Module 1

VIOLENCE AGAINST WOMEN JOURNALISTS IN SUB-SAHARAN AFRICA

Modules on Online Violence against Journalists in Sub-Saharan Africa

MEDIA DEFENCE

Published by Media Defence: www.mediadefence.org
This module was prepared with the assistance of Catherine Muya, Sigi Waigumo Mwanzia, and ALT Advisory: https://altadvisory.africa/

Published in 2024

TABLE OF CONTENTS

MODULE 1

VIOLENCE AGAINST WOMEN JOURNALISTS IN SSA

- **Online violence against women journalists not only violates the individual rights to freedom of expression, freedom of the press, the right to privacy, equality and non-discrimination, and the freedom of violence among others but also has widespread societal impacts.**

- **Violence against women journalists has increased rapidly in recent years, enabled by online tools, and is exacerbated for journalists with multiple intersecting identities.**

- **Women journalists face different forms of online violence, despite strong legal protections.**

- **States have both positive and negative obligations to protect women journalists, and various other actors must take urgent steps to play their part in protecting these journalists and reducing systemic online violence.**

1. INTRODUCTION

Online assaults targeting women journalists pose one of the gravest contemporary threats to their safety, gender equality, and media freedom. These attacks are often vicious, coordinated, highly sexualized, and malicious, particularly targeting women belonging to religious and ethnic minorities or gender non-conforming individuals.[1] Regrettably, the various manifestations of online violence faced by women journalists with various intersecting identities are the "new frontline in journalism safety."[2] There are several distinct characteristics of online violence targeting journalists:

- **Impact**: Online violence targeting women journalists[3] aims to belittle and intimidate them, fostering a climate of fear and withdrawal.[4] It further seeks to tarnish their professional credibility, undermining trust in the media. This "amounts to an attack on democratic deliberation and media freedom, encompassing the public's right to access information, and it cannot afford to be normalised or tolerated as an inevitable aspect of online discourse, nor contemporary audience-engaged journalism."[5]

[1] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on reinforcing media freedom and the safety of journalists in the digital age' (2022) (accessible here) at para 36 (UNSR on FreeEx Report).
[2] International Centre for Journalists, 'Online Attacks on Women Journalists Leading to 'Real World' Violence, New Research Shows' (2020) (accessible here).
[3] For conciseness, we refer hereafter to "women", however, this does not discount online violence perpetrated against members of the queer community, gender non-conforming persons, sexual and gender minorities, vulnerable members of society, or persons with disabilities. Where specific reference is to women, this should be read as a comment on a descriptive reality, and not be read as a prescriptive or exclusionary statement of which members of society may be victims and survivors of online violence.
[4] UNESCO 'The Chilling: Global trends in online violence against women journalists' (2021) (accessible here) at 6 (The Chilling).
[5] Id.

- **Rights implications**: The right to be free from discrimination, threats, and violence applies both off- and online. Countering online violence that targets women journalists is critical to the promotion of, among others, the rights to freedom of expression, media freedom, and privacy. It is not only limited to the digital sphere but frequently spills into physical spaces.[6]

- **Targets:** While any person can be a victim of online violence, women and those with marginalised or 'at risk' identities are disproportionately targeted and affected by online violence due to their gender, sexual orientation, identity, and other intersecting factors.[7] Often targeted as a result of their gender and their work, women journalists are exposed to threatening and intimidating content which has detrimental impacts on not only their personal lives and safety but also their ability to carry out their important work.[8]

- **Digital tools and spaces:** The evolution of new digital technologies and information and communications technology (ICT) tools and services has given rise to different and more pervasive forms of online violence against journalists.[9] These technologies have enabled coordinated attacks at a previously unprecedented scale and with anonymity that creates challenges for securing accountability for perpetrators. It is anticipated that these will continue to enable more attacks against journalists in the coming years.[10]

- **Various forms of harm**: Gendered online violence against women journalists is frequently perpetrated through and linked with other online harms. For example, orchestrated disinformation campaigns,[11] and being targeted with deepfakes to create false narratives and artificially generated or edited images to shame and undermine their credibility. Doxxing and cyber-stalking dealt with in greater detail in Module 2 in this series, are also common tools to attack journalists and inhibit reporting.

- **Prevalence**: Although violence against journalists, particularly women, is a widespread and serious issue, even existing estimates of prevalence are likely significantly undercounted. UNESCO reports that journalists, specifically women journalists, often do not lodge complaints or reports with law enforcement agencies, and even fewer pursue legal remedies, signifying the "need for improvement in legal and judicial responses to online violence against women journalists."[12] In sub-Saharan Africa (SSA), various states have enacted legislative prohibitions against online violence impacting journalists. However, their adequacy to effectively deal with online violence has been called into question, with gendered violence posing a specific challenge.

---

[6] Id.
[7] UN Women, 'Online and ICT-facilitated violence against women and girls during COVID-19' (2020) (accessible here).
[8] UNHRC, 'Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective', 18 June 2018 (accessible here) (UNSR on VAW Online Violence Report).
[9] Id.
[10] Centre for International Governance, 'What Is Online Gender-Based Violence?' (2021) (accessible here).
[11] Id. See further, Centre for International Governance, 'Deepfakes and Digital Harms: Emerging Technologies and Gender-Based Violence', 27 November 2020 (accessible here).
[12] UNESCO, The Chilling, above n 4.

This module provides a high-level overview of this emerging trend and examines the international law framework as it relates to online violence against journalists, with a focus on the gendered impact on women journalists.

2. EMERGING TRENDS IN SUB-SAHARAN AFRICA

2.1. Sharp increases in online violence

UNESCO's 2020 global snapshot of online violence against women journalists found that of the women surveyed—

- 73% had experienced online violence in the course of their work;
- 25% had received threats of physical violence;
- 18% had been threatened with sexual violence; and
- 20% reported being attacked offline in connection with online violence they had experienced.[13]

General trends include:

- The significant increase in incidents of violence against women journalists comes in the wake of **increasing online activity** due to the COVID-19 pandemic as well as the consequences of the global rise of disinformation and the pervasive toxicity of digital platforms.[14]

- "Platform capture" — the **weaponisation of social media** by malicious actors, exacerbated by structural failures of the platforms' business models and design, and the increasing dependence of news organisations and journalists on these platforms.[15]

- Women journalists who cover **political issues** are increasingly likely to face attacks and threats online.[16] When compounded with entrenched misogyny, discrimination, and hate speech, which have seeped into the online world, women journalists face ongoing threats to their safety.

These global trends are prevalent in Sub-Saharan Africa, with online harassment and violence being a source of significant fear for women journalists in the region.[17] For example:

- A study of five countries in **sub-Saharan Africa** found that "organized trolling has been on the rise, especially against women with public-facing careers such as journalists, media personalities, activists and politicians."[18] Similar findings were documented in a

[13] UNESCO 'Online violence against women journalists: a global snapshot of incidence and impacts', 2020 (accessible here). The research involved over 700 women participants from 125 countries.
[14] UNESCO, The Chilling, above n 4.
[15] Id.
[16] UNESCO, 'Violence against journalists, the integrity of elections, and the role of public leadership: draft concept note' (2023) (accessible here).
[17] Fojo Media Institute and Africa Women in Media (AWiM), Barriers to Women Journalists, (2020) (accessible here).
[18] APC, 'Alternate realities, alternate internets: African feminist research for a feminist internet,' (2020) (accessible here) at 26.

report on eight countries in Southern Africa where women journalists, alongside politicians, are most commonly and severely targeted for online abuse.[19]

- In 2018, the Association of Media Women of **Kenya** (AMWIK) found that numerous Kenyan female journalists have been targeted by online smear campaigns that utilise hashtags, edited photos, and videos featuring nude imagery.[20] More recently, in 2022, women journalists from Kenya revealed how "one day, you could be an ordinary journalist going about your reporting duties with zeal and dedication; the next day, the internet is flooded with your private pictures and videos and abusive comments from anonymous people who don't have a clue of who you are."[21]

- iWatch **Ghana** likewise reports that in the second quarter of 2020, a female journalist in Ghana faced an average of 61 incidents of abuse in the reporting period, compared to a male journalist at 28, noting hateful comments related to appearance, gender, and sexuality.[22]

- In **Zimbabwe**, there has been a rise of "blatant sexist and misogynistic" online attacks against women journalists.[23]

- In **Tanzania**, the Executive Secretary of the Media Council has noted with concern, how the targeted and unjustified attacks of women journalists online have a "debilitating effect on journalism".[24] Women journalists in Tanzania explain that they are targeted because of their gender often facing appearance-focused criticisms and objectifications.[25]

- Recent research on online gender-based violence in **Uganda** revealed that women journalists endured multiple forms of online harassment and violence due to their work, with those reporting on political issues more likely to be targeted for online vitriol and abuse.[26]

- **South Africa** is no different, with pervasive and persistent efforts to silence, threaten, and harass women journalists online.[27]

---

[19] Meta & Centre for Human Rights, 'Understanding gender-based violence in Southern Africa,' (2021) (accessible here).
[20] AMWIK, 'Online safety for women journalists: An update of the Survey on Women Journalists in Kenya' (2018) (accessible here).
[21] Walusala, 'Online Violence Against Women: In whose hands are journalists safe?' Centre for International Media Assistance (2022) (accessible here).
[22] iWatch Africa, 'Q2 Report: Manasseh Azure, Nana Aba Anamoah & Justice Annan among most abused journalist online, Tracking digital rights in Ghana' (2020) (accessible here).
[23] South African National Editors Forum (SANEF), 'SANEF calls on Zimbabwe to stop online abuse of female journalists and to release journalist Hopewell Chin'ono' (2021) (accessible here). See also, Mokwetsi, 'How to create a safe space for women journalists in Zimbabwe' (2021) (accessible here).
[24] Tech & Media Convergency (TMC), 'A Comprehensive Analysis: Uncovering Journalistic Perspectives on Online Gender-based Violence (OGBV): Tanzania Context' (2023) (accessible here) at viii.
[25] Id at 35.
[26] Walulya & Selns, '"I thought You Are Beautiful": Uganda Women Journalists' Tales of Mob Violence on Social Media' Digital Journalism (2023) (accessible here).
[27] Daniels & Skinner, 'Cybermisogyny signals sexism in the media and newsroom' Daily Maverick (2023) (accessible here).

- In **Namibia**, recent research confirms, that while underreported, online gender-based violence targeting female journalists is an emerging phenomenon that cuts across gender, racial, ethnic, and professional identities.[28]

It is evident from the above that violence against women journalists forms part of a broader trend of misogyny and violence against women across the continent. That said, it is highly likely, due to underreporting and the deprioritising of online harms that the rate and impact of online violence against women journalists is far worse and remains a growing concern.[29]

2.2. State's failures to enable media freedom

Perhaps most concerningly, the UNESCO research found that not only are states struggling to respond effectively to the proliferation of online harms, but such conduct is also frequently sponsored, supported, or amplified by high-level political leaders and state-related actors.[30] 37% of respondents noted that political actors were the source of the attacks they faced — the second most frequently cited source.[31] The trend of politicians orchestrating or at least tacitly encouraging attacks was similarly identified by the UNSR on VAW in her 2020 report on combatting violence against women journalists."[32]

Zimbabwe's political targeting of women journalists

In recent years, Zimbabwe has been the site of government-aligned as well as political attacks against women journalists. In 2020, the South African National Editors Forum (SANEF) condemned the actions of the Press Secretary in the Office of the President of Zimbabwe and the Permanent Secretary in the Ministry of Information of Zimbabwe for their "vicious online and social media trolling of women journalists and media workers in Zimbabwe".[33] In 2021, criticised the ruling party, ZANU-PF's, Director of Information and Publicity for using social media to intimidate and harass a female journalist.[34]

While states have a negative obligation under international human rights law to refrain from actions that infringe on human rights, including the right to freedom of expression and the press, they also have a positive obligation to protect rights, which means taking steps to create and promote an enabling environment in which journalists can effectively play their essential role in democracy.[35] This means passing appropriate laws, providing protection for journalists where necessary, preventing attacks, and properly investigating and prosecuting them when they do occur.

---

[28] Zviyita & Mare, 'Same threats, different platforms? Female journalists' experiences of online gender-based violence in selected newsrooms in Namibia' Journalism (2023) (accessible here).
[29] CIPESA & UNESCO, 'The State of Media Freedom and Safety of Journalists in Africa' (2022) (accessible here) at 25. See also Journalism Initiative on Gender Based Violence (JiG), 'Reporting Challenges' (2021) (accessible here).
[30] UNESCO, The Chilling, above n 4 at 11.
[31] Id at 14.
[32] UNHRC 'Combating violence against women journalists: Report of the Special Rapporteur on violence against women, its causes and consequences', (2020) (UNSR on VAW: Combating violence against women journalists Report) (accessible here).
[33] SANEF above n 23.
[34] Id.
[35] Centre for Law and Democracy & International Media Support, 'Freedom of Expression as a Human Right' (2015) (accessible here).

For example, the 2023 Joint Declaration on Media Freedom and Democracy (**Joint Declaration**), issued by multiple key mandate holders in international fora,[36] confirms that the scope of this obligation includes a **positive obligation** to create an enabling environment for media freedom, which includes:

- adopting comprehensive measures for the safety of journalists and media workers to protect them from violence, online and physical attacks, threats and harassment, or illegitimate surveillance, while integrating gender and intersectionality perspectives; and

- taking measures to protect journalists and media outlets from strategic lawsuits against public participation (SLAPPs) and the misuse of criminal law and the judicial system to attack and silence them, including by adopting laws and policies that prevent and/or mitigate such cases and provide support to victims.[37]

Encompassing the **negative obligation** the Joint Declaration recommends that states should:

- refrain from unduly interfering with the right to freedom of expression. In particular, states should "ensure that any restrictions on the right to freedom of expression comply with international human rights standards";[38] and

- ensure that "legal frameworks should not be abused to illegitimately obstruct the work of independent media".[39]

The African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa similarly provides that "the right to express oneself through the media by practising journalism shall not be subject to undue legal restrictions."[40] In order to promote this right, states must take measures to prevent attacks on journalists and other media practitioners, including acts of intimidation or threats undertaken by State and non-State actors.[41]

Case note: An enabling environment without fear, intimidation, or harassment

In *Maughan v Zuma and Others* (2023), a South African High Court found that efforts by former President Zuma to silence female journalist Karyn Maughan by trying to have her criminally charged was tantamount to a SLAPP suit. In its reasoning, the Court reiterated that states have an obligation to ensure an enabling environment to ensure conditions in which expressive rights and vigorous public debate can thrive. This requires an environment

[36] UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information in Africa.
[37] Joint Declaration on Media Freedom and Democracy (2023) (accessible here).
[38] Id.
[39] Id.
[40] African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa,' (2019) at principle 19(1).
[41] Id at principle 20(2).

in which the media are able to exercise the right to freedom of expression and report freely on matters of public interest without threats and without fear, intimidation, and harassment.[42]

Challenges to the fulfilment of the state's obligations include:

- **Lack of recognition**: There are challenges in getting lawmakers and law enforcement officials to recognise the severity and import of online harassment.[43] There appears to be a lack of understanding of the severity of the consequences of online harms, as well as its close relationship with offline violence. This creates a widespread sense of impunity is created which contributes to a vicious cycle of continued violence against women journalists.

- **Challenges in conflict zones**: Journalists in active conflict zones or areas experiencing crises face physical challenges and threats. In recent years, this has been exacerbated by the use of new digital tools to threaten and silence journalists, with particular risks for women journalists. In times of crisis, there is often greater sensitivity to honest and potentially critical reporting and frequent misuse of the 'national security' justification for opacity. Conflict zones place journalists, especially women journalists at risk of military attacks, police intimidation, surveillance, and GBV.[44]

3. INTERNATIONAL LAW AND STANDARDS

3.1. Rights to freedom of expression and media freedom

The right to freedom of expression and media freedom are firmly grounded in international human rights law:

- The right to freedom of opinion and expression is 'gender neutral' and is enshrined under Article 19 of the UDHR and Article 19 of the International Covenant on Civil and Political Rights (ICCPR).[45]

- The right to freedom of expression applies to all journalists – *of all genders* –and encompasses the right to work free from the threat of violence.[46]

- Reporting freely and safely is necessary for media freedom – a free, uncensored, and unhindered press is cornerstones of a democratic society."[47]

[42] Id at para 1133.
[43] Media Defence, 'Cyber Rights and Wrongs: Safeguarding Human Rights Online in Kenya,' (2023) (accessible here).
[44] International Federation of Journalists, 'Women reporting conflicts: Changing the narrative, staying safe,' (2023) (accessible here).
[45] ICCPR, (1966) (accessible here). Universal Declaration of Human Rights (accessible here).
[46] UNESCO 'UN Action Plan on the Safety of Journalists' (accessible here); and UNESCO, 'Freedom of expression: A fundamental human right underpinning all civil liberties', (accessible here).
[47] UNHRC, 'General comment No. 34 on Article 19: Freedoms of opinion and expression' (2011) (accessible here).

- In 2014, UNHRC affirmed that "the same rights that people have offline must also be protected online, in particular freedom of expression."[48]

Threats against journalists undermine freedom of expression and media freedom:

- **Restrictive in nature**: Both threats of violence and actual violence, whether perpetrated online or offline against journalists, arbitrarily restrict their ability to exercise their right to freedom of expression, and "pose a very significant threat to independent and investigative journalism… and to the free flow of information to the public."[49]

- **Self-censorship**: Threats of violence against journalists and their families, as a result of their journalistic activities, 'often deters journalists from continuing their work or encourages self-censorship, consequently depriving society of important information.'[50] Notably, some journalists opt to either deactivate their social media accounts completely or resort to using pseudonyms to continue exercising their freedom of speech and expression online.

- **Physical threats**: In worst-case scenarios, online threats of violence spill over into physical spaces, leading to physical violence or the murder of journalists. This escalation was demonstrated by the 2017 murder of Daphne Caruana Galizia, a Maltese journalist.[51]

- **Democratic deficit**: In addition to threats to safety, gender equality and media freedom,[52] the various forms of online violence amount to a "direct attack on women's visibility and their full participation in public life", and "not only violates a woman's right to live free from violence and to participate online but also undermines the exercise of democracy and good governance, and as such creates a democratic deficit".[53]

As an indicator of the gravity of threats of violence against journalists, the UNGA has, on more than one occasion, unequivocally condemned all violence against journalists and media workers, highlighted the need to prevent violence against journalists, ensure accountability through investigations into alleged threats of violence, and provide legal remedies to victims of threats, including by ensuring that perpetrators of violence are brought to justice.[54]

Combating the spread of threats of violence – on- and offline – is critical given its disproportionate impact on journalists' right to freedom of expression and the consequent impact on media freedom and democratic values.[55] Given that these rights are founded in international human rights law, there is a strong basis from which to formulate responses to the manifestations of online violence faced by journalists of all genders and with various intersecting identities.

---

[48] UNHRC, 'The promotion, protection and enjoyment of human rights on the Internet' (2014) (accessible here).
[49] IFEX, 'Report on key issues and challenges facing freedom of expression' (2020) (accessible here).
[50] UNGA, 'The safety of journalists and the issue of impunity' (2019) (accessible here).
[51] UNESCO, 'Threats to freedom of press: Violence, disinformation & censorship' (2022) (accessible here).
[52] UNSR on FreeEx Report above n 1 at para 36.
[53] UNSR on VAW: Combating violence against women journalists Report above n 32 at para 33.
[54] UNGA, 'The safety of journalists and the issue of impunity' (2019) (accessible here); and UNGA, 'The safety of journalists and the issue of impunity' (2014) (accessible here).
[55] UNHRC, 'The promotion, protection and enjoyment of human rights on the Internet' above n 48.

