenyalaw.org/caselaw/cases/view/121033/).
[68] See also, *Shreyal Singh v India*, Writ 167 of 2012 (accessible at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2015/06/Shreya_Singhal_vs_U.O.I_on_24_March_2015.pdf).
[69] International Justice Resource Center, 'Courts and Tribunals of Regional Economic Communities,' (accessible at: https://ijrcenter.org/regional-communities/).

punishable by a fine or a period of imprisonment. Many anti-harassment acts include bullying and cyberstalking. Legal representation is usually not necessary, and orders can be applied for at the lower courts.[70]

- **Report behaviour to the relevant platform that was used.** Most social media platforms have mechanisms for reporting illegal or unethical behaviour, which may result in content being taken down or the offending user being blocked either temporarily or permanently. It may help to review the relevant platforms' terms of use prior to reporting to identify the most salient term that has been violated.[71]

CONCLUSION

Although the rise of cybercrimes must be addressed, a growing trend of using cybercrimes legislation to clamp down on dissent and free speech is deeply concerning. While the internet is a rapidly evolving space, legislation can and should be designed to include specific protections for online harms both at an individual level, such as cyberstalking and at a societal level, such as regulating the flow and use of personal data. Social media companies also have a role to play in ensuring that their platforms are not used for the distribution of illegal and harmful content. More generally, there is a need for countries in Africa to collaborate on an approach to tackling cybercrimes, which are frequently transnational in nature.

[70] Department of Justice and Constitutional Development, Protection from Harassment Act, 2011 (Act 17 of 2011 (accessible at: https://www.justice.gov.za/forms/form_pha.html).

[71] Complaints platforms are available:
Facebook: https://www.facebook.com/help/263149623790594;
Instagram: https://help.instagram.com/192435014247952;
Twitter: https://help.twitter.com/en/rules-and-policies/twitter-report-violation#:~:text=Open%20the%20profile%20you'd,the%20issue%20you're%20reporting;
YouTube: https://support.google.com/youtube/answer/2802027?co=GENIE.Platform%3DAndroid&hl=en-GB; and
TikTok: https://support.tiktok.com/en/privacy-safety/report-inappropriate-content-default.