3.2. Multilayered rights implications

In addition to the impact on expressive rights and democratic values, online violence against women journalists has multilayered rights implications, impacting among others:

- **Free from violence**: The CEDAW Committee has reaffirmed the interlinkage of women's right to a life free from gender-based violence as "indivisible from and interdependent on other human rights, including the rights to… freedom of expression."[56] This applies to technology-mediated environments, such as the Internet and digital spaces.[57] The CEDAW Committee, which oversees States' compliance with the Convention, defines GBV against women as "violence that is directed against a woman because she is a woman or that affects women disproportionately. It includes acts that inflict physical, mental, or sexual harm or suffering, threats of such acts, coercion and other deprivations of liberty."[58] Online threats of violence against women journalists are captured in this definition, as they amount to harmful practices and crimes against journalists' which constitute forms of gender-based violence against women.[59]

- **Equality**: The gendered nature of online attacks against women journalists – because they are women – impacts their rights to equality and non-discrimination. The gendered consequences and harm inflicted by various forms of online violence are rooted in structural inequality, discrimination, and patriarchal norms.[60] Multiple international human rights law instruments provide for the right to equality and non-discrimination, including the UDHR, (Article 2), the Convention on the Elimination of All Forms of Discrimination against Women, the International Covenant on Economic, Social and Cultural Rights (article 20, International Covenant on Civil and Political Rights (Article 2).

- **Privacy**: Article 12 of the UDHR, and Article 17 of the ICCPR provide for the right to privacy. Numerous forms of online violence infringe the privacy rights of women journalists. For instance, the dissemination of intimate photographs or doctored images online without consent amounts to a privacy violation. Doxxing, the malicious publication of private information like contact details, breaches privacy rights and exposes women journalists to harassment. Online stalking unwanted messages and surveillance tactics further, encroach upon their privacy rights.[61]

3.3. Regional Standards

At the regional level, various and intersecting rights are protected:

[56] Id at 95.
[57] CEDAW, 'General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19 (1992)' (2019) (accessible here).
[58] Id.
[59] Id.
[60] UNSR on VAW Online Violence Report above n 8.
[61] Id.

- The rights to freedom of expression of the press are protected and promoted for all African peoples', irrespective of sex, under article 9 of the African Charter on Human and Peoples' Rights (**African Charter**).

- The Africa Charter further provides for the rights to non-discrimination (article 2), equality (article 3), dignity (article 5), and the obligation to ensure the elimination of discrimination against women (article 18(3)).

- The **Maputo Protocol**, signed by 44 African states, provides strong protections against gender-based discrimination, harassment, and violence.

Case note: Egyptian Initiative for Personal Rights v Egypt

The case of *Egyptian Initiative for Personal Rights v Egypt* (2011) brought before the African Commission on Human and People's Rights (**ACHPR**) illustrates the interplay of the rights to freedom of expression and discrimination and inequality.[62]

The case centred around electoral reform protests in 2005 during which journalists who were protesting and those reporting on the demonstration were assaulted by riot police. In their complaint to the ACHPR, the complaints argued that the main reasons they were assaulted were because they "hold particular political views, are women and journalists".[63] In finding violations of the rights to non-discrimination, equality, and freedom of expression, among others, the ACHPR found the "violations were designed to silence women who were participating in the demonstration and deter their activism in the political affairs".[64]

The case has been welcomed as an important decision that recognises gender discrimination and gender-based violence in the content of expression and media freedom.[65]

There is also a body of non-binding commentary on threats of violence and the impact on journalists' right to freedom of expression and press freedom. For example:

- The ACHPR issued Resolution 185 on the **Safety of Journalists and Media Practitioners in Africa** in 2020. It clearly identifies the correlation between the "enjoyment of freedom of expression, press freedom, and access to information" and "freedom from intimidation, pressure and coercion" for media practitioners and journalists.

- The ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa (**African Declaration**) has also affirmed that the "exercise of the rights to freedom of expression and access to information shall be protected from

[62] *Egyptian Initiative for Personal Rights and Interights v Egypt* 323/06 (2011) (accessible here).
[63] Id at para 77.
[64] Id at para 166.
[65] See LSE Centre for Women, Peace and Security, 'EIPR and Interights v. Egypt' (accessible here) and Global Freedom of Expression, 'Egyptian Initiative for Personal Rights v. Egypt' (accessible here) for the case summary and analysis.

interference both online and offline…" Principle 20 deals at length with the safety of journalists and other media practitioners, including by stating that states must take measures to ensure the safety of female journalists and media practitioners by addressing gender-specific safety concerns, including sexual and gender-based violence, intimidation and harassment.

- In 2022, the ACHPR passed an important **Resolution on the Protection of Women Against Digital Violence in Africa**. The Resolution calls on states to review or adopt legislation companies of digital violence and expands the definition of gender-based violence to include digital violence against women. In relation to journalists, the Resolution calls on states to:

    - Undertake measures to safeguard women journalists from digital violence, including gender-sensitive media literacy and digital security training; and

    - Repeal vague and overly wide laws on surveillance as they contribute to the existing vulnerability of female journalists.[66]

The African Declaration on Internet Rights and Freedoms (**ADIRF**), a Pan-African civil society initiative, has emphasised the need to safeguard journalists from attacks, asserting that assaults on individuals involved in journalistic activities infringe upon the right to freedom of expression, and advocates for the establishment of protective guidelines for those who gather and share information, including journalists, women's rights activists, and human rights defenders, to ensure their safety.

Other regions have also developed significant guidelines, resolutions, and standards for the protection of journalism that can serve as guidance for future progress in SSA:

- In **Europe**, the Council of Europe's Committee of Ministers has noted that threats of violence against journalists serve as indicators of broader threats to freedom of expression, signalling a deterioration in human rights, democracy, and the rule of law.[67] Emphasising the need for effective interim protection measures for those facing such threats, the Committee underscores that ensuring the right to freedom of expression without fear necessitates guaranteeing safety, security, and practical protection, particularly for journalists and media professionals. It also noted that threats of violence frequently target female journalists, highlighting the need for "gender-specific responses" to these gendered threats of violence.

- the General Assembly of the **Organisation of American States** adopted resolution 2908 (XLVII-O/17) on the right to freedom of thought and expression and the safety of journalists and media workers in 2017 which stressed that "journalism must be practised free from threats, physical or psychological aggression, or other acts of intimidation."[68]

[66] Id at paras 8 and 9.
[67] Council of Europe 'Recommendation CM/Rec(2016) 4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors', 13 April 2016 (accessible here).
[68] OAS, 'Promotion and Protection of Human Rights' (accessible here).

- Concerns of threats of violence against journalists have also been raised before **courts** across the globe.[69]

4. THREATS OF VIOLENCE

- **Definition**: A 'threat of violence' is defined as an expression or a declaration of an "intention to inflict emotional, physical or psychological harm, injury, pain or damage' to another person, through virtual or physical means."[70] Women journalists bear a disproportionate burden of these threats and attacks, especially those occurring online.[71]

- **Rights implications**: As in the offline context, threats of online violence against journalists under international law are not tolerated given their ability to infringe on human rights, particularly the rights to freedom of expression and press freedom. In 2015, the OSCE Representative on Freedom of the Media issued recommendations on countering online abuse of female journalists and recognised that 'threats and other forms of online abuse of female journalists and media actors is a direct attack on freedom of expression and freedom of the media.'[72]

- **Platforms and sites**: Notably, threats of violence against journalists are typically issued or transmitted through major social media platforms, such as Twitter and Facebook, or through messaging applications or other platforms or technologies, including WhatsApp and Telegram. Additionally, threats directed towards journalists are also frequently posted in the comment sections provided by media houses or news outlets on their official websites or official social media pages.[73]

- **States obligations**: As mentioned above, international human rights law places obligations on States to create conditions for effective investigation, prosecution, and protection in response to threats of violence against journalists. Further, international human rights law defines the responsibilities of private sector actors, including businesses and corporations, such as private social media companies and intermediaries, where threats of online violence against journalists are typically transmitted.

States and Platforms

The UN Guiding Principles on Business and Human Rights (UNGPs), a widely accepted non-binding global standard defining the responsibilities of businesses to protect and advance human rights, calls on private sector actors to fulfil their positive responsibilities to

[69] For more case law regarding threats of violence affecting journalists in jurisdictions including Australia, Finland, France, Singapore, amongst others, see: The Law Library of Congress, 'Laws protecting journalists from online harassment,' September 2019 (accessible here). For other online harassment cases, see: Pen America, 'Online Harassment Case Studies' (accessible here).
[70] Collins Dictionary, 'threat of violence,' (accessible here) and Reverso Dictionary (accessible here).
[71] United Nations 'International Day to End Impunity for Crimes against Journalists' (accessible here).
[72] Organization for Security and Cooperation in Europe, 'Recommendations following the Expert Meeting New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists', (accessible here).
[73] See UNESCO, The Chilling above n 4.

mitigate human rights impacts of their operations, publish transparency reports and provide remedies for potential human rights violations.[74] More recently, and with a focus on women journalists, the UNSR on FreeEx noted the dual responsibility of states and the private sector:

> "The ultimate responsibility rests with States, as the primary duty bearers of human rights, to ensure that women journalists are safe from online violence. As the main vectors of online attacks, social media companies are also responsible for exercising due diligence and taking measures to ensure the safety of journalists on their platforms in accordance with the Guiding Principles on Business and Human Rights."[75]

In the SSA region, observed threats of online violence include threats of sexual or physical violence, including rape or death threats, and threats of digital security attacks (e.g., hacking or trolling), amongst others. For example:

- SANEF and partners observed that "online threats targeting journalists such as hate speech, harassment, and doxing" were received from the police, political parties, and the public in **South Africa**.[76] Concerningly, these threats of violence targeting journalists also extend towards their family members, leading to wider concerns about online and physical safety and security.

- iWatch Africa reports that journalists who report on contested social and political issues in **Ghana** are subjected to online violence including threats of physical violence and rape.[77]

Finally, it should be noted that there is a fine line, in reality, between a threat and actual violence in the online sphere, but that the legal requirements for proving such actions are likely to differ. For example, a threat of violence accompanied by the release of personal information, doxxing, can be seen as both an act of actual violence through the tangible and real-world harm that results from doxxing, as well as a threat for further violence to be perpetrated through the release of the information (e.g. a threat to show up at one's house).

5. TYPES OF VIOLENCE

While the manifestations of online violence against women journalists vary widely, some commonly accepted types have developed over time that assist in understanding the breadth of experiences faced by women journalists as well as how regulation and enforcement can better address these harms. These types are discussed in more detail in **Module 2 of this**

[74] UN Guiding Principles on Business and Human Rights (accessible here).
[75] UNSR on FreeEx above n 1 at para 39.
[76] Amnesty International South Africa, Campaign for Free Expression, Committee to Protect Journalists, Media Monitoring Africa, and the South African National Editors' Forum, 'Submission for the 41st Session of the Universal Periodic Review Working Group' (2022) (accessible here).
[77] iWatch Africa, 'Q2 Report: Manasseh Azure, Nana Aba Anamoah & Justice Annan among most abused journalist online, Tracking digital rights in Ghana' (2020) (accessible here).

series on Digital security attacks and Online Gender-Based Violence (OGBV). In summary, these include, but are not limited to:

- Cyber-harassment;
- Doxxing;
- Stalking;
- Non-consensual dissemination of intimate images;
- Online sexual exploitation and abuse;
- Dis- and misinformation campaigns;
- Privacy and data protection violations;
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Government surveillance;
- Commercial surveillance;
- Phishing; and
- Confiscation of hardware.

It should be noted that, in contrast to offline gender-based violence, OGBV is characterised by continuity due to the ability of perpetrators to utilise different online and offline platforms to transmit harmful speech or behaviour for extended periods, leading to the "constant re-victimisation of victims."[78] This issue of re-victimisation is further entrenched by the reality that any form of targeted online violence creates a "permanent digital record that can be distributed worldwide and cannot be easily deleted."[79]

6. IMPACT OF ONLINE VIOLENCE ON THE WORK OF JOURNALISTS

6.1. Psychological harm

According to the UNESCO report, at least 26% of the women journalists interviewed had suffered impairment to their mental health as a result of online violence.[80] Out of these, only 12% had sought medical help. In Africa, psychological harm is one of the most devastating effects of online violence against journalists. UNESCO also emphasised that these experiences are not limited to the short-term, often causing long-lasting physical and psychological stress. A study conducted by ARTICLE 19 and AMWIK in **Kenya** also documented the psychological harm experienced by journalists who were victims of online violence.[81]

6.2. Spill-over of online violence to offline spaces

There is a close relationship between online and offline violence, with online threats or abuse frequently being followed up with offline violence and vice versa. For example:

[78] World Wide Web Foundation, 'Covid-19 and increasing domestic violence against women: The pandemic of online gender-based violence', July 2020 (accessible here).
[79] UNSR on VAW Online Violence Report above n 8.
[80] UNESCO, The Chilling, above n 4 at 13.
[81] ARTICLE 19 & AMWIK, 'Women Journalists Digital Security', February 2018 (accessible here).

- **Doxxing** is often committed with the express intent of enabling offline harassment of the targeted person.
- **Online stalking** is frequently accompanied by other, offline methods of stalking.
- **NCII** and other forms of harassment are designed to generate violations of dignity and undermine one's credibility and professional standing in the real world.
- In 2017, the Committee to Protect Journalists stated that at least 40% of the journalists who were murdered had received **death threats**, including online threats prior to their death.[82]
- In **Ghana**, journalists from the Multimedia Group received direct threats of physical harm via social media for their work around the 2020 elections.[83]
- In 2017, an online message calling for the killing of certain identified journalists was circulated across social media platforms in **Togo** accompanied by the dissemination of personal data, ostensibly to support the government regime.[84]

Case note: Litigating violence against journalists in Africa

In *South African National Editors Forum v. Black First Land First* (2017) the High Court of South Africa granted several orders relating to the protection of journalists from harassment. The case related to attacks that had been made both on- and offline against journalists who had reported negatively on an organisation, Black First Land First (BLF).

The Court held that the journalists had a right to the protection of their physical and human dignity and to carry out their profession, and that in making threats and sending abuse to the journalists online, gathering in front of their homes, and turning off the water supply to the house, the members of BLF had intended to harass, intimidate, and threaten the journalists and violated their right to the protection of their bodily and physical integrity, to dignity, and to follow the profession of their choice.

Importantly, the Court also ordered the Respondents not to use social media in an intimidating and threatening way.

6.3. Loss of credibility

Online harassment and abuse of journalists and media houses can have severe effects on their credibility, casting doubt on their independence and impartiality to their audience and leading to a general climate of loss of trust in the media, with devastating effects on democracy and the free flow of information. For example:

- In **Nigeria**, journalist Ruona Meyer was attacked by online trolls for publishing an exposé on the abuse of codeine and those profiting from the trade.[85] Due to her marriage to a

[82] Elisabeth Witchel, 'Getting away with Murder: CPJs 2017 Global Impunity Index spotlights countries where journalists are slain and the killers go free', 31 October 2017 (accessible here).
[83] Media Foundation for West Africa, 'Journalists receive threats via social media in the aftermath of early December general election', 2020 (accessible here).
[84] Reporters Without Borders, 'Online Harassment of Journalists; Attack of the Trolls' (accessible here).
[85] BBC, 'Africa Eye: How a codeine investigation changed Nigeria', 6 June 2019 (accessible here).

German national and association with the BBC, she was tagged as a foreign agent and her work was a result of foreign interference.[86]

- In **Kenya**, the Nation Media Group was in 2019 harassed by online trolls and dubbed *#NationMediaGarbage*, a tag designed to attack the credibility of the organisation.[87] Likewise in Kenya, the term 'Githeri Media' is used to rubbish the work of journalists and media houses and to imply state or political influence on news.[88] Further, research[89] has demonstrated that the Kenyan Government actively used misinformation and coordinated inauthentic campaigns on social media to discredit the 'Pandora Papers.'[90]

- UNESCO's research on the widespread attacks faced by **Filipino-American journalist**, Maria Ressa, co-winner of the 2021 Nobel Peace Prize for her work to safeguard freedom of expression, revealed that 60% of the attacks were designed to undermine her professional credibility and public trust in her journalism.[91]

The above examples illustrate how perpetrators frequently abuse the public's recognition of widespread mis- and disinformation to invoke false claims of a journalist's work being "fake news." Orchestrated attacks by armies of trolls or supporters are also often used to create substantial dents in the perceived credibility of a journalist.

6.4. Culture of violence

Failure by different stakeholders to address online violence leads to a culture of impunity in which perpetrators of online violence escape without consequences, with limited response from platforms, the state, and media houses, leading to ongoing and repeated cycles of violence that, over time, can develop into an accepted culture of violence against women and/or journalists.

Of the journalist killings documented between September 2013 and August 2023, in 78% (204 cases) no one had been held accountable, according to an analysis by the Committee to Protect Journalists.[92] Securing accountability for online attacks is also challenging due to a range of factors:

- The difficulties in holding private digital platforms, which do not have a physical presence in most African countries and determine their own content moderation standards separate and distinct from domestic laws, accountable for removing content in languages and contexts in which they have little expertise;
- The lack of awareness among law enforcement of the severity and impacts of online abuse against women journalists;

[86] UNESCO, The Chilling, above n 4.
[87] Reporters Without Borders, '2020 RSF Index: Future of African Journalism under threat from all sides' (accessible here).
[88] Twitter, Larry Madowo (accessible here).
[89] Madung & Obilo, 'How to manipulate Twitter and Influence People: Propaganda and the Pandora Papers in Kenya', 3 November 2021, (accessed here).
[90] The largest investigation in journalism history exposes a shadow of financial system that benefits the world's most powerful and rich. See: ICIJ, 'Pandora Papers' (accessible here).
[91] UNESCO, The Chilling, above n 4 at 48.
[92] VOA, 'Impunity in Journalist Killings Remains the Norm, Report Says,' (2023) (accessible here).

- A dearth of appropriate legislation and regulations dealing specifically with online violence against journalists, particularly women;
- Challenges in identifying and tracking down perpetrators who often operate anonymously online; and
- Unsupportive state apparatuses that are often complicit in enabling attacks against journalists and actively seeking to undermine freedom of expression and of the press for various reasons.

In addition, and because of the above, there is a need for media houses and employers of women journalists to play a more active role in supporting and protecting journalists from these attacks. Concerningly, in a global survey released by the International Federation of Journalists, two-thirds of the respondents stated that online harassment was not a priority for their media company while 44% stated that the issue was not even discussed.[93]

One **Kenyan** journalist states:

> "We are harassed in the online space by perpetrators who get away without any consequences. There are no adequate measures to protect us against such harassment: Our media organisations do not know how to act when we are facing these attacks online, and our legal protections, which look very promising on paper, are not implemented. The big question then is, in whose hands are journalists safe?"[94]

Perpetrators of online violence associated with the state contribute to this culture of violence as it creates the impression that such conduct is permissible. In **Rwanda**, people with access to the President's Twitter account were linked to harassment and trolling against journalist Sonia Rolley.[95]

Case note: Accountability for failure to investigate – *Hydara v Gambia*

In the foundational case of *Hydara v Gambia* (2014) in the ECOWAS Court, the Court held that the state's failure to effectively investigate the assassination of a prominent Gambian journalist allowed impunity and violated the right to freedom of expression, as well as failing to provide redress to his family. In its judgment, the Court emphasised the obligations of the state to protect media practitioners, including those critical of the state, and to enable a safe and conducive atmosphere for the practice of journalism to avoid the chilling effect that systematic impunity had on journalism and the right to freedom of expression.

6.5. Self-Censorship

[93] International Federation of Journalists, 'Time to end Media inaction over online abuse, says IFJ' (2022) (accessible here).
[94] Lourdes Walusala, 'Online Violence against women: In whose hands are journalists safe?' (2022) (accessible here).
[95] Reporters Without Borders, 'Online Harassment of Journalists; Attack of the Trolls' (accessible here).

Online violence against journalists causes self-censorship as a protective mechanism, with journalists seeking to avoid reporting on topics that appear sensitive and that could lead to online violence, or ultimately to withdraw from journalism entirely. For example:

- In **Kenya**, ARTICLE 19 found that online violence has caused female journalists to withdraw from the use of the internet and stop working for some time.[96]

- In **Namibia** the occurrence of online gender-based violence against female journalists in Namibia has led some to resort to self-censorship out of fear of retaliation.[97]

The **impact** of self-censorship and withdrawal is profound:

- Withdrawing and self-censorship implicate freedom of expression and press freedom but also exacerbate the pre-existing inequalities regarding participation levels between men and women journalists as professional counterparts.

- Further, the withdrawal of large numbers of women journalists from online spaces as well as from the industry as a whole creates serious concerns for representation and diversity of perspectives within the media, with potentially serious economic, social, and political consequences.

- As stated by UN Women, limiting the participation of women online "is a significant concern given the majority of the estimated 2.9 billion people who remain unconnected to the Internet are women and girls."[98]

7. RELEVANCE TO PRESS FREEDOM AND FREEDOM OF EXPRESSION

In addition to the individual-level effects detailed above, which constitute serious infringements of the right to freedom of expression of individual journalists.

- **Media freedom**: UNESCO's research shows that journalists are attacked more frequently when their journalistic activities focus on the themes of gender, politics, elections, human rights, and social policy.[99]

- **Access to information**: Online violence is likely to have the most detrimental chilling effect on serious reporting that informs citizens and the public about important social, economic, and political issues. The consequences are, therefore, not limited to individual journalists or even the profession as a whole but extend to the ability of the public to be informed about critical public issues.

- **Political actors**: It is also notable that politicians and political party officials or associated persons are some of the key instigators and amplifiers of online violence

[96] ARTICLE19 & AMWIK, 'Women Journalists Digital Security', February 2016 (accessible here).
[97] Zviyita & Mare above n 28.
[98] UN Women, 'FAQs: Trolling, stalking, doxing and other forms of violence against women in the digital age,' (accessible here).
[99] UNESCO, The Chilling, above n 4 at 13.

against women journalists.[100] Attacks against journalists are frequently used as a political tool, with levels of violence increasing around election times and other periods of political contestation.

- **Impact on democracy**: Online violence has significant implications for the free flow of information in democratic systems and during elections. In 2021, Pollicy noted that during **Uganda's** 2021 general election, online violence was used to harass women in politics and to reinforce existing patterns of power and dominance against women, limiting their civic participation. The report also states that whereas both men and women in politics used online tools for engagement, "greater online activity was linked with higher levels of online violence for women as opposed to men."[101]

Case note: Litigating violence against journalists: state obligations to prevent violence

In *Dávila v. National Electoral Council* (2023), the Constitutional Court of Columbia issued a ruling in a case brought by a group of women journalists seeking to vindicate their constitutional rights against the National Electoral Council of Colombia, arguing that they had suffered misogynistic and sexist online violence on Twitter that had sought to censor them and demean their profession and that the Council had failed to adopt measures to prevent or sanction sexist violence perpetuated or tolerated by members and affiliates of political parties in their social networks.

The Court held that "there is an evident pattern of online violence against women journalists as a result of their reporting on the activities of political figures in the public interest" and ordered a series of transformative measures to prevent, investigate, and punish such behaviour. These measures called for included, amongst others, the implementation of ethical guidelines by political parties to sanction online violence and the enacting of legislation targeting sexist digital violence.

8. INTERSECTIONAL TARGETING OF MARGINALISED JOURNALISTS

- **Intersectionality**: The individuals most affected by gender-based violence and inequality are often those who are already marginalized and disadvantaged: black and brown women, indigenous women, women residing in rural areas, young girls, girls with disabilities, as well as transgender and gender non-conforming youth.[102] The UNSR on VAW reiterates that this intersectional discrimination arises due to the combination of, and interplay between, multiple characteristics and identities noting that those from marginalized groups are especially vulnerable targets of online violence.[103]

[100] Id at 17.
[101] Pollicy, 'Amplified Abuse; Report on Online Violence against women in the 2021 Uganda General election', (2021) (accessible here).
[102] UN Women, 'From where I stand: "Just the act of wearing our traditional clothes is an expression of resistance' (2019) (accessible here).
[103] UNSR on VAW Online Violence Report above n 8.

- **Journalists**: Journalists experience also intersectional discrimination and gender-based targeting based on several defining characteristics. These include, but are not limited to, "race, ethnicity, caste, culture, religion, sexual orientation, gender identity and expression, abilities, age, geographic location (urban/rural setting), social, economic and legal status, class, income, minority affiliation, amongst others."[104]

- **Africa**: African culture has been criticised for promoting heteronormativity which entrenches homophobia and discrimination of sexual minorities.[105] It is common for same-sex relations to be considered 'un-African,' and many countries continue to criminalise homosexuality. This propagates a culture of violence against members of the LGBTQI+ community that extends into the online world. Even in countries where decriminalisation has been achieved, substantial barriers remain to ensuring equal treatment and participation for LGBTQI+ individuals and groups:

    - In **South Africa**, for example, despite a progressive constitution providing for equality and non-discrimination, heteronormative culture continues to perpetuate homophobic violence.[106]
    - In **Angola**, despite the decriminalisation of same-sex conduct, sexual minorities are still subjected to online violence.[107]

- **Gender identity and sexual orientation**: Identity and sexuality are common vectors along which attacks against journalists are directed and can exacerbate violence against women with intersecting identities. UNESCO's research has likewise found that "women journalists who are also disadvantaged by racism, homophobia, religious bigotry, and other forms of discrimination face additional exposure to online attacks, with worse impacts."[108] In particular, many attacks are deeply racialised and leverage structural racism to amplify the effect on the target.

Enhancing the safety of all women journalists using an intersectional gender approach

In 2022, ARTICLE 19 released three guidelines for the enhancement of safety for all women journalists relying on an intersectional gender approach. These include:

1. **Guideline 1:** Monitoring and documenting attacks against journalists and social communicators;
2. **Guideline 2:** Advocating on emblematic cases for change; and
3. **Guideline 3:** Organising protection training.

These guidelines offer novel insights for actors, using a gendered intersectional approach, to understand how other intersectional characteristics "influence, and thus

[104] UNSR on VAW: Combating violence against women journalists Report above n 32.
[105] Mkhize & others, 'Unpacking pervasive heteronormativity in sub-Saharan Africa: Opportunities to embrace multiplicity of sexualities,' *Progress in Human Geography* 47(3) (2023) (accessible here).
[106] Reygan & Lynette, 'Heteronormativity, homophobia and 'culture' arguments in KwaZulu-Natal, South Africa' (2014) (accessible here).
[107] Meta & Centre for Human Rights above n 19.
[108] UNESCO above n 3 at 16.

exacerbate, violations of journalists' and social communicators' right to freedom of expression."[109]

9. CONCLUSION

In addition to having severe effects on freedom of expression and of the press, online violence against women journalists impacts a wide range of human rights that are protected and promoted in international human rights law. Online violence, irrespective of the form or manifestation, is a targeted attack on journalists' rights and freedoms, with the intention of intimidating, silencing, and stigmatising journalists. It systematically targets women and those with intersecting identities including race, gender identity, and sexual orientation and is resulting in the systematic suppression of women's voices from online spaces and from the media, leading to serious concerns for representation, equality, and democratic participation. More action is needed by a range of actors, including the platforms, states, regional bodies, and media houses, to protect women journalists in online spaces and to counter the growing tide of online abuse that poses a serious risk to the advancement of the right to freedom of expression in the digital era.

[109] ARTICLE 19 'Guide 1: An intersectional gender guide to monitoring and documenting attacks against journalists and social communicators', April 2022 (accessible here).

Module 2

DIGITAL ATTACKS AND ONLINE GENDER-BASED VIOLENCE

Modules on Online Violence against Journalists in Sub-Saharan Africa

MEDIA DEFENCE

Published by Media Defence: www.mediadefence.org
This module was prepared with the assistance of Catherine Muya, Sigi Waigumo Mwanzia, and ALT Advisory: https://altadvisory.africa/

Published in 2024

TABLE OF CONTENTS

MODULE 2

DIGITAL ATTACKS AND ONLINE GENDER-BASED VIOLENCE (OGBV)

- **Digital attacks against journalists occur in a wide range of formats that are constantly evolving as new technologies develop.**

- **This module provides an analysis of cyber-harassment, non-consensual dissemination of intimate images, dis-and misinformation, privacy violations, DoS and DDoS attacks, government and commercial surveillance, phishing, and the confiscation of hardware as examples of the attacks commonly faced by women journalists.**

- **Despite theoretically strong protections in international human rights law, many countries have not yet legislated these harms effectively. Nevertheless, an analysis of alternative legal remedies in existing legislation across the continent indicates some promising options for defenders of women journalists online.**

- **In addition, this is a field that is rapidly developing, and there is scope to influence the development of appropriate laws to provide protection against online abuse, harassment, surveillance, etc.**

1. INTRODUCTION

Across the continent, attacks against journalists continue to rise[1] as both state and non-state (corporations and individual) actors seek, either directly or indirectly, to muzzle their reporting and infringe on their rights to freedom of expression, and other intersecting rights. In the internet age, it is perhaps unsurprising that many of these attacks are perpetrated through digital tools and platforms and target journalists on social media and other platforms on which they work and interact. Digital attacks can take many different forms, but as discussed in **Module 1** in this series, all have the potential to seriously impact freedom of expression online, including freedom of the press, particularly when targeted at journalists.

Online gender-based violence (OGBV), an increasingly common manifestation of digital attacks forms part of the continuum of GBV in society.[2] Many of the gender-based harms that occur offline frequently occur online. Similarly, the harms that occur online often enable those

[1] See, for example, Amnesty International, 'East and Southern Africa: Attacks on journalists on the rise as authorities seek to suppress press freedom,' (2023) (accessible here) and VOA, 'Attacks, Harassment Threaten Media Across Africa,' (2023) (accessible here).
[2] Nwaodike & Naidoo, 'Fighting Violence Against Women Online: A Comparative Analysis of Legal Frameworks In Ethiopia, Kenya, Senegal, South Africa, and Uganda' (2020) (accessible here).

that occur offline. OGBV is like any other form of GBV – it violates the rights and freedoms of victims and survivors' rights,[3] and can have severe and enduring consequences."[4]

- **Definition**: The United Nations Special Rapporteur on Violence against Women (UNSR on VAW), explains OGBV as "any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately".[5] Women journalists are at a heightened risk of OBGV by virtue of their gender and profession, and those with further intersecting identities facing additional risks.

- **Targets**: Women journalists bear the brunt of digital attacks and OGBV, often including visceral and deeply gendered threats of violence relating to both their professional and private lives and often extending to other members of their families, including children.[6] As a result, the United Nations Special Rapporteur on Freedom of Expression (UNSR on FreeEx) has stressed the need to take a gender-sensitive approach when considering measures to address the issue of violence against journalists and media workers, including in the online sphere.[7]

- **Rights implicated**: Traditionally, human rights mechanisms have examined the impact of these threats by relying on international standards on the rights to freedom of expression, press freedom, and privacy. In recent times, this has been extended to other mutually reinforcing international standards on the rights of assembly and association, freedom from discrimination, and civil and political rights relating to participation online and offline, amongst others.

This module examines several forms of digital attacks against journalists, including:

- Cyber-harassment;
- Non-consensual dissemination of intimate images (NCII);
- Dis- and misinformation;
- Privacy and data protection violations, including doxxing and cyber-stalking;
- Denial of service (DoS) and distributed denial of service (DDoS) attacks;
- Silencing the online expression of victims and survivors;
- Government surveillance;
- Commercial surveillance;
- Phishing; and
- The confiscation of hardware.

---

[3] The terms "victim" and "survivor" may be used interchangeably and refer to those who have experienced GBV and/or OGBV. These terms have different connotations and implications and do not intend to, by any means, impose a definition or response on any persons who have experienced some of the severe violations to their dignity and safety.

[4] Power Law 'Deconstruct: Online Gender-Based Violence Toolkit' (2021) (accessible here).

[5] UNHRC, 'Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective' (2018) (accessible here) (UNSR on VAW Report on online violence).

[6] CIPESA 'Annual Report', (2020) (accessible here) and UNESCO 'The Chilling: Global trends in online violence against women journalists' (2021) (accessible here).

[7] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (2012) (accessible here).

2. CYBER-HARASSMENT

2.1. Overview

- **Cyber-harassment**: Cyber-harassment, also referred to as online harassment or online abuse, refers to a situation in which an individual or group is severely or pervasively targeted through harmful online behaviour that may be for either a short or extended duration, may be perpetrated by either an individual or coordinated by a group of people, and which is aimed at causing severe emotional distress or emotional harm.[8]

- **Forms**: Cyber-harassment can occur in a variety of forms that specifically target women,[9] and might be considered an umbrella term for a range of other digital attacks, such as:[10]

    - **Cyberbullying**, which is common among children and young adults and typically involves sending digital messages that are aimed at causing embarrassment or humiliation.[11]

    - **Non-consensual dissemination of intimate images (NCII)**,[12] which refers to the sharing or publication of images of a subject, whether obtained with or without consent, with the aim of causing them harm.[13] This will be discussed in further detail below.

    - **Online sexual harassment**, which refers to exposing a subject to unwanted direct or indirect, verbal, or non-verbal content of a sexual nature, such as the unsolicited sending and or receiving of sexually explicit material that violates the dignity of a person and creates a hostile or humiliating environment.[14]

    - **Abusive comments**, including, for example, abusing and/or shaming a woman for expressing views that are not normative, for disagreeing with people (often men), or for refusing sexual advances.

    - **Incitement** of others to physical violence, including advocating for femicide and incitement to commit suicide.

    - **Hate speech**, whether through social media posts or digital mail, which is targeted at one's actual or presumed protected characteristics, such as gender, sexuality, or race, including the use of sexist or gendered name-calling.

    - **Online sexual exploitation** which refers to the use of digital technologies to

[8] Media Defence, 'Factsheet: Gender and Online Harassment' (2021) (accessible here).
[9] For conciseness, we refer hereafter to "women" to include all those who identify as women and those with marginalised or at-risk identities including members of the LGBTQI+ community, except where specific instruments or documents referenced refer explicitly to "women" or some other grouping.
[10] Internet Governance Forum, 'Best Practice Forum (BPF) on Online Gender-Based Violence against Women' (2015) (accessible here).
[11] Stop Bullying, 'What Is Cyberbullying,' (accessible here).
[12] Media Defence, 'Module 7: Cybercrime', (2020) (accessible here).
[13] UNSR on VAW Report on online violence above n 5.
[14] Id.

exploit or abuse a position of power over a victim for sexual purposes. It occurs in many forms including online grooming, live streaming of sexual abuse, child sexual abuse material (CSAM), online sex trafficking, online sexual coercion, and image-based sexual abuse. While these types of violations are not new, digital technologies have provided a platform through which perpetrators can reach wider audiences and derive illicit financial gain. This form of violence disproportionately affects women and children.

Cyber-harassment of journalists

A UNESCO report on the Safety of Journalists Covering Protests noted that "while experiencing the same kinds of physical violence as their male counterparts, women media workers are also more highly exposed to the threats of sexual violence and rape.[15] During the protests in Egypt in 2011, for example, and in addition to physical attacks, there were notable instances of female journalists being "attacked by prominent male media figures on either social media or broadcast media, resulting in widespread online violence campaigns."[16]

In addition to the above, a range of other **terms** have developed to describe the complex and varied ways in which harassment can take place and the tactics that are used on digital platforms. For example:

- **Astroturfing**: creating the false impression that coordinated activity is a widespread, spontaneous grassroots movement when it is actually controlled by a concealed group or organisation.[17]
- **Concern trolling:** offering undermining criticisms under the guise of concern with the aim of sabotaging the issue being discussed and causing dissent within a community.[18]
- **Cyber-mob attacks**: a large group gathering online to try to collectively shame, harass, threaten, or discredit a target[19]
- **Deep fakes**: images convincingly altered or manipulated to misrepresent something having been done or said.[20]
- **Hashtag poisoning**: creating abusive hashtags or hijacking existing hashtags that are used to rally cyber mob attacks.[21]
- **Cyberstalking**: the utilisation of technology to surveil or track an individual's online and

[15] UNESCO, 'Safety of journalists covering protests: preserving freedom of the press during times of turmoil (2020) (accessible here).
[16] Megan Brown et al, 'Gender-based online violence spikes after prominent media attacks' (2022) (accessible here).
[17] Merriam-Webster Dictionary, 'astroturfing,' (accessible here).
[18] Distionary.com, 'concern troll' (accessible here).
[19] PEN America, 'Defining online harassment: A glossary of terms', accessible here).
[20] Merriam-Webster Dictionary, 'deep fake,' (accessible here).
[21] Pen America, 'Defining "Online Abuse" A glossary of terms' (accessible here).

offline activities, which may include monitoring locations, activities, and content (this can involve real-time tracking or historical monitoring of an individual's behaviour).[22]

- **Controlling devices**, which involves accessing, using, or manipulating an individual's electronic devices without their consent, whether in their presence or remotely, for instance, advancements in technology enable individuals to remotely control or manipulate the activation and deactivation of devices, adjust temperatures, and lock or unlock spaces.[23]

Multiple forms of harm

The multifaceted scope of cyber-harassment is illustrated by the wave of online attacks against members of Ethiopia's LGBTQI+ community in 2023 who were faced with increased online harassment and threats of physical violence with posts being shared on Tik Tok. Various posts called for, among other things, "homosexual and transgender people to be whipped, stabbed and killed."[24] LGBTQI+ activists raised concern that TikTok users were also "outing Ethiopians by sharing their names, photographs and online profiles", with some of the outing videos stating: "Let's kill them, give us their address."[25] Harassment, outing, doxxing, and threats and incitement to violence are often interwoven placing marginalised or at-risk communities of attacks both on and offline.

2.2. International law and standards

As discussed in Module 1, online violence against women journalists – including cyber-harassment implicates multiple cross-cutting rights protected in international law, including the rights of freedom of expression, equality and non-discrimination, and freedom from violence, among others. These rights of women journalists are bolstered by a range of international human rights instruments, including:

- The Universal Declaration of Human Rights (**UDHR**);
- The International Covenant on Civil and Political Rights (**ICCPR**);
- The International Covenant on Economic, Social and Cultural Rights (**ICESCR**);
- The International Convention on the Elimination of All Forms of Racial Discrimination (**CERD**);
- The Convention on the Elimination of All Forms of Discrimination against Women (**CEDAW**);
- The Convention against Torture and Other Cruel, Inhuman or Degrading Treatment (**CAT**); and
- The Convention on the Rights of Persons with Disabilities (**CRPD**).

The Council of Europe's Istanbul Convention on Preventing and Combatting Violence against Women and Domestic Violence, although not directly relevant to Africa, provides a

[22] Deconstruct: Online Gender-Based Violence Toolkit above n 4.
[23] Id.
[24] Anna, 'LGBTQ+ people in Ethiopia blame attacks on their community on inciteful and lingering TikTok videos' (2023) (accessible here).
[25] Id.

comprehensive definition of the types of violence against women, including online and ICT-facilitated violence, and sets out useful guidance for states.[26]

Notably, however, Council of Europe Convention No. 185, known as the **Budapest Convention**, arguably the most influential global standard on cybercrime and one to which nine African countries have signed up,[27] does not explicitly address ICT-induced violence against women (while it does address the sexual exploitation of children online).

As with all human rights, women's rights in this regard apply in full measure in online spaces,[28] arenas in which gender-based violence is not only perpetuated but also exacerbated in new and challenging forms. Several rights are implicated in the various forms of cyber-harassment detailed above, such as the right not to be subject to discrimination, to privacy, to dignity, and freedom of expression.

2.3. National laws

Research into 48 African countries found:

- 75% (36) of the countries have no cyber-harassment law;
- 19% (9) of the countries have a cyber-harassment law but it does not address sexual harassment; and
- Only 6% (3) have a cyber-harassment law that does address sexual harassment.[29]

Regulation of these harms can be difficult due to several factors:

- First, cyber-harassment is often **difficult to control** online and can replicate and morph rapidly. This is further complicated by the fact that it **often involves multiple offenders** in **different jurisdictions** over platforms that provide anonymity to users.[30]

- Second, regulating cyber-harassment necessarily **involves some form of limitation of the speech** of perpetrator(s), and such limitations must meet the three-part test under international law.

- Third, the wide variety of forms of cyber-harassment can be **difficult to define** and its manifestation in online spaces **can change rapidly** as new technologies and uses develop over time, which makes defining offences difficult.

- Finally, **enforcement** of laws is challenging, often requiring extensive sensitisation of law enforcement officers and the judiciary as to the seriousness and impact of these crimes.

---

[26] World Bank, 'Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws,' (2023) (accessible here).
[27] Council of Europe, 'The Budapest Convention (ETS No. 185) and its Protocols,' (accessible here).
[28] CEDAW, 'General recommendation No. 35 on gender-based violence against women,' (2017) (accessible here).
[29] World Bank above n 26.
[30] Equality Now, 'Ending Online sexual exploitation and abuse of women and girls: A call for International standards, Executive Summary and Key findings', November 2021 (accessible here).

Legislating cyber-harassment

Despite these challenges, various provisions seeking to criminalise the many forms of cyber-harassment have been passed into law in Africa in recent years. For example:

- **South Africa's** Cybercrimes Act, 2019, criminalises cyber-bullying, defined as the sending of electronic messages or social media posts to a person that incite or threaten that person with violence or damage to their property (sections 14 and 15), and cyber-extortion, defined as committing various offences for the purpose of obtaining an advantage from another person or compelling the person to perform or abstain from an act (section 10). South Africa's Electronic Communications and Transactions Act, 2002, also provides for several offences relating to using electronic communications to harass or defame another person. This is in addition to provisions in the Protection from Harassment Act, 2011, that refer explicitly to both offline and online harassment.

- Also of note is **Nigeria's** Cybercrimes Act, 2015, which provides a comprehensive definition of cyber-harassment and spells out specific offences such as 'cyberstalking' provision under Article 24 which provides that 'any person who knowingly or intentionally sends a message or other matter by means of computer systems or network… to bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm or to another person' will attract imprisonment for a term of 10 years and/or a minimum fine of N25,000,000.00 (USD59,406.5).[31]

3. NON-CONSENSUAL DISSEMINATION OF INTIMATE IMAGES (NCII)

3.1. Overview

- **Image-based abuse:** Non-consensual dissemination of intimate images (NCII) is considered one form of the broader category of image-based sexual abuse, which is, in turn, a form of technology-facilitated gender-based violence (TFGBV) or OGBV. Other forms of image-based abuse include "voyeurism/creepshots, sexploitation, sextortion, the documentation or broadcasting of sexual violence, and non-consensually created synthetic sexual media, including sexual deepfakes."[32]

- **NCII:** NCII "occurs when a person's sexual images are shared with a wider than intended audience without the subject's consent."[33] It is irrelevant whether the person gave initial consent for the creation of the images or consent for them to be shared with other individuals; any dissemination beyond the initially intended audience can be said to constitute NCII. Intimate images can be in the form of either photos or videos and typically depict "nudity, partial nudity or sexually explicit acts."[34] While NCII can and does

[31] Cybercrimes (Prohibition and Prevention) Act, 2015 (accessible here).
[32] Suzie Dunn 'Technology-Facilitated Gender-Based Violence: An Overview' (accessible here) at 8.
[33] Suzie Dunn and Alessia Petricone-Westwood, 'More than 'revenge porn': Civil remedies for the non-consensual distribution of intimate images,' (2018) (accessible here).
[34] CIGI 'Non-Consensual Intimate Image Distribution: The Legal Landscape in Kenya, Chile and South Africa,' 2021 accessible here)..

affect people of all genders, research indicates that 90% of those victimised are women,[35] although LGBTQ+ persons and those with disabilities have also fallen victim.[36]

- **Technology enabled**: Technological and cultural shifts, epitomised by ubiquitous phones with cameras and a vast digital audience, increase the ease of causing harm and exacerbate the consequences. Motivations behind such actions span a spectrum: from clandestine actors aiming to disrupt individuals' lives to vengeful ex-partners; from seeking entertainment or validation among peers to profit-driven endeavours; and from cyberbullying tactics aimed at humiliation or control to various other motivations.[37]

- **Evolving terminology**: It is notable that NCII has come to replace the outdated term "revenge porn:

    - **"Revenge" is misplaced**: Revenge typically involves harming someone in response to perceived wrongdoing. Labelling it as "revenge" implies that the victim or survivor initiated harm deserving retribution. Additionally, perpetrators are not always motivated by revenge, they may be acting out of spit, or out of a desire for profit, notoriety, or entertainment.

    - **"Pornography" is misplaced**: Using the term pornography implies victims or survivors are seemingly consenting porn actors. It further "turns a harmful act into a form of entertainment".

Intermediaries and NCII

Given that NCII are often shared on platforms and websites considerations around the role of intermediaries come into play, more specifically, intermediary liability which refers to the practice of holding internet intermediaries liable for content published on their platform.

In sub-Saharan Africa, several countries have enacted laws around intermediary liability including **Ghana**,[38] **Uganda**,[39] and **Kenya**.[40] In **South Africa**, for example, Chapter 11 of the Electronic Communications Act, 2005 requires members of the Internet Service Providers Association to take down content upon receiving take-down requests.

Concerns have emerged, however, about the use of take-down procedures to entrench censorship and disproportionate power being given to private companies to moderate free speech.[41] As online violence often occurs on social media platforms such as Facebook, X, or Instagram, it is important to understand the role of the platforms in protecting users from such harms. While platforms are not required to regulate speech on the platform, they are responsible for taking measures to keep their users safe, especially because they provide terms and conditions of use that do not allow content that violates users' trust or safety.

[35] Cyber Rights Organisation, 'NCII: 90% of victims of the distribution of non-consensual intimate imagery are women,' (accessible here).
[36] CIGI, above n 34.
[37] Id.
[38] Section 92 of Ghana's Electronic Transactions Act of 2008 (accessible here).
[39] Section 29 of Uganda's Electronic Transactions Act of 2011 (accessible here).
[40] The Copyright Act, CAP 130, Section 35B (accessible here).
[41] Godana Galma, 'Digital Rights Implication of the Copyright (Amendment) Act 2019', (2020) (accessible here).

Litigation in India serves as a useful illustration of intermediary accountably in the context of NCII. In *Mrs X v Union of India* (2023), the Delhi High Court required intermediaries to remove *all* NCII of Mrs X (a victim of NCII) not just the links Mrs X had provided. The Court analysed the involvement of intermediaries in removing NCII, noting that while the "originators" who initially publish the content bear responsibility for uploading it, intermediaries are involved in its dissemination and continued presence online. The Court held that Indian legislation mandates intermediaries to exert "reasonable effort" to prevent users from sharing unauthorised or obscene content and that intermediaries must make use of technology to remove reposts of offending images.[42]

3.2. International law and standards

As with online harms in general several human rights are implicated when it comes to NCII:

- **Freedom of expression**: NCII can and has been used as a tactic to shame and harass women journalists around the world and thereby discourage critical reporting or shut down freedom of expression. Even where it is not shared to shame or stigmatise victims into silence and self-censorship intentionally, individuals can and do use nudity, depictions of sex, or eroticism as a "private demonstration of sexuality" or to "express their artistic, journalistic and academic freedoms,"[43] and non-consensual dissemination undermines and punishes this valid expression.

- **Privacy, dignity, and freedom from violence**: In 2018 and 2020, the UNSR on VAW observed that the "publication or posting online without the consent of intimate photographs or photoshopped images that are sexualised" violates the subject's rights to privacy, to dignity, and to live a life free from violence[44] and that this emerging form of online violence "defames and silences women journalists."[45] NCII also implicates sexual expression. According to the World Health Organisation (WHO), "sexual rights protect all people's rights to fulfil and express their sexuality and enjoy sexual health."[46]

As noted above, and in Module 1, these rights are protected in several instruments and guiding documents in international human rights law. Obligations arise for both states and the private sector:

- **States** are required to, among others, create conditions for the effective investigation, prosecution, and protection of attacks against journalists as part of the mandate for protecting and promoting freedom of expression.

- The United Nations Guiding Principles on Business and Human Rights (UNGPs) place positive responsibilities on **private sector actors**, including businesses and corporations, such as private social media companies and intermediaries through which

[42] See Global Expression, 'Mrs X v Union of India (2023) (accessible here) for more details.
[43] ARTICLE 19, 'Kenya: Withdraw proposed amendments to cybercrimes law' (2021) (accessible here).
[44] UNSR on VAW Report on online violence above n 5.
[45] UNHRC 'Combating violence against women journalists: Report of the Special Rapporteur on violence against women, its causes and consequences', (2020) (accessible here).
[46] WHO, 'Developing sexual health programmes: a framework for action,' (2010) (accessible here).

many of these abuses flow, to mitigate the human rights impacts of their operations, publish transparency reports, and provide remedies for potential human rights violations.[47]

At the **regional level**, while the African Union Convention on Cyber Security and Personal Data Protection (**Malabo Convention**), which came into effect in 2023, has been faulted for failing to specifically provide for the offence of NCII,'[48] its data protection provisions can also provide some measure of protection if properly implemented at the domestic level.

In addition, the African Commission on Human and Peoples' Rights (ACHPR) in the Declaration of Principles on Freedom of Expression and Access to Information in Africa affirms that NCII is a punishable offence emanating from the "harmful sharing of personal information."[49] Despite the Declaration being a soft law, this provides a persuasive indication of the linkage between the right to informational privacy and this particular manifestation of online violence affecting journalists.

3.3. National laws

Numerous states, including in Africa, have passed, or are attempting to pass domestic civil and criminal laws to provide legal solutions for NCII, either as a form of sexual abuse or harassment or as a privacy violation, albeit with varying degrees of success.

NCII: Legal protections in four sub-Saharan countries[50]

- **Kenya:** The Computer Misuse and Cybercrimes Act (CMCA), 2018 establishes various digital and technology-facilitated offences, including cyber-harassment in section 27 and the "wrongful distribution of obscene or intimate images" in section 37. However, the broad wording of the provision criminalises the sharing of all intimate images, a framing that could have the unintended effect of deterring victims from reporting cases of NCII. Since 2018, this legislation has been the subject of judicial contestation, including an order suspending the operation of sections 27 and 37 in 2018[51] which was subsequently overturned in 2020.[52] The matter is reportedly being appealed before the Court of Appeal.[53]

- **South Africa:** Various pieces of legislation are relevant to NCII. The Cybercrimes Act, 2020, in section 16, criminalises the unlawful and intentional disclosure of a data message of an intimate image of a person if the subject retains a reasonable expectation of privacy, the message violates the sexual integrity or dignity of the person or amounts to sexual exploitation, and without that person's consent, and

[47] UN Guiding Principles on Business and Human Rights (accessible here).
[48] CIGI, above n 34.
[49] Principle 42, Declaration of Principles on Freedom of Expression and Access to Information in Africa, (accessible here).
[50] Sarai Chisala-Tempelhoff & Monica Twesiime Kirya 'Gender, law and revenge porn in Sub-Saharan Africa: a review of Malawi and Uganda', (2016) (accessible here); CIGI, above n 34.
[51] CIPESA, 'Promoting Best Practice among Activists for More Effective Collaboration in Digital Rights Litigation in Kenya,' (2019) (accessible here).
[52] Digital Space Case Digest, ' Civic Space Protection Platform,' (accessible here).
[53] Id.

includes within its scope both real and simulated intimate images. In addition, the Film and Publications Amendment Act, 2019, creates the offence of knowingly distributing private sexual photographs and films without consent in any medium with the intent to cause the subject harm (section 24E). The Protection of Personal Information Act, 2013 (POPIA) may also provide some protection in the form of seeking relief for damages against a perpetrator for data protection violation. Lastly, the Protection from Harassment Act, 2011, enables victims and survivors to apply for protection orders and the common law crime of *crimen inuiria* can be used in cases involving the wilful impairment of a person's dignity and privacy. Commentators have also expressed concern about potential loopholes in the relevant legislation, particularly around intent to do harm and the definition of private images.[54]

- **Malawi:** In Malawi, although no specific legislation exists, a patchwork of laws may provide some limited protection for victims and survivors. For example, the Electronic Transactions and Cybersecurity Act, 2016 criminalises cyber-harassment (section 86), offensive communication (section 87), and cyber-stalking (section 88). However, the broadness of these provisions may also have negative consequences for freedom of expression online, and implementation of the law has proven challenging with many women facing difficulties in reporting these crimes to the police.[55] Notably, Section 30 also sets out the responsibilities of intermediary service providers to take down content that is unlawful or violates rights.[56] Section 137 of the Malawi Penal Code, 1930 also criminalises "insulting the modesty of a woman" and the Gender Equality Act, 2016 prohibits "harmful practices… on account of sex [or] gender" although these vague provisions may also have negative side-effects.[57]

Many of these laws raise challenges for ensuring accountability for victims and survivors:

- Laws dealing with NCII usually prioritise intent when determining whether a human rights violation or civil or criminal offence has occurred, which can be a steep evidentiary burden for victims and survivors.[58]
- Sometimes, perpetrators may act without aiming to hurt the subject.[59]
- Many do not address threats to release a certain image or video but only the actual release itself.[60]
- Developing appropriate legal responses to address NCII is further complicated by the fact that recent technological advancements have "opened the door to new forms of

[54] Schindlers, 'South Africa Cracks Down on Revenge Porn,' (2020) (accessible here).
[55] African Feminism, 'Accessing Justice for Image-Based Sexual Abuse A Challenge For Victims in Malawi,' (2020) (accessible here).
[56] Seonaid Stevenson-McCabe and Sarai Chasala-Tempelhoff, 'Image-Based Sexual Abuse: A Comparative Analysis of Criminal Law Approaches in Scotland and Malawi,' (2021) (accessible here).
[57] Id.
[58] Foreign Policy 'The World Hasn't Figured Out How to Stop 'Revenge Porn', (2021) (accessible here).
[59] CCRI (accessible here).
[60] UNHRC, 'Right to Privacy: Report of the Special Rapporteur on the right to privacy' (2019) at para 71 (accessible here).

abuse" which include the use of artificial intelligence to create images at scale and which creates challenges for tracing origin and removal.[61]

- Further, even where legal recourse can be achieved against the primary distributor, a long chain of others who redistribute, view, or engage with these images may be created which makes permanent removal and full accountability exponentially difficult.[62]

An alternative argument is that intimate images are protected under a moral right of copyright, which allows individuals to:

- claim authorship of a photo or video, and
- enforce the right to prohibit or authorise the distribution of a photo or image.

This argument draws on the **Berne Convention** for the Protection of Literary and Artistic Works and Article 27 of the UDHR, which protects "the moral and material interests resulting from any scientific, literary or artistic production of which he is the author."[63] However, in using such a copyright approach, which may be the only viable option for some social media platforms, victims or survivors have sometimes been required to prove that they hold copyright over the images prior to removal by intermediaries.[64]

Global approaches to NCII

Cases around the world have demonstrated the various approaches to seeking accountability for incidents of NCII. For example, in the case of *Holly Jacobs vs. Ryan Seay & Others* (2014) in the Circuit Court of the Eleventh Judicial Circuit in Florida, United States, a woman initiated a claim relying on the intentional infliction of emotional distress, which required demonstrating a lack of consent and the intention by the abuser to cause emotional distress.

In *Khadija Ismayilova v Azerbaijan* (2019) the European Court of Human Rights (ECtHR), it was held that Azerbaijan had violated the right to privacy and freedom of expression of a journalist in a matter involving the online dissemination of intimate videos recorded covertly in her bedroom. The Court held that the failure by the state to properly investigate the crimes constituted a failure in its positive obligations to protect her journalistic freedom of expression and her private life.

These cases illustrate that different legal routes are available in NCII claims and that different rights are implicated

Others have relied on a breach of confidentiality, a well-established legal concept, by demonstrating an express or implied breach of confidentiality. An implied breach would focus

[61] Suzie Dunn 'Identity Manipulation: Responding to Advances in Artificial Intelligence and Robotics', (2020) (accessible here); Suzie Dunn 'Technology-Facilitated Gender-Based Violence: An Overview', 2020 (accessible here).
[62] McGlynn, Clare and Erika Rackley, 'Image-Based Sexual Abuse', (2017).
[63] Article 27, Universal Declaration on Human Rights.
[64] Foreign Policy 'The World Hasn't Figured Out How to Stop 'Revenge Porn' (2021) (accessible here).

on whether trust has been breached, rather than the "private or offensive" nature of the distributed information.[65]

Case note: Litigating Non-Consensual Distribution of Images

In 2016, the High Court of **Kenya** determined a case, *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* (2016) involving the non-consensual distribution of the petitioner's nude photographs by an ex-boyfriend, resulting in her dethronement as Miss World Kenya 2015.

The Court held that Ebrahim had a legitimate expectation of privacy, that she did not waive her right to protection of privacy by taking nude photographs and did not consent to their dissemination to third parties, and as such, her right to privacy under Article 31 of the Constitution of Kenya had been violated. It further ordered the ex-boyfriend to pay damages and directed the organisers of the Miss World Kenya not to publish the nude photographs in their possession.

The case provides valuable insights into the 'reasonable expectation of privacy,' whether images are obtained in an intrusive manner, and whether the presence of illegalities may invalidate a right to privacy claim.[66]

Finally, in states where NCII is not criminalised, the options are limited to other crimes, such as stalking, harassment, unlawful surveillance, or the dissemination of child pornography.

4. DIS- AND MIS-INFORMATION

4.1. Overview

- **Threats to journalism**: the pervasive information disorders that have severely disrupted societies around the world in recent years, including mis- and disinformation, are "multi-pronged and intersecting threats" that impact journalists, their safety and security, and their ability to do their jobs in various ways.[67] Misinformation and disinformation are defined by UNESCO as follows:

Disinformation	Information that is false is disseminated by a person who knows it is false. "It is a deliberate, intentional lie, and points to people being actively disinformed by malicious actors."[68]
Misinformation	Misinformation is information that is false, but the person who is disseminating it believes that it is true.

[65] Woodrow Hartzog 'Reviving Implied Confidentiality' (2013) (accessible here).
[66] For further information on the use of the 'tort of invasion of privacy,' the public disclosure of embarrassing facts, breaches of the torts of breach of confidence and intentional infliction of mental distress, see: *Jane Doe 464533 v. D. (N.)* (accessible here); See also: Equality Project 'Technologically-Facilitated Violence: Non-Consensual Distribution of Intimate Images Case Law', January 2019 (accessible here).
[67] UNESCO 'The Chilling' above n 6.
[68] UNESCO 'Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training', 2018 (accessible here).

- **Mistrust in the media**: At a passive level, the proliferation of mis- and disinformation online has contributed to a growing sense of mistrust among the general public in journalism and news as a whole and has made it harder for credible information produced by journalists to compete in the heavily saturated information eco-system.[69]

- **Targets**: In addition, mis- and disinformation campaigns are actively used to target journalists in order to deter participation in the public sphere, silence their reporting, and punish criticism, with "serious consequences for human rights, diversity in public debates and the media, and ultimately, democracy and development."[70] The UNSR on FreeEx has observed that journalists are increasingly facing "smear campaigns [that] have become more pernicious on social media networks."[71]

The impact of mis- and disinformation is compounded by several factors:

- **Gender dynamics**: The UNSR on FreeEx highlighted the insidious nature of gendered disinformation, which not only spreads falsehoods but also utilizes highly emotive and context-specific content to undermine women's credibility, competence, and societal standing.[72] These campaigns often sexualize women journalists, attacking their character, appearance, and intelligence to discredit their reporting and deter their continued work. Targeted disinformation tactics are also used to silence, delegitimize, and devalue women in positions of power across politics, media, entertainment, and activism.

- **The legacy of colonialism**: In Africa, disinformation campaigns frequently employ anti-colonialism narratives to undermine women's rights activists and imply their opposition to decolonial efforts and ties to Western influences.[73] Sub-Saharan African women are disproportionately affected by online gender-based abuse fuelled by disinformation, with a UNESCO-ICFJ survey revealing that 41% of respondents, including women journalists, attributed their experiences of online violence to orchestrated disinformation campaigns. [74]In the region, online gendered disinformation tactics have been used particularly during critical national or public interest moments, including during elections and the COVID-19 pandemic. Such disinformation campaigns frequently weaponised gender narratives, sexualising them and attacking their character and credibility.[75]

- **Evolving digital landscape**: Concerningly, with the evolution of digital tools, artificial intelligence technologies have now become an ingrained feature of this form of online violence, with deep fakes surfacing as a preferred form of malicious misrepresentation. According to the International Centre for Journalists, "[t]he perpetrators range from individual misogynists and networked mobs [including anonymous trolls])... to State-

[69] Id.
[70] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on Disinformation and freedom of opinion and expression ' (2021) (accessible here) (UNSR FreeEx Report on Disinformation).
[71] Id.
[72] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on Gendered Disinformation' (2023) (accessible here) at para 46.
[73] Id.
[74] David Maas 'New research details ferocity of online violence against Maria Ressa', 8 March 2021 (accessible here).
[75] UNSR FreeEx Report on Disinformation above n 70.

linked disinformation agents aiming to undercut press freedom and chill critical journalism through orchestrated attacks."[76]

Gendered disinformation manifests in various ways and amplifies OGBV

In its submissions to the UNSR on FreeEx for her report on gendered disinformation, **South African** civil society organisation Media Monitoring Africa (MMA) referenced several local examples of how gendered disinformation manifests:[77]

- **Targeted attacks against female journalists**: Journalist Ferial Haffajee faced online dissemination of manipulated images, often portraying her in sexualized contexts, falsely insinuating connections with specific businessmen and government officials. Similarly, journalist Qaanitah Hunter was targeted on X (formerly Twitter) by politicians, accusing her of spreading lies and being financially supported by a "Master."

- **Legal attacks and disinformation campaigns**: Journalist Karyn Maughan encountered attempts to silence her through a SLAPP suit, which not only aimed to intimidate her legally but also served as a platform for online bullying and attacks against her. MMA explained that the weaponization of the legal system appears to be intertwined with disinformation campaigns, often with gendered implications.

- **Disinformation targeting the LGBTQI+ community**: MMA found that gendered disinformation intersects with the targeting of LGBTQI+ community members. For instance, a fabricated article purportedly authored by openly gay journalist Eusebius McKaiser was circulated containing homophobic content aimed at exploiting the journalist's profile to disseminate disinformation against the LGBTQI+ community.

MMA provided further examples of how disinformation can form part of or magnify different forms of OGBV for example:

- **Manipulated content**: Instances such as Haffajee's experience reflect a growing trend of technology-manipulated content, including images, text, videos, or audio, being disseminated without the consent of the depicted individual. MMA submitted that cyber-misogynistic attacks are strategically employed to silence journalists.

- **Threats and incitement**: MMA highlighted recent tweets targeting Maughan in which a former political spokesperson, noting that "we must keep on kicking this dog harder so that her owner who pays her comes out". These attacks were in response to her recent high-profile reporting on corruption in South Africa. This was intended to dehumanise and insult Maughan, but moreover, to incite physical violence.

[76] UNESCO, Online violence against women journalists: a global snapshot of incidence and impacts', 2020 (accessible here).
[77] MMA, 'submission to the Special Rapporteur on the Promotion and Protection of Freedom of Opinion and Expression regarding the gender dimensions of disinformation' (2023) (accessible here). For further submissions made see 'Inputs Received' (accessible here).

4.2. International law and standards

Gendered disinformation implicates various rights:[78]

- The misleading gender and sex-based narratives implicate the rights to **equality** and **dignity**.
- The intention to deter women from participating and engaging impacts **freedom of expression**.
- The intersectional nature of the spread of false and harmful sex and race-based narratives that undermine public trust impacts **equality**, **dignity**, **access to information**, and **media freedom**, among others.

Balancing rights

While tackling mis- and disinformation is clearly critical, regulations are also frequently abused to stifle freedom of expression. Thus, international law is clear that attempts to combat the spread of online dis- and misinformation must not violate the right to freedom of expression:

- General prohibitions of expression are not permitted under the ICCPR.[79]
- Any limits placed on online expression, including mis- and disinformation, must pass the three-part test for permissible restrictions to freedom of expression outlined in the ICCPR Article 19(3).

Any limitations on information that is false must be **carefully crafted** to "minimise chilling effects on potentially beneficial speech"[80] and must not be "weaponized to inhibit women's cultural, gender and sexual expression and academic freedom, or restrict feminist discourse and women's organisations."[81] As such, mandating that states legislate mis- and disinformation can be problematic.

Multi-pronged approaches to address this could include:[82]

- media and information literacy campaigns;
- holding digital platforms accountable for appropriate and contextualised content moderation; and
- providing digital security tools for women journalists, in particular, to report and take action on campaigns made against them.

For more on mis- and disinformation, see the dedicated Module 8: 'False News', Misinformation and Propaganda in the Media Defence Resource Hub.

[78] UNSR FreeEx Report on Disinformation above n 70.
[79] UNHRC, 'General comment No. 34 Article 19: Freedoms of opinion and expression' (2011) (accessible here).
[80] Id.
[81] Id.
[82] Id and UNSR FreeEx Report on Disinformation above n 70.

4.3. National laws

During the COVID-19 pandemic, the explosion of pandemic-related mis- and disinformation prompted many states, including those in Africa, to pass laws criminalising or otherwise regulating the publishing of mis- or disinformation online. As of December 2023:[83]

- 3 countries in sub-Saharan Africa had dedicated disinformation laws (**Ethiopia**, **Mauritania**, and **Nigeria**).
- 3 were considering drafts (**Gambia**, **Mozambique**, and **Senegal**).
- 84 general speech laws were in effect, which raises concerns regarding a lack of clarity, broad scope, a lack of independent decision-making over the determination of speech, and disproportionate responses.[84]

In **Nigeria**, the Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries, 2022 requires digital platforms to file an annual compliance report that details rates and take-downs of mis- and disinformation and must provide users with easily accessible tools to report such information. However, the Code has been criticised for threatening freedom of expression in several ways.[85]

Case note: Disinformation implications for free speech

In *Federation of African Journalists (FAJ) v. The Gambia* (2018) a foundational order given by the Economic Community of West African States Community Court of Justice (ECOWAS Court) in 2018, provisions in The Gambia's Criminal Code that provided for criminal sanctions for defamation and false news were held to have violated the right to freedom of expression under international law. The case was brought by the Federation of African Journalists and four Gambian journalists who had been prosecuted and detained under the provisions. The Court ordered The Gambia to amend the Criminal Code to bring it into conformity with the international law position on mis- and disinformation.

5. PRIVACY AND DATA PROTECTION VIOLATIONS

5.1. Overview

- **Different forms**: ICT-related violations of privacy exist in a wide range of different forms that are rapidly changing and evolving as new technologies develop and become widespread, and as both users of these tools and perpetrators find innovative new tools and loopholes to target the growing volume of personal information available online. Some examples include:
    - **Cyberstalking**, which includes repeated, intrusive, and persistent behaviour over digital channels such as messaging or calls or placing a subject under surveillance aimed at harassing or creating fear in the subject.

[83] Lexota, (accessible here).
[84] Lexota, 'Compare laws,' (accessible here).
[85] CWPDF, 'Critical Feedback: Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries,' (2022) (accessible here).

- **Sextortion**, in which a perpetrator blackmails a victim into either creating sexually explicit material like images or videos engaging in unwanted sexual acts for payment or using threats against the victim or their loved ones.[86] It therefore includes other forms of violence such as hacking accounts, intercepting communications and NCII.
- **Doxxing**, or the publication of personal data of an individual without their consent and with the intent to embarrass, humiliate or expose a victim to harassment.[87]
- **Hacking**, which includes the unauthorised access of a person's device, network, or account for nefarious purposes, for example obtaining personal data.
- **Impersonation**, creating a fake account using the person's name, image, or both in order to post false, misleading, inciteful, maligning or inflammatory content.[88]

- **Targets**: Privacy violations such as the examples above are frequently used as tactics to target and attack women journalists, frequently in combination with other digital attacks. It is clear that there is significant overlap between privacy violations and other forms of digital attacks, especially the various forms of cyber-harassment which often involve a component of intruding into one's personal space or collecting personal information without consent.

Cyberstalking: How can journalists be targeted?

Cyberstalking can manifest itself in many forms. A few examples of ways in which journalists can be targeted include:

- The use of emails or messages to send sexist, suggestive, or threatening content to the victim;
- The repetitive and excessive tagging of the victim on their own or unrelated posts;
- Unwavering participation in the target's online activities, through liking, commenting, retweeting, or sharing their online content;
- The creation of fake posts, e.g., with sexually explicit videos or photos of themselves, to embarrass and shame the victim.

The hacking into or hijacking of the target's online accounts, laptop, or smartphone camera to track or record the victim's movements and activity.[89]

Spyware: The threat of Pegasus and Predator

In recent years, Spyware has emerged as a significant concern, enabling covert access to information on target computer systems or devices. Predator and Pegasus are prominent spyware programs capable of clandestinely infiltrating mobile phones and other devices

[86] UNSR on VAW Report on online violence above n 5.
[87] Amnesty International, 'What is online violence and abuse against women?', 20 November 2017 (accessible here).
[88] Pen America above n 21.
[89] Sheri Gordon, 'What Is Cyberstalking?', 16 August 2021 (accessible here)

running Android and iOS, exploiting the latest mobile operating systems. Journalists, politicians, government officials, chief executives, and directors are often targeted.

Notable Incidents:

- In 2019, Amnesty International documented network injection attacks in Morocco, infecting human rights defenders and journalists with NSO Group's Pegasus spyware.
- In 2021, Egyptian exiled politician Ayman Nour and an anonymous news program host were hacked with Predator spyware developed by Cytrox.
- In 2023, the Predator Files global investigation revealed the widespread use of surveillance technologies and government failures in regulation.
- The Citizen Lab reported a similar system targeting a political opposition figure in Egypt with Intellexa's Predator spyware in September 2023.
- As of 2024, 11 nations, including Angola, Armenia, Botswana, Egypt, Indonesia, Kazakhstan, Mongolia, Oman, the Philippines, Saudi Arabia, and Trinidad and Tobago, are suspected Predator customers.

Protective measures:

Amnesty International has developed some practical guidance for individuals who may be at risk of these digital attacks:

- Keep your web browser and mobile operating system software updated to mitigate security vulnerabilities.
- Enable the enhanced security "Lockdown Mode" on Apple devices to increase resistance against compromise.
- Use a reputable VPN provider to enhance privacy and prevent surveillance from ISPs or governments.
- Utilise features like Signal's "Relay Call" mode to obscure metadata and reduce exposure to network attacks.
- Employ disappearing messages and regular device restarts to minimize exposure to spyware infections.
- Seek expert assistance if you receive warnings of state-sponsored attacks to assess ongoing risks for your accounts or devices.
- If you are concerned about an attack or have been attacked, reach out to Amnesty's Security Lab at securitylab.amnesty.org for assistance.

5.2. International law and standards

The **rights to privacy** and **gender equality** are interlinked, with digital security attacks targeting women journalists being incidences of **gender-based violence** and **discrimination.**[90] International law also protects against both **unlawful and arbitrary interference** and interceptions of telephonic, telegraphic, and other forms of communication,

[90] UNHRC 'Report of the Special Rapporteur on the right to privacy', (2020) at para 19(e) (accessible here).

such as the interception of personal communication are prohibited.[91]

Doxxing is an example of a privacy violation that also has various rights:

- **Privacy**: Frequently used to abuse, intimidate, and silence, women journalists. In instances in which a perpetrator retrieves and discloses personal information and data to the public with "malicious intent," is a "clear violation of the right to privacy."[92] Privacy is protected by Article 17 of the ICCPR and is found in regional instruments such as the Malabo Convention[93] which, under Chapter II, protects personal data and calls on States Parties to "punish any violation of privacy."[94]

- **Freedom of expression**: PEN America notes that doxxing, through the use of "harassment, intimidation, extortion, stalking or identity theft,"[95] is used to silence and shame journalists and malign their reputation and character, leading to its identification as a "global threat to journalists."[96]

- **Media freedom**: Further, doxxing can be used as a tactic by perpetrators to lift the veil of digital anonymity for journalists working in critical environments or using pseudonyms to protect their online identity, which is central to media freedom. Concerningly, doxxing also increases the threat for "at-risk confidential sources"[97] and can place the families of journalists in a vulnerable situation, making them inadvertent targets as well.[98]

- **Data protection:** Under international law, illegally obtaining and releasing journalists' private information, or confidential information that is not in the public domain, amounts to an infringement of their right to privacy, including the right to informational privacy (also known as data protection).

5.3. National laws

Several countries within the SSA region have passed data protection legislation in recent years that seeks to provide redress for victims of privacy violations in the online and offline realms, in addition to the more generalised anti-harassment laws discussed above.

The state of privacy and data protection in Africa

Dataprotection.africa is an online platform that maps the state of data protection legislation in all 55 AU-recognised countries. It highlights that 35 countries currently have laws in place, while a further three and considering draft bills.

[91] UNHRC, 'CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (accessible here).
[92] UNSR on VAW Report on online violence above n 5.
[93] Media Defence, 'Module 4: Data Privacy and Data Protection', (2020) (accessible here).
[94] Id.
[95] Pen America above n 21.
[96] Kathrine Huntington, 'Journalism in the Age of Doxxing', 2020 (accessible here).
[97] UNESCO 'The Chilling' above n 6.
[98] Pen America 'Protecting from Doxing' (accessible here).

Most recently, **Nigeria** signed the Data Protection Act into law in 2023[99] and **Tanzania's** Personal Data Protection Act came into effect in May 2023.[100]

Some countries also have relevant provisions in their Cybercrimes legislation. For example, section 17 of **Kenya's** Computer Misuse and Cybercrimes Act, 2018 criminalises the "unauthorised interception" of data to or from a computer system over a telecommunication system.[101]

Concerningly, many SSA countries do not have holistic legal frameworks to combat and prevent doxxing and cyberstalking. As such, "depending on the jurisdiction in which it took place… [they] may be prosecuted under the legal provisions relating to violation of privacy or harassment."[102]

Affected journalists can seek redress via **civil and criminal law**, especially where the perpetrators can be clearly identified and where personal information not in the public domain was illegally obtained.[103] As discussed in the case below, doxxing cases can also be raised in the context of the **right to freedom of the press** and the importance of the role of the mass media in a democratic society.

Case note: Litigating 'Doxxing' against Journalists

The South African case of *Brown v Economic Freedom Fighters*, related to, journalist Karima Brown was subjected to an extended and severe doxxing attack following the public and unauthorised disclosure of Brown's personal cellular telephone number on Twitter by a prominent political leader, Julius Malema of the Economic Freedom Fighters (EFF), in the build-up to the country's 2019 parliamentary elections, ostensibly as punishment for her erroneously sending a message to the political party's WhatsApp group.

As a result, Brown began to receive threatening and "graphic messages on social media as well as her phone through voice and WhatsApp messages, many threatening rape and murder" and many with deeply charged racial connotations. Colleagues who came to her defence online were likewise subjected to a torrent of online abuse and harassment.[104]

Brown lodged an application before the High Court of South Africa in 2019 founded on the obligations of political parties and their leaders under the Electoral Code of Conduct. The High Court observed that the threats fell "well within the ambit of being harassing, intimidatory, hazardous and threatening" and that Mr Malema and the EFF had failed to

[99] DPA, 'Nigeria: President Bola Tinubu signs the Nigeria Data Protection Act 2023 into law,' (2023) (accessible here).
[100] DPA, 'Tanzania: Personal Data Protection Act comes into effect,' (2023) (accessible here).
[101] The Computer Misuse and Cybercrimes Act, No. 5 of 2018 (accessible here).
[102] Safety of Journalists 'Practical and legal tools to protect the safety of journalists' (accessible here).
[103] For more case law regarding doxing and cyberstalking affecting journalists in jurisdictions including Australia, Finland, France, Singapore, amongst others, see: The Law Library of Congress, 'Laws protecting journalists from online harassment' (2019) (accessible here). For other online harassment cases, see: Pen America, 'Online Harassment Case Studies' (accessible here).
[104] CPJ, 'South African journalist doxxed by Economic Freedom Fighters leader, threatened', (2019) (accessible here).

properly discharge their obligations under the Electoral Act by failing to issue specific instructions to EFF supporters to stop intimidating or threatening Brown.[105]

6. DENIAL OF SERVICE AND DISTRIBUTED DENIAL OF SERVICE ATTACKS

6.1. Overview

- **Denial of Service (DoS)**: A DoS attack is defined as a "cyberattack that temporarily or indefinitely causes a website or network to crash or become inoperable by overwhelming a system with data."[106]

- **Distributed denial of service attack (DDoS)**: A DDoS attack involves the malicious use of multiple distributed computers and connections to attack and disrupt the normal traffic of a targeted journalist's devices, service, or network with an overwhelming flood of Internet traffic with the aim of making these inaccessible.[107]

DDoS attacks in Africa

In November 2021, SEACOM, an ICT service provider, reported that "Africa experienced 382,500 DDoS attacks between January and July 2021." **Kenya** and **South Africa**, both ardent champions of digitisation and Internet access, accounted for a staggering 59% of these attacks.[108]

6.2. International law and standards

DoS and DDoS attacks have a disproportionate impact on the right to freedom of expression, media freedom and the public's right to information, and privacy:

- **Freedom of expression**: These attacks effectively heighten censorship and present significant hurdles as they impede information dissemination and viewing, directly censoring content.[109] Whether perpetrated by State actors or their proxies, contradicts Article 19 of the ICCPR. Given their clandestine and unlawful nature, these actions typically violate the legal requirement for restrictions on freedom of expression. [110] They also disrupt access to entire online platforms, hindering the dissemination of vital and time-sensitive information. Consequently, such measures are nearly always unnecessary and disproportionate under Article 19(3).[111]

[105] High Court of South Africa, Gauteng Division, Case No. 14686/2019 (accessible here).
[106] PEN America above n 21.
[107] Id. See also: Cloudflare, 'What is a DDoS attack?', (accessible here); UNESCO, 'Building Digital Safety For Journalism - A Survey Of Selected Issues' (2015) (accessible here).
[108] SEACOM, 'Latest research shows DDoS attacks up by 300% in Africa since 2019' (2021) (accessible here).
[109] UNESCO, 'Building Digital Safety for Journalism - A Survey of Selected Issues' (2015) (accessible here).
[110] UNSR, 'Research Paper 1/2019: Freedom of Expression and Elections in the Digital Age' (2019) (accessible here).
[111] Id.

- **Media freedom and the public's right to know:** Under international law, all journalists have the right to work free from the threat of violence to ensure the right to freedom of opinion and expression for all.[112] These attacks directly impact journalists' and news organisations' ability to provide and disseminate news and information, amounting to a curtailment of media freedom and the right of journalists to freely impart information.[113] Additionally, these attacks restrict the public's right to know by preventing some or all Internet users from accessing targeted content and websites.[114]

- **Privacy:** The UNHRC, in its Resolution on the Safety of Journalists, has emphasised that DoS attacks which "force the shutdown of particular media websites or services amount to a violation of journalists' rights to privacy and to freedom of expression."[115]

Role of the private sector

Under the UN Guiding Principles on Business and Human Rights, business enterprises have a "responsibility to respect freedom of expression [and] companies should invest resources in security measures and improvements to infrastructure that prevent or mitigate the effects of DDoS attacks involving their products or services."[116]

6.3. National laws

Typically, DoS and DDoS attacks against journalists and media houses can be combatted by relying on civil and criminal liability provided under national laws regulating cybercrimes or computer misuse.[117]

Cybercrime laws and DoS and DDoS

UNCTAD reports that 39 out of 54 African countries (72%) have enacted cybersecurity or cybercrime laws[118] which typically create offences that can be used to counter DoS and DDoS attacks against journalists and media houses.

Generally, these offences are located in provisions prohibiting crimes against computer systems and computer data, including:

- unauthorised access,
- unauthorised interference,
- unauthorised interception, or
- access with intent to commit further offences.

[112] UNESCO, 'Freedom of expression: A fundamental human right underpinning all civil liberties', (accessible here).
[113] AlterMidya, 'DDoS attacks: A menace to the people's right to know' (2021) (accessible here).
[114] Susan McGregor, 'Why DDoS attacks matter for journalists'(2016) (accessible here).
[115] UNHRC 'Resolution adopted by the Human Rights Council on the safety of journalists' (2020) (accessible here) (UNHRC Resolution on the safety of journalists).
[116] Id.
[117] Thomson Reuters, 'Distributed Denial-of-Service (DDoS) Attack' (2022) (accessible here).
[118] UNCTAD, 'Cybercrime Legislation Worldwide' (accessible here).

In **Ethiopia**, for example, the Computer Crime Proclamation, No. 958/2016 criminalises illegal access to computer systems, data or networks, the illegal interception of non-public computer data or data processing services, intentional interference with the proper functioning of a computer system, and causing damage to computer data rendering it useless or inaccessible.

For SSA countries without or with inadequate cybercrime laws, recourse might be found through other legal avenues:

- For SSA countries without or with inadequate cybercrime laws, legal recourse might alternatively be found in **data protection legislation**. For example, Section 72 of **Kenya's** Data Protection Act, 2019 prohibits obtaining access to personal data without prior authority of the data controller or data processor in certain circumstances.

- Lawyers may rely on **civil provisions**, including trespass to chattel, or a breach of contract if the attack violates a website owner's or internet service provider's terms of use.[119]

- In the alternative, if a perpetrator has used threats in an attempt to extort a journalist or a media house, one could potentially rely on **criminal offences** under the Penal or Criminal Code.

Litigating DDoS Attacks: United States[120]

The sentencing of Andrew Rakhshan in the United States for launching multiple, international DDoS attacks on media sites in Australia, New Zealand, and Canada illustrates the **viability of legal recourse against DDoS attacks** where there is an identifiable perpetrator.[121]

Rakhshan was charged and convicted with violating United States Code § 1030 (a)(5)(A) (knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer).[122] However, in April 2019, owing to ineffective assistance of trial counsel, the court ordered a retrial in which the state alleged the offence of U.S.C. § 1030 (b) (conspiracy to violate 1030 (a)).[123] In June 2020, Rakhshan, after pleading guilty to the conspiracy charge, was sentenced to five years in federal prison and ordered to pay more than $520,000 in restitution.

[119] Thomson Reuters above n 117.
[120] Department of Justice, 'Man Receives Maximum Sentence for DDoS Attack on Legal News (2020) (accessible here); Department of Justice, 'Seattle Man Arrested for the Attempted Extortion of Leagle.com and Several Other Media Companies' (2017) (accessible here).
[121] *United States v Kamyar Jahanrakhshan also known as "Kamyar Jahan Rakhshan, Andy or Andrew Rakhshan," "Andy or Andrew Kamyar," and "Kamiar or Kamier Rakhshan* (accessible here).
[122] 18 U.S. Code § 1030 - Fraud and related activity in connection with computers (accessible here).
[123] *United States of America v Kamyar Jahanrakhshan* (2018) (accessible here).

Critically, this case illustrates that litigating DoS and DDoS cases impacting digital journalism requires **technical expertise** and may often require the **cooperation of multiple state and non-state actors**, including those from multiple jurisdictions. As noted by Sentinel One, the use of the law to combat cybercrimes is "not always easy and cases often lag for years or are tried ineffectively due to a lack of technical prowess across all involved parties."[124]

Securing accountability for such attacks usually strictly requires being able to clearly attribute it to a specific state or non-state perpetrator(s).[125] However, there are some **practical challenges** to be aware of:

- Accurately identifying the origin of an attack and the perpetrator is extremely difficult due to the technical skills and know-how required and the prevalence of online anonymity tools, which makes these attacks effective intimidation tools.

- Anonymity protections online enable perpetrators to remain hidden, a challenge exacerbated by 'false flag' attacks that are committed to disguise the real perpetrator and shift blame to a third party.[126]

7. GOVERNMENT SURVEILLANCE

7.1. Overview

- **Forms:** Government surveillance of journalists can occur in both mass and targeted forms. In the former, all communications of a population are monitored in order to identify trends or specific incidents for further investigation. In the latter, a particular individual or set of individuals will be targeted to have their communications intercepted and monitored.

- **Justification**: State surveillance and interception of communications, and the accompanying processing of personal data, are usually conducted in the context of law enforcement and justified by the need to uphold national security, public order, and public morals.[127]

- **Targets**: The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has emphasised that targeted surveillance appears to be widely used to target journalists, with severe consequences for media freedom and the safety of journalists."[128]

[124] Sentinel One, 'The Good, the Bad and the Ugly in Cybersecurity – Week 25' (2020) (accessible here).
[125] Dimitar Kostadinov, 'The attribution problem in cyber attacks', (2013) (accessible here).
[126] David Trilling, 'Hacking: What journalists need to know. A conversation with Bruce Schneier', (2016) (accessible here).
[127] UN Human Rights Office of the High Commissioner, 'The Corporate Responsibility to Respect Human Rights', (2012) (accessible here).
[128] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on Reinforcing media freedom and the safety of journalists in the digital age' (2022) (accessible here) (UNSR on FreeEx Report on the safety of journalists in the digital age).

- **Anonymity and encryption:** Surveillance is intricately connected with the issues of anonymity and encryption, in that surveillance technologies often bypass encryption protections which are central to journalists' ability to conduct their work safely.

- **Regional impact**: Civil society organisations from SSA have noted that, in the region, "targeted surveillance against… media is growing, and is carried out in complex collaboration between government, the private sector and foreign governments" and that transparency gaps, weak legislative protections, and capacity gaps at the regulator, judiciary, and lawyer levels all contribute to the continued exposure and vulnerability of journalists, leading to "a chilling effect on their use of technology to assert their rights and freedoms."[129]

7.2. International law and standards

Both mass and targeted surveillance have the potential to severely impact several human rights, including the rights to privacy, data protection, and freedom of expression, among others:[130]

- **Privacy**: Unless undertaken lawfully, proportionately and necessarily, these acts "represent infringements of the human right to privacy."[131] The UNHRC has also observed that surveillance should only be used "in accordance with the human rights principles of lawfulness, legitimacy, necessity and proportionality and that legal mechanisms of redress and effective remedies [must be] available for victims of surveillance-related violations and abuses."[132]

- **Freedom of expression**: As observed by ARTICLE 19 Eastern Africa, "while protections against arbitrary or unlawful surveillance have focused on guaranteeing the right to privacy, these interferences also have a chilling effect on the rights to freedom of expression and information, and assembly and association."[133]

- **Media freedom**: In 2022, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression also observed that the "safe and free practice of journalism in the digital age is impacted by three major contemporary threats, including impunity for crimes against journalists; gender-based online attacks; and targeted digital surveillance."[134] Further, the targeted surveillance of journalists also risks the confidentiality of journalistic sources, which is a cornerstone of the profession and firmly solidified in international human rights law.[135]

- **Safety**: The UNHRC, in its Resolution on the Safety of Journalists, has emphasised that journalists face "particular risks with regard to [their safety]... including the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance and/or

[129] CSRG, ICNL & CIPESA, 'Digital Space and the Protection of Freedoms of Association and Peaceful Assembly in Africa' (2019) (accessible here).
[130] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Surveillance and human rights:' (2019) (accessible here).
[131] UNHRC, 'Right to privacy: Report of the Special Rapporteur on the right to privacy', 16 October 2019 (accessible here).
[132] UNHRC Resolution on the safety of journalists above n 115.
[133] ARTICLE 19 Eastern Africa, 'Unseen Eyes, Unheard Stories' (2021) (accessible here.
[134] UNSR on FreeEx Report on the safety of journalists in the digital age above n 128.
[135] Id.

the interception of communications…in violation of their rights to privacy and to freedom of expression."[136]

At the regional level:

- The **Malabo Convention** is the primary regional standard relating to violations of privacy and prescribes steps that states should take to legislate matters including surveillance.[137]

- The **African Declaration**, under Principle 25 (3), categorically prohibits communications surveillance except where such surveillance is ordered by an impartial and independent court and is subject to appropriate safeguards.[138] Principle 40 also prohibits indiscriminate and untargeted surveillance of individuals' communications. Further, targeted communication surveillance is only permitted where this is "authorised by law… that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim."[139]

7.3. National laws

Many countries, particularly in SSA, have struggled to structure and build the competence necessary to have meaningful oversight over surveillance capabilities. As such, the UN Special Rapporteur on the Right to Privacy has observed that there is an "imbalance between global surveillance capabilities and national oversight mandates," resulting in weakened privacy protections for journalists against targeted state-led surveillance.[140]

As countries in the region increasingly invest in a wide range of sophisticated surveillance technologies that can track many things beyond communications, including, for example, an individual's real-time movements and transactions,[141] there is an urgent need for oversight and regulation to be augmented.

Government Surveillance in South Africa[142]

In 2018, the Right2Know Campaign launched a Handbook detailing rampant and unchecked government surveillance of journalists in South Africa. In the Handbook, it was observed that 'journalists in South Africa have been a particular target for state spying, and more recently, even private-sector spying.[143] This seems to be especially true for journalists who have uncovered corruption, state capture, and abuse of power and in-fighting in agencies like the National Prosecuting Authority (NPA), the State Security Agency (SSA), the Crime Intelligence Division of the police, and the Hawks.'

[136] UNHRC Resolution on the safety of journalists above n 115.
[137] Id.
[138] Declaration of Principles on Freedom of Expression and Access to Information in Africa above n 50.
[139] Id.
[140] Ann Väljataga, 'UN Special Rapporteur on Privacy Calls for an International Treaty and a Specialised Oversight Body on Cyber Surveillance' (accessible here).
[141] Institute of Development Studies, 'Surveillance Law in Africa: a review of six countries' (2021) (accessible here).
[142] Right2Know Campaign, 'Spooked: Surveillance of Journalists in SA' (2018) (accessible here).
[143] Right2Know, 'Stop the Surveillance: Activist Guide to RICA & State Surveillance in SA,' (2018) (accessible here).

Since then, litigation has revealed extensive government surveillance of activists and civil society organisations in the country[144] and the President appointed a High-Level Review Panel on the State Security Agency to, among other things, interrogate the state of the agency's surveillance capabilities, its appropriateness, and oversight mechanisms. The Panel found that there had been:

> "a serious politicisation and factionalisation of the intelligence community over the past decade or more, based on factions in the ruling party, resulting in an almost complete disregard for the Constitution, policy, legislation and other prescripts, and turning our civilian intelligence community into a private resource to serve the political and personal interests of particular individuals."[145]

In addition, and as detailed further below, a constitutional challenge to the country's communications surveillance law, the Regulation of Interception of Communications Act (RICA), was successfully upheld by the Constitutional Court in 2021.[146]

Researchers are now conducting research on the state of surveillance laws across southern Africa as well as the efficacy and challenges of oversight mechanisms in these jurisdictions, seeking to apply the lessons from the RICA judgment to other countries in the region.[147]

Concerningly, the challenge of legal imprecision poses a major challenge in the SSA region, with permissible grounds for government surveillance in law, such as national security, either being insufficiently defined or inconsistently applied, "providing scope for abuse of power and making legal challenges practically impossible."[148] Despite this, legal challenges contesting government surveillance targeting journalists in the SSA region have been instituted before national and regional courts with varying degrees of success.

Regulating Government Surveillance in Kenya

Generally, arbitrary and illegal government surveillance against journalists can be contested by relying on several different safeguards, as demonstrated below by the example of Kenya.

1. **Safeguards in national constitutions, such as the right to privacy;**

   The right to privacy in Article 31 of the Constitution of Kenya, 2010, has been upheld by the Kenyan judiciary in the context of surveillance, including in *Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & others v Cabinet Secretary Ministry of Health & others* (2015) in which it was held that the government's directive to collect

[144] Greenpeace, 'Greenpeace Africa withdraws from state spying case after SSA disclosure,' (2023) (accessible here).
[145] 'Report of the High-Level Review Panel on the SSA,' (2018) (accessible here).
[146] *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*, 16 September 2019 (accessible here)
[147] See various pieces of research by Intelwatch here.
[148] Institute of Development Studies, 'Surveillance Law in Africa: a review of six countries' (2021) (accessible here).

data on HIV-positive people violated the right to privacy under the Constitution of Kenya, 2010.

2. Safeguards in dedicated surveillance laws:

Although there is no specific surveillance law in Kenya, several laws, and regulations touch on communications surveillance. For example, the Information and Communications Act, 2009, prohibits licensed telecommunications operators from intercepting communications while the Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations grant extensive powers to state authorities to collect and access the data of mobile phone users.[149]

3. Safeguards in data protection laws:

Kenya's Data Protection Act, 2019 provides that any state entity handling data subjects' information (i.e., personal information or sensitive personal information) must ensure conformity with Section 25 on the 'Principles of Data Protection' and with Section 26 on the 'Rights of a Data Subject,' which provide limits on the manner in which data subjects' data, including journalists' personal data, may be collected, processed and stored.[150] The Data Protection Act was tested in court in the context of surveillance in the matter of *Ondieki V Maeda* (2023) in which the High Court held that the installation of CCTV cameras by a private person violated the petitioner's right to privacy and rights as a data subject under the DPA. However, the decision has been criticised for being inconsistent with the Act, and it is clear that further consideration by the courts will be needed to provide greater clarity on these issues.[151]

Litigating Government Surveillance: South Africa[152]

The amaBhungane Centre for Investigative Journalism instituted a petition in the High Court of South Africa after information surfaced that the confidential communications of a journalist, Sam Sole, had been intercepted by state agencies.

The petition challenged the constitutionality of various provisions of RICA that permitted the interception of communications of any person by authorised state officials subject to prescribed conditions as well as the admitted practice of the State in conducting 'bulk interceptions' of telecommunications traffic.

The High Court held several sections of the law unconstitutional and invalid on the basis that they:

[149] Privacy International and the National Coalition of Human Rights Defenders in Kenya, 'Universal Periodic Review Stakeholder Report: 21st Session, Kenya: The Right to Privacy in Kenya,' (2015) (accessible here).
[150] The Data Protection Act of 2019 (accessible here).
[151] Bowmans, 'Kenya: The High Court And The Office Of The Data Protection Commissioner Issue Decisions On Complaints And The Right To Privacy In The Use Of CCTV Cameras,' (2023) (accessible here).
[152] *amaBhungane* above n 146.

- Failed to prescribe a procedure for notifying the subject of the interception;
- Failed to prescribe an appointment mechanism and terms for the designated oversight judge which would ensure the judge's independence;
- Did not adequately provide for appropriate safeguards to deal with the fact that the orders in question are granted *ex parte;*
- Did not prescribe proper procedures to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions; and
- Failed to expressly address circumstances in which a subject of surveillance is either a practising lawyer or a journalist.

The Court also declared that the bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre were unlawful and invalid.

The order was subsequently upheld by the Constitutional Court in 2021.

8. COMMERCIAL SURVEILLANCE

8.1. Overview

- **Commercial surveillance**: This involves the collection, processing, monitoring, analysis, and storage of their data relying on technological tools developed by the private surveillance industry but could ultimately be conducted by either state or non-state actors.[153]

- **Tools and technology**: In recent years, a powerful, profitable, and growing private surveillance industry has emerged driven by the demand by state entities for the services and products of private technology companies. Many of these tools have been procured and used by states specifically to target journalists, activists, opposition figures and others critical of the state.[154] Commercial surveillance tools and technologies "ultimately [serve] as a means of intimidation, increasing the risks faced by journalists and their sources and undercutting critical reporting."[155]

- **Calls for action**: This targeting of journalists has led to calls from civil society for an immediate moratorium on the sale and transfer of these tools while appropriate human rights safeguards can be put in place.[156] Privacy International has noted the various transparency, public procurement, accountability, oversight, and redress challenges of public-private surveillance partnerships.[157]

[153] UNHRC, 'Resolution on the Right to Privacy in the Digital Age,' (2019) (accessible here).
[154] UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on Surveillance and human rights '(2019) (accessible here) (UNSR on FreeEx Report on Surveillance and human rights) and OHCHR, 'Digital surveillance treats "journalists as criminals"' (2022) (accessible here).
[155] UNSR on FreeEx Report on the safety of journalists in the digital age above n 128.
[156] ARTICLE 19 Eastern Africa, 'Unseen Eyes, Unheard Stories' (2021) (accessible here).
[157] Privacy International, 'Safeguards for Public-Private Surveillance Partnerships' (2021) (accessible here). Seea also Privacy International, 'PI's Guide to International Law and Surveillance' (2021) (accessible here).

8.2. International law and standards

As noted above, surveillance implicates several rights under international human rights law, including privacy, dignity, freedom of expression, and media freedom. In the context of commercial surveillance important considerations around business and human rights come to the fore:

While states are primary duty-bearers under international human rights law, the endorsement of the UN Guiding Principles on Business and Human Rights by the UNHRC in its Resolution 17/4 solidified that **business entities also have responsibilities** for respecting and promoting human rights.[158] This includes:

- respecting human rights;
- mitigating human rights impacts of their operations; and
- providing remedies for human rights violations.[159]

As part of this responsibility, companies should "conduct due diligence and impact assessment[s] to prevent or mitigate any adverse impact on human rights resulting from their operations, products, or services, including attacks on journalists and the erosion of media freedom."[160]

Tech companies

In 2011, the UN established the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, which has encouraged technology companies to "commit to the confidentiality of digital communications, including encryption and anonymity" and urged tech companies to remind states that the surveillance of individuals, including journalists, "may only be conducted on a targeted basis, and only when there is reasonable suspicion that someone is engaging, or planning to engage, in serious criminal offences, based on principles of necessity and proportionality, and with judicial supervision."[161]

8.3. National laws

Generally, in the SSA region, the commercial surveillance infrastructure remains obscured from public view, with public-private surveillance agreements frequently being negotiated in private with little public oversight.[162]

[158] UNHRC, 'Human rights and transnational corporations and other business enterprises' (2011) (accessible here).
[159] UN Guiding Principles on Business and Human Rights above n 47. See also OHCHR, The Corporate Responsibility to Respect Human Rights an Interpretive Guide' (2012) (accessible here). See further APC, 'Why cybersecurity is a human rights issue, and it is time to start treating it like one' (2019) (accessible here).
[160] UNSR on FreeEx Report on the safety of journalists in the digital age above n 128.
[161] UNHRC, 'The Guiding Principles on Business and Human Rights: guidance on ensuring respect for human rights defenders', (2021) (accessible here).
[162] Privacy International, 'Safeguards for Public-Private Surveillance Partnerships', December 2021 (accessible here).

As such, the use of **litigation** as a course of action to remedy unlawful or arbitrary commercial surveillance is **challenging**, with the UNSR on FreeEx noting that victims of targeted surveillance have frequently had little success in the courts and that at the domestic level, there is a lack of judicial oversight, remedies, and enforcement.[163]

Legal Action Against Commercial Surveillance Targeting Journalists: NSO Group

In 2021, the Pegasus Project revealed that more than 180 journalists across 20 countries have been potentially targeted for surveillance by governments relying on spyware produced by NSO Group Technologies. Pegasus, NSO's premier spyware tool, breaks encryption protections for communications devices before proceeding to infect the devices with spyware to monitor communications.[164] NSO Group sells this software on a subscription basis to law enforcement and intelligence agencies around the world.[165]

Legal action has been taken against NSO Group by several actors with varying legal bases. In 2020, Amnesty International unsuccessfully approached an Israeli District Court seeking to have NGO Groups' export license revoked.[166] In India, the Supreme Court ordered an investigation in 2021 into the government's alleged use of the spyware to illegally surveil journalists, activists, and political opponents.[167] In 2022, the committee concluded its investigation but did not release its findings publicly beyond noting that the Indian authorities "did not cooperate" with the investigators, and new incidents of the use of technology to spy on journalists continue to be revealed.[168]

9. PHISHING

9.1. Overview

- **Phishing**: Phishing is defined as a "cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords."[169] Once this information has been provided, the hacker can gain access to, and sell, the individual's personal accounts and claim the hacked individual's identity (identity theft).

- **Campaigns**: Phishing is a prevalent form of targeted surveillance and digital security attacks which can impact journalists. Phishing campaigns can also be used to enable

[163] UNHRC, 'Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', 28 May 2019 (accessible here).
[164] ARTICLE 19, 'Rwanda: Surveillance revelations opportunity to reform legal and encryption environment', 26 July 2021 (accessible here).
[165] Ronen Bergman & Mark Mazzetti, 'The Battle for the World's Most Powerful Cyberweapon', 28 January 2022 (accessible here).
[166] Amnesty International, 'Israel: Court rejects bid to revoke notorious spyware firm NSO Group's export licence,' (2020) (accessible here).
[167] The Guardian, 'Indian supreme court orders inquiry into state's use of Pegasus spyware,' (2021) (accessible here).
[168] Amnesty International, 'India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists,' (2023) (accessible here).
[169] Phishing.org, 'What Is Phishing?' (accessible here).

hackers to install surveillance technology to access a journalist's personal information, data, and sources often without the journalist's knowledge, to blackmail them through the misuse of personal information, and to provoke self-censorship.[170]

9.2. International law and standards

Phishing attempts, whether successful or otherwise, violate journalists' right to **privacy**, **data protection**, and **freedom of expression**, with these abuses being characterised by continuity, due to the ability of perpetrators to utilise different online and offline platforms to constantly re-victimise victims, including through identity theft attacks.[171]

As such, the UNSR on FreeEx has noted that targeted digital surveillance technologies and methods targeting journalists, including phishing, are "**contrary to international human rights law**, according to which both reporter and source enjoy rights that may be limited only in accordance with the strict requirements of Article 19(3) of the ICCPR."[172]

9.3. National laws

Civil and criminal liability under national laws regulating cybercrimes or computer misuse could be used to address phishing attacks against journalists.[173] As noted, 39 out of the 54 listed African countries have enacted cybersecurity or cybercrime laws.[174]

Phishing in Nigeria

In **Nigeria**, it is commendable that Section 32 of the Cybercrimes (Prohibition, Prevention, Etc) Act of 2015 explicitly criminalises phishing[175] while Section 22 explicitly addresses the scenario in which a phishing campaign against a journalist results in either identity theft or impersonation.[176]

For SSA countries without or with inadequate cybercrime laws, alternative legal routes that may be pursued could relate to **data protection** and the compromising of confidentiality and integrity of data, and/or the disclosure of personal information without the data subjects' prior and informed consent, amounting to a violation of a journalist's right to informational privacy.[177]

Other **civil provisions**, such as trespass to chattel or a breach of contract if the attack violates a website owner's or internet service provider's terms of use, might also be relevant.[178] Lastly, **criminal offences** under the Penal or Criminal Code might be relevant where, for example, a perpetrator, in carrying out a phishing attack, blackmails a journalist.

---

[170] UNESCO, 'Building Digital Safety for Journalism - A Survey of Selected Issues', 2015 (accessible here).
[171] Id.
[172] UNHRC, 'Reinforcing media freedom and the safety of journalists in the digital age: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan', 20 April 2022 (accessible here).
[173] Thomson Reuters above n 117
[174] UNCTAD, 'Cybercrime Legislation Worldwide' (accessible here).
[175] Cybercrimes (Prohibition, Prevention, Etc) Act of 2015 (accessible here).
[176] Id.
[177] Media Defence, 'Module 4: Data Privacy and Data Protection,' December 2020 (accessible here).
[178] Thomson Reuters above n 117.

10. CONFISCATION OF HARDWARE

10.1. Overview

- **Confiscation**: The confiscation of journalists' hardware is defined as the temporary or permanent seizure of a journalist's professional or personal equipment, including laptops, phones, and cameras, amongst others. This is a tactic frequently used by state actors to intimidate or harass journalists, especially those reporting during high-tension periods, such as elections, or during protests.

10.2. International law and standards

The confiscation of a journalist's equipment amounts to an attack against **freedom of expression**, which runs counter to the permissible limitations under Article 19(3) of the ICCPR.[179] It might also be considered prior restraint — restricting access to content before it has been published — that is generally seen under international human rights law to be unnecessary and disproportionate.[180]

10.3. National laws

The confiscation of journalists' hardware is a rampant challenge in the SSA region, with many law enforcement officers relying on **search and seizure** provisions in national laws such as the **Penal Code**, or **cybercrime or computer misuse laws**.[181]

Case Note: Search and seizure and privacy

Unfortunately, examples abound in SSA of law enforcement seizing the hardware and equipment of journalists, often under dubious circumstances. In the **Kenyan** *Standard Newspapers Limited & another v Attorney General & Others* (2006) case, the Standard Newspaper's and Kenya Television Network's premises were raided in by officers acting under the authority of the Minister in Charge of Internal Security without a search warrant.[182] They vandalised and destroyed broadcasting and other equipment, broke the printing press, and seized other items ostensibly to protect sensitive information which, if published would have threatened national security.

The High Court emphasised that while the right to privacy is not absolute, any limitation must not be one that would strip the right of its very core or purpose. It held that the search and seizure was arbitrary, in violation of due process requirements, had no lawful justification, and was in breach of the petitioners' rights to privacy.

[179] Coen, 'Parliamentary Assembly of the Council of Europe Recommendation 1506: Freedom of expression and information in the media in Europe', 2001 (accessible here).
[180] Media Defence, 'Module 1: General Overview of Trends in Digital Rights Globally and Expected Developments – Advanced Modules on Digital Rights and Freedom of Expression Online,' (2022) (accessible here).
[181] See: International Federation of Journalists, 'Ethiopia: Media houses raided and 9 media workers arrested', 25 May 2022 (accessible here). See: Sudan Tribune, 'Ethiopia releases NY Times journalists detained for 5 days', 23 May 2007 (accessible here).
[182] Civil Society Protection Platform, 'Digital Space Case Digest,' (2020) (accessible here) at p. 21.

11. CONCLUSION

In addition to stifling freedom of expression and independent reporting, digital attacks against journalists also prevent or discourage women journalists from entering or staying in the field, preventing greater diversity and representation in the field that is much needed.

It must be emphasised that the function of journalism covers a broad range of actors, "including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the internet or elsewhere."[183] Protections against digital attacks must, therefore, be directed not only at professional journalists but also at others who play an important role in facilitating the free flow of information online.

Defenders of freedom of expression and gender rights can look to the international human rights mechanisms, including the reports of UN Special Procedures, for guidance and tools to act against digital attacks against journalists and further provide journalists with critical access to legal remedies where appropriate. Additionally, it must be borne in mind that the UNGPs define the responsibilities of private sector actors to respect human rights, mitigate the human rights impacts of their operations, and provide remedies for human rights violations, "given that the private sector owns and/or operates most of the infrastructure, hardware and software upon which the internet relies."[184]

In taking forward the sober challenges raised in the Module, it is vital that activists, lawyers, human rights defenders, and supporters of the media understand the various manifestations of online attacks against women journalists, as well as the relevant international and domestic legal provisions, to consider legal actions that can defend and promote the right of women journalists in Africa to practice their craft free from violence. In this regard, it is notable that this module is complemented by Module 3 in this series, which provides detailed guidance on the practicalities of potential litigation for digital attacks affecting journalists.

[183] UN Human Rights Committee, 'General comment No. 34 Article 19: Freedoms of opinion and expression', 12 September 2011 (accessible here).
[184] UN Guiding Principles on Business and Human Rights above n 47 and APC above n 159.

Module 3

PRACTICAL APPROACHES TO COMBATTING ONLINE VIOLENCE AGAINST WOMEN JOURNALISTS

Modules on Online Violence against Journalists in Sub-Saharan Africa

MEDIA DEFENCE

Published by Media Defence: www.mediadefence.org
This module was prepared with the assistance of Catherine Muya, Sigi Waigumo Mwanzia, and ALT Advisory: https://altadvisory.africa/

Published in 2024

TABLE OF CONTENTS

MODULE 3
PRACTICAL APPROACHES TO COMBATTING VIOLENCE AGAINST WOMEN JOURNALISTS

- **The prevalence and severe impacts of online violence against women journalists in SSA calls for concerted and wide-ranging efforts to protect them online and seek accountability for such harms.**

- **Litigation can be a particularly impactful way of doing so, but comes with particular requirements that warrant careful consideration, such as jurisdiction, standing, and admissibility.**

- **Alternatively, or in concert with litigation, supporters can consider law reform strategies as well as advocacy campaigns that can build public or targeted support for a particular issue or case.**

- **Finally, it is vital that journalists take practical steps to protect themselves online and to deal with online violence when it occurs to mitigate against the silencing effect of these attacks.**

1. INTRODUCTION

The media, the government, the state, and civil society organisations are struggling to respond effectively to online violence against women journalists. This highlights the urgent need for policy reform and innovative legal, legislative and normative responses, in order to ensure compliance with international human rights law.[1]

Effectively countering online violence against journalists, particularly women journalists,[2] in sub-Saharan Africa (SSA) is a pressing global issue that demands:

- Localised;
- Contextualised;
- Intersectional; and
- Practical strategies.

This module focuses on the **practicalities of litigation** to protect and defend the rights of women journalists online, providing guidance from the initial phases of consideration of litigation through to the legal requirements. In addition to litigation, this module considers complementary strategies such as **advocacy**, which can support litigation by building public

[1] UNESCO 'The Chilling: Global trends in online violence against women journalists' (2021) (accessible here).
[2] For conciseness, we refer hereafter to "women" to include all those who identify as women and those with marginalised or at-risk identities including members of the LGBTQI+ community, except where specific instruments or documents referenced refer explicitly to "women" or some other grouping.

awareness and support, as well as **digital security tactics** and tools for victims and survivors of online violence to protect themselves in the digital sphere.[3]

It is complemented by Module 6 in Media Defence's series of Advanced Modules on Digital Rights and Freedom of Expression in sub-Saharan Africa on Litigating Digital Rights Cases in Africa, which details how to litigate within several of the key human rights fora on the continent.

2. LITIGATION STRATEGIES

- **Strategic litigation**: Strategic litigation, sometimes also referred to as impact litigation, is a method of seeking broad social change, beyond a remedy for an individual, by carefully selecting and bringing a case to court.[4] It has been used extensively around the world, including in SSA, to set progressive jurisprudence and achieve accountability for human rights abuses.

- **Challenges and opportunities**: While it can be risky — with the potential for a negative judgment or unforeseen externalities — and tends to require significant investments of time and resources, it can be a highly effective way of stimulating law reform, influencing public opinion, and having a real impact on the lives of people affected by rights violations.

- **Key considerations**: In considering whether litigation can or should be launched in case of online violence against women journalists, one should consider:

    - the outcomes sought;
    - whether litigation can reasonably achieve these outcomes;
    - whether the victims, survivors or affected communities will be best served by litigation;
    - what various potential paths the litigation could take; and
    - how the outcomes of litigation could be leveraged for positive social change.

Strategic litigation in the context of digital rights and online harms poses unique challenges and opportunities that should also be considered when developing litigation strategies.[5]

The impact of strategic litigation in SSA

Strategic or impact litigation has played an important role in advancing freedom of expression in sub-Saharan Africa for many years. Media Defence has supported some key cases relating to journalists operating in both the offline and online realm including:

- *Konaté v Burkina Faso* (2013): the African Court on Human and Peoples' Rights held that criminal defamation laws that imposed sanctions of imprisonment were

[3] The terms "victim" and "survivor" may be used interchangeably and refer to those who have experienced GBV and/or OGBV. These terms have different connotations and implications and do not intend to, by any means, impose a definition or response on any persons who have experienced some of the severe violations to their dignity and safety.
[4] Child Rights International Network, 'What is strategic litigation?' (accessible here).
[5] Digital Freedom Fund, 'Strategic Litigation Toolkit' (2022) (accessible here).

incompatible with Article 9 of the African Charter of Human and Peoples' Rights and other international human rights provisions.

- *Media Council of Tanzania v Attorney-General of the United Republic of Tanzania* (2019): the EACJ held that certain provisions of Tanzania's Media Services Act relating to fake news and rumours violated the right to freedom of expression by their broad and vague wording.

- *SERAP v Federal Republic of Nigeria* (2022): the ECOWAS Court held that the government's suspension of Twitter in the country in 2021 violated the rights to freedom of expression, access to information and the media.

- *Amnesty International Togo v the Togolese Republic* (2020): The ECOWAS Court held that the Togolese government violated the right to freedom of expression by shutting down the internet during protests in September 2017.

2.1. Forums

The selection of a **suitable forum** with jurisdiction is critical to the eventual success of litigation. Lawyers should consider what is effective and available at the national, regional, and international levels. Typically, regional and international fora are only available where national remedies have been exhausted or where non-binding decisions are being sought, although there are some exceptions.

There are a range of such fora to be considered, including:[6]

- The United Nations Human Rights Council (**UNHRC**);
- The African Court on Human and Peoples' Rights (**African Court**);
- The African Commission on Human and People's Rights (**ACHPR**);
- The Economic Community of West African States Community Court of Justice (**ECOWAS Court**); and
- The East African Court of Justice (**EACJ**).

Each of these has its own requirements for founding jurisdiction, which must be carefully considered before launching an application or a complaint.

[6] See International Press Institute, 'A resource toolkit of laws, commitments, and mechanisms protecting press freedom in Africa' (2023) (accessible here) for high-level guidance on international, regional, and sub-regional treaties, protocols, mechanisms, and commitments that comprise the frameworks for media freedom, the right to access information, and the safety of journalists in Africa. See further the Pan African Lawyers Union, 'Manual for litigating when accessing the ECOWAS Court of Justice' (2022) (accessible here) for technical guidance on litigating before the ECOWAS Court of Justice.

Use of quasi-judicial fora

There are several quasi-judicial international and regional fora available that can also be valuable in providing progressive opinions and guidelines for states on regulating online harms and protecting freedom of expression.

For example, in *Nyanzi v. Uganda* (2017) the United Nations (UN) Working Group on Arbitrary Detention (WGAD) issued an opinion finding that the detention of a Ugandan human rights activist for violation of the Cybercrime Act was arbitrary and a violation of her rights. The WGAD condemned the broad and vaguely worded provisions under which Nyanzi was arrested, which were said to have a chilling effect on freedom of expression in the country.

While the WGAD's opinions are **not legally binding**, its findings, in this case, that Stella Nyanzi's arrest and detention amounted to a violation of the rights to freedom of expression, a fair trial, the presumption of innocence, liberty and security of person, and freedom from torture or to cruel, inhuman or degrading treatment nevertheless have **significant persuasive power**, and states against whom opinions are made are requested to provide follow-up information on the implementation of the recommendations within six months.[7]

2.2. Jurisdiction

Jurisdiction refers to the ability or competency of a court or forum to consider and decide a particular matter.

Defining jurisdiction

In the Kenyan case of *Owners of Motor Vessel Lillian's' vs Caltex Oil Kenya Limited* (1989), the Court of Appeal at Mombasa confirmed that the term means:

> "The authority which a court has to decide matters that are before it or take cognisance of matters presented in a formal way for its decision. The limits of this authority are imposed by statute, charter or commission under which the court is constituted and may be extended or restricted by the like means."

When determining whether a court has jurisdiction, it is important to look at several sub-components:[8]

- **Jurisdiction *ratione personae***: whether the court has jurisdiction over the person of both the complainant and the respondent.

[7] United Nations, 'Opinions adopted by the Working Group on Arbitrary Detention,' (accessible here).
[8] Media Defence, 'Digital Rights Litigation Guide, Litigating Digital Rights and Freedom of Expression in East, West and Southern Africa' (2020) (accessible here).

- **Jurisdiction *ratione materiae***: whether the subject matter falls within the scope and mandate of the forum concerned.

- **jurisdiction *ratione temporis***: whether the violations occurred within a time frame that allows the forum to exercise jurisdiction. Temporal jurisdiction usually refers to whether:

    - the violation occurred after the relevant treaty establishing or granting the court authority had come into force for a particular country, and
    - the victim brought the claim before the forum within a reasonable period after the violation occurred.

For more information on jurisdiction, admissibility and proceedings at regional fora in Africa, please see Module 6 on Litigating Digital Rights in Africa.

2.3. Standing

Standing refers to the **ability of a party to bring a matter before the court**. It involves a potential litigant demonstrating a sufficient connection between the issue and their interest in the issue. Different courts and fora may have different standing requirements, this should be considered and determined early on in strategic litigation.

- In **domestic courts**, standing is determined by national law and the subject matter of the suit.
- In **regional and international courts**, standing is determined by the rules of procedure of the forum.

The table below lists some examples of the standing requirements of different fora:

Fora	Standing requirements
Domestic	Article 22 of the **Kenyan** Constitution allows a person to: • act in their own interest; • act on behalf of another who cannot bring the suit in their own name, • act in the interest of a group or class, or • act in the public interest to institute a suit claiming that a right or fundamental freedom has been violated, threatened, or infringed.
ECOWAS Court	The ECOWAS Court has fairly broad standing provisions. Articles 9 and 10 of the Supplementary Protocol provide that the following litigants may approach it: • Member states. • The Executive Secretary (now the President of the ECOWAS Commission). • The Council of Ministers. • Community Institutions. • Individuals.

	• Corporate Bodies. • Staff of any Community Institution. • National Courts of ECOWAS Member States.
ACHRP	The ACHPR has broad standing provisions. Anyone can register a communication, including CSOs. This includes: • a state claiming that another state party to the African Charter has violated one or more of the provisions in the African Charter; • CSOs (which do not need to be registered with the AU or have observer status); • victims of abuse; or • interested individuals acting on behalf of victims of abuse. The matter can also be brought for the public good, as class or representative actions, under the actio popularis approach.[9]

- **Considerations on standing:** When considering whether a party has standing, it is important to consider and assess:

    - Whether an individual, community or civil society organisation is best placed to bring the matter to the court or forum?
    - Would a combination of different applicants be strategic?
    - What are the different interests in the matter?
    - What are the different risks of instituting a matter on behalf of certain parties?
    - What is in the best interest of the case and the affected parties?
    - What are the resources or capacity constraints?[10]

Value of broader standing requirements

The use of **Kenya's** expanded standing was successful in the case of *Bloggers Association of Kenya v Attorney General & 3 others ARTICLE 19 Eastern Africa & another* (2020) in which the Bloggers Association of Kenya (BAKE) launched a constitutional petition challenging the constitutionality of 26 sections of the Computer Misuse and Cybercrime Act.

In both *Article 19 v Eritrea* (2007) and *Law Society of Zimbabwe and Others v Zimbabwe* (2016), the **ACHPR** underscored the significance of broader standing provisions, adopting an *actio popularis* approach. This approach allows individuals, NGOs, and groups with no direct relationship to victims to bring forth communications, ensuring that even marginalized victims of human rights violations can receive assistance from distant entities. While compliance with standing requirements is necessary, the ACHPR's flexibility in allowing non-victim entities to file complaints emphasizes its commitment to promoting accountability and addressing human rights abuses across the continent.

[9] For more on standing see Pedersen, 'Standing and the African Commission on Human and Peoples' Rights' African Human Rights Law Journal (2006) (accessible here) and Mayer, 'NGO Standing and Influence in Regional Human Rights Courts and Commissions' Notre Dame Law School (2011) (accessible here).
[10] Media Defence, 'Module 6: Litigating Digital Rights Cases in Africa,' (2020) (accessible here).

2.4. Representation and Expertise

Different courts have their own rules on representation, and in some cases, legal representation may not be mandatory. It should be kept in mind that there are a range of organisations working to provide technical and legal support to legal efforts to protect journalists' safety and freedom of expression, which can be drawn on if needed, particularly by providing access to experienced senior digital rights lawyers. These include, for example:

- Media Defence;
- The International Women's Media Foundation;
- The International Press Institute;
- The Legal Network for Journalists at Risk;
- The Vance Center for International Justice;
- The Pan African Lawyers Union;
- The Thomson Reuters Foundation TrustLaw programme; and
- The International Senior Lawyers Project.

2.5. Admissibility

- **Admissibility**: This refers to the process applied by international human rights fora to ensure that only cases that need international adjudication are brought before them.

- **Requirements**: Usually, it is required that all local remedies have been exhausted, that consideration be given to whether there are rules relating to prescription, and whether the forum recognises the concept of ongoing harm.

- **Exceptions**: There are exceptions to the local remedies requirement, such as if local remedies are non-existent, unreasonably prolonged or inaccessible, etc.[11] Notably, the ECOWAS Court and the EACJ do not require local remedies to have been exhausted before bringing a matter,[12] although the ECOWAS Court does require that the matter has not been determined on the merits by domestic courts.[13]

2.6. Identifying the parties

It is important to consciously reflect on and identify the most appropriate respondent in a matter, especially in cases involving anonymous or pseudonymous users or multi-national technology companies based in foreign jurisdictions. To assist in this, a litigant may seek an order from the court for an intermediary to disclose the identity of the user or to provide clarity on business structures. Law enforcement officers may also send a legal request to an intermediary requesting them to disclose the identity of the user.

[11] Media Defence, 'Digital Rights Litigation Guide, Litigating Digital Rights and Freedom of Expression in East, West and Southern Africa', June 2020 (accessible here).
[12] Id.
[13] Media Defence, 'Digital Rights Litigation Guide, Litigating Digital Rights and Freedom of Expression in East, West and Southern Africa' (2020) (accessible here).

Case law examples

In *Muwema v Facebook Ireland Ltd* (2016), the plaintiff sought an order directing Facebook to provide details on the identities and location of the person or persons who operated a particular Facebook page that had posted allegedly defamatory materials, or the individual posters to that page.[14] The court granted this order and directed Facebook to disclose the identity of the owner of the page on terms agreed to between the parties.

In South Africa, a 13-year-old girl received threatening posts from an anonymous user on Instagram. She made several failed attempts to obtain the identity of the user from Facebook. She then obtained orders from the High Court in Johannesburg directing Facebook to disclose the identity of the user but had to instruct an advocate in the United States to serve the order to Facebook at their offices in California. Eventually, Facebook complied with the order, but this came at a great cost for the plaintiff.[15]

2.7. Amici curiae

Amicus curiae are friends of the court who, while not a main party to the litigation, instead offer advice to the court to assist in the determination of the matter. An *amicus* may petition the court to be granted leave to serve as an *amicus* or may be invited by the court to offer expertise. Thus, serving as an *amicus* can be an influential way to support strategic and impact litigation and to provide relevant guidance to the court, particularly on international human rights standards and comparative law, as well as by providing technical expertise on digital or technological questions.

Each court or forum will usually have its own rules regarding the admission of *amici*, but often this involves proving that one's submission will be unique and additive to the litigation.

Fora	Amici requirements
Domestic	In South Africa in terms of the Uniform Rules of Court, in order for a party to be admitted as an *amicus curiae*, the following requirements must be met: • It must have an interest in the proceedings; • The submissions to be advanced must be relevant to the proceedings; and. It must raise new contentions that may be useful to the court. South African Courts have explained that the role of *amici* is to draw the court's attention to relevant legal and factual matters not otherwise highlighted. Admission as an amicus requires demonstrating an interest in the proceedings, the relevance of submissions, and the introduction of new, beneficial contentions.[16]

[14] Id.
[15] Tania Broughton, 'Joburg teen sues Facebook for name of Insta stalker who threatened rape & murder' (2020) (accessible here).
[16] See for example *Hoffman v South African Airways* [2000] ZACC 17 (accessible here) and *In Re: Certain Amicus Curiae Applications; Minister of Health v Treatment Action Campaign* [2002] ZACC 13 (accessible here).

EACJ	*Amici curiae* are allowed to apply to be involved in a matter per Article 36 of the EACJ Rules. An application must be made by notice of motion and provide the following information: • A description of the parties. • The name and address of the *amicus curiae.* • A description of the claim or reference. • The order in respect of which the *amicus curiae* is applying for leave to intervene. • A statement of the *amicus curiae*'s interest in the result of the case.
African Court	Amici curiae are allowed in the African Court as per Rule 45(1) of the African Court Rules, which grants the Court the authority to hear from individuals or entities deemed likely to provide assistance in fulfilling its duties. Furthermore, Rule 45(2) empowers the African Court to request any person or institution to provide information, opinions, or reports as needed. The procedure for requesting to act as amicus curiae is outlined in sections 42 to 47 of the African Court's Practice Directions: • Individuals or organizations interested in acting as amicus curiae must submit a request to the African Court, specifying their intended contribution to the matter. • If the request is granted by the African Court, the requester will be notified by the Registrar and invited to submit their contributions, along with all relevant pleadings. It's important to note that the decision to grant a request to act as amicus curiae rests solely with the discretion of the African Court.

2.8. Administrative considerations

Litigation is costly, with implications for both the victim/affected party, relevant third parties, and lawyers themselves. It is important to ensure that any litigation that is pursued is **adequately funded**. This includes funding for all future potential stages of appeal and review.

Litigants should also, at an early stage, consider the most effective timing for launching litigation or important milestones in the case and evaluate the staff and capacity needs — both in terms of legal support and otherwise — to ensure the case can be managed effectively to its end.

2.9. Choice of remedy

Another key element for consideration, particularly in terms of evaluating the substantive goals of litigation, is the choice of remedy. Depending on a country's legal framework, online violence can be both a criminal and civil offence, which would influence the practicalities of litigation.

Online Violence under Criminal Law

- **In Ethiopia:** article 13 of the Computer Crime Proclamation, No. 958 of 2016 criminalises online activities that intimidate; threaten, or cause fear, threat, or psychological strain.[17]

- In **Kenya:** section 27 of the Computer Misuse and Cybercrime Act, 2018 provides for the offence of cyber harassment and imprisonment for up to 10 years.

- In **Uganda:** the Computer Misuse Act, 2011 prescribes offences such as cyber harassment, cyber stalking and offensive communications that can be used to prosecute online violence.

Online Violence in Civil Law

National law and common law can allow a victim of online violence to seek civil law remedies such as:

- A civil suit for defamation;
- An order for the payment of compensation;
- A declaration of rights;
- A declaration of invalidity of any law that denies, violates, infringes, or threatens a right or fundamental freedom; or
- A protection order that restrains an abuser from certain behaviour.

Several factors influence the appropriate relief to be pursued for an online violence case, including:

- **Standard of proof**: the standard of proof in criminal cases is beyond reasonable doubt, much higher than that in civil law, in which it is a balance of probabilities.

- **Responsibility of the prosecution**: Depending on national law, the responsibility to prosecute is usually placed on the state, state agency or independent institution created by national law. This means that criminal prosecution may be out of reach for would-be litigants. However, one can consider whether the country provides mechanisms for private prosecution or can act for a client either by watching brief or advancing a defence in the case of an accused person.

- **Defences offered by the respondent/defendant***:* The available defences to the respondent or defendant will have an important impact on the prospects of success of the litigation. One should, therefore, consider the context and facts of a case to determine which defences might impact the relief being sought.

[17] Computer Crime Proclamation 958 of 2016 of the Federal Democratic Republic of Ethiopia (accessible here).

Defence of Innocent Publication

In *Muwema v Facebook Ireland Ltd* (2016), the Facebook account of a pseudonymous user published three articles about a Ugandan lawyer, Fred Muwema, on a Facebook page, which Muwema alleged were defamatory for falsely accusing him of various acts of fraud, bribery, and political subterfuge. Muema sought to have the posts removed by Facebook, based in Ireland, requests which were declined based on the argument that Facebook was not the publisher of the content and could only take down content following a valid order of court.

Muema brought proceedings in the High Court of England seeking an order prohibiting the publication or further publication of the content. According to the law, such order can only be granted where;

- the statement is defamatory, and
- the defendant has no defence to the action that is reasonably likely to succeed.

The court declined to grant the order on the grounds that the defendant had a reasonable chance of success in raising the defence against defamation of innocent publication, which would mean that it had taken "reasonable care" in publishing the material.

2.10. Gathering evidence

A central challenge facing proponents of safer digital spaces is the collection of admissible evidence. In sub-Saharan Africa, the ICT Policy Centre for Eastern and Southern Africa (CIPESA) reports that the quantification of instances of online GBV remains a challenge "due to several inhibitions, including the culture of silence."[18]

Documenting abuse

Victims of online violence can also assist in gathering evidence by documenting the abuse they face. It is, therefore, important to inform victims of measures they can take to document their experiences. Of note in this regard are the following guidelines:

- Pen America has created a guide that one can use to document online harassment.[19]
- Open Global Rights has listed an array of modules, apps and tools that seek to assist human rights activists with the collection, preservation, and verification of online evidence of human rights violations.

Key considerations around evidence gathering include:[20]

[18] CIPESA, 'In Search of Safe Spaces Online: A Research Summary' (2020) (accessible here).
[19] PEN America, 'Online Harassment Field Manual: Documenting Online Harassment' (accessible here).
[20] Media Defence, 'Module 6, Litigating Digital Rights in Africa', (2020) (accessible here).

- **Balancing exercise**: Lawyers must balance victims' rights to digital anonymity with the anonymity of perpetrators while ensuring that evidence is admissible and collected legally.
- **Domestic laws**: Gathering evidence is crucial for litigating online violence, necessitating an understanding of domestic laws on electronic evidence to tender relevant and admissible evidence to the court.
- **Experts**: Obtaining specialist technical assistance may be necessary to gather and interpret digital information effectively.
- **Requirements**: Legal and technical requirements must be considered by litigants and courts when assessing the admissibility of evidence, including the digital forensics procedures and tools used, the digital laboratories where analyses occur, and the qualifications of digital forensics analysts and expert witnesses.

Gathering Electronic Evidence

Gathering electronic evidence appropriately often requires understanding a complex puzzle of various pieces of legislation.

In **Uganda**, for example, in addition to the Evidence Act, one must also consider the Computer Misuse Act of 2011, the Electronic Signatures Act of 2011, and the Electronic Transactions Act of 2011. Section 9 of the Computer Misuse Act, 2011 allows an investigating officer to apply to court for a preservation order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.[21]

In **Kenya**, section 78A of the Evidence Act provides requirements for how the probative value of the evidence must be determined,[22] which includes assessing the reliability of the manner in which the electronic and digital evidence was generated, stored or communicated and the manner in which the originator of the electronic and digital evidence was identified.

2.11. Safety and security considerations

Potential litigants also need to consider the **virtual and physical risks** associated with litigating issues of online GBV, including the risk of attracting negative attention from perpetrators and their supporters. Based on this, the protection of victims/survivors of online

[21] KTA Advocates, 'Electronic Evidence, Legal Alert', (2020) (accessible here).
[22] Rutenberg, Kiptiness & Sugow, 'Admission of Electronic Evidence: Contradictions in the Kenyan evidence Act', 2021 (accessible here).

GBV, their family members, witnesses, and any other relevant third parties, such as colleagues, should be carefully dispensed with before a matter is instituted.[23]

This may require lawyers to deploy solutions to address safety and security concerns, deal with issues around anonymity and confidentiality, and take steps to prevent the potential re-traumatisation of the victim/survivor and other third parties.

Example: seeking accountability for NCII

Victims or survivors of the non-consensual dissemination of intimate images, (NCII) might consider the following practical elements in determining whether there is a legal remedy they could pursue, and how to do so:

- Check whether your country has a specialised legal framework on NCII or cyber harassment more broadly;
- Check whether your country has harassment or stalking laws which could be applied to the situation, such as those regarding protection orders or cybercrime laws;
- Determine whether domestic violence or family violence regulations could be applied to your situation;
- Check your country's laws on requiring electronic service providers to identify individuals responsible for online crimes, which would allow for suing the perpetrator for damages.

3. ADVOCACY STRATEGIES

3.1. Development of advocacy strategies

The potential impact of litigation can often be augmented and supported by accompanying advocacy campaigns that seek to bolster public support and awareness around the relevant issues. This may be particularly true in matters of online violence which involve technical elements and with which stakeholders, including magistrates or judges, may be unfamiliar.

Advocacy design and impact

Litigators should consider the ultimate goal of the litigation and design an appropriate advocacy strategy that works towards complementing this goal by, for example:

- Researching particular issues to shed greater light on the case;
- Aiming to educate specific or general audiences;
- Seeking to build public support for the case or an issue more broadly;
- Attempting to influence public perceptions of an issue;
- Instigating public protests or other forms of support;
- Advocating for policy or law reform; or

[23] European Human Rights Advocacy Centre (EHRAC) & Middlesex University London, 'EHRAC Guide to Litigating Cases of Online Violence against Women, Domestic & Sexual Violence', (2020) (accessible here).

- Aiming to better understand the public's position on a topic.

An effective advocacy campaign can also help to ensure that, even where a case is ultimately unsuccessful, other impact is achieved through greater awareness of an issue or the development of a network of allies.[24]

Keep in mind that advocacy campaigns typically require a different skillset from litigation and require building a compelling narrative or story that will resonate with large numbers of people.

Further, lawyers can refer to, and tailor, the guidance provided by the UN Women regarding the development of an advocacy strategy to tackle violence against women.[25] This strategy can be tailored with support from country-based individuals and groups to ensure that intersectionality guides the strategy development.

3.2. Literacy for the courts and media

Numerous commentators note that online GBV is still a relatively nascent area of consideration in the SSA region. There is a need for efforts to engage judicial officers, as well as the media, to **sensitise** them on the impact of digital security attacks on journalists' human rights, media freedom, and democratic values.

Litigating online violence: South Africa

The case of *South African Human Rights Commission v Matumba* (2018), heard in the Equality Court of **South Africa**, provides some guidance on some of the practical challenges of litigating online violence matters in the lower courts in the region.

Matumba was accused of running a Twitter account in which he pretended to be a white woman and through which he made derogatory comments against black women, ostensibly in an attempt to sow racial discord and misogyny.[26] The South African Human Rights Commission sought an order that the posts constituted harassment in terms of the country's Equality Act.

- **Digital landscape**: The SAHRC, in bringing forward the case, had to make use of a tracing agent to link the Twitter account to Matumba, as well as request information from Twitter through its legal representatives to link the account to Matumba's cell phone number. An *amicus* submission by media organisation Media Monitoring Africa provided extensive submissions on the context presented by social media platforms, including how that context affects the spread of the information, who constitutes the

[24] Digital Freedom Fund above n 5 at 51.
[25] UN Women, 'Developing an Advocacy Strategy' (2010) (accessible here).
[26] SAHRC, 'Trial of EFF councillor who allegedly masqueraded as a white woman on Twitter gets underway,' (2022) (accessible here).

hypothetical reasonable reader on Twitter, and how to craft effective remedies in such a situation where harassment has been perpetrated online.[27]

- Terminology: Due to the contemporary nature of the mode of harassment, it was necessary for the parties to assist with court with **definitions**, **guidance,** and **examples** of terms associated with the online world such as "post", "like", "retweet", "bitly", and "account owner".

Given that some of the terms and processes of the online world may be new to judicial officers it is important to provide useful explanations or **comparative examples** to ensure clarity and understanding of potentially novel terms.

This case illustrates those amici submissions, alongside those of the parties, can be an important and impactful way to enable and enhance the **literacy of judicial officers** on issues of online violence.

3.3. Legislative/policy reform

In addition to instituting litigation, efforts to seek legislative and policy reform can be simultaneously pursued as a measure to ensure that legal provisions are put in place to provide meaningful protection to women journalists online.[28]

The Organisation for Security and Co-operation in Europe (OSCE) provides guidance on how to ensure that legislative frameworks, most notably pre-existing harassment laws, can appropriately respond to the new challenges of online violence against women journalists. It recommends that these laws should be amended to explicitly apply to online harassment, so as not to create room for doubt as to the extension of their application, and that they should:

- Include indirect communication, such as the creation of fake social media accounts or photoshopped images of victims shared with third parties;
- Target online harassment that is sexual and/or sexist;
- Include language that addresses harassment campaigns perpetrated by multiple individuals; and
- Adopt tiered responses to punish online harassment of varying levels.[29]

Engaging with lawmakers to enhance protection

When the Domestic Violence Amendment Bill was first introduced in 2020 in South Africa, it gave some consideration to the role of technology in domestic violence. This sparked the interest of a diverse group of activists, technologists, policymakers, researchers, and feminists, who made submissions to Parliament.[30]

[27] Power Law, '*South African Human Rights Commission v Matumba*: Written Submissions,' (2021) (accessible here).
[28] Mariana Valante, 'Do we need laws to address non-consensual circulation of intimate images: the case of Brazil', 17 June 2018 (accessible here).
[29] Dart Centre for Journalism & Trauma, 'Journalism and Online Harassment' (2020) (accessible here).
[30] See T Power, New law protects women against online abuse' (2022) (accessible here).

This enabled a robust engagement with lawmakers on emerging issues and ultimately paved the way for more detailed and enhanced protection against various online threats in the Domestic Violence Amendment Act. For example:

- The expanded definition of **harassment** now encompasses various forms of online harassment, including repeated electronic communication, unauthorized access to electronic devices or accounts, monitoring or tracking of individuals without consent, sending abusive or degrading messages, sharing private information or abusive content with others, and unwelcome sexual communications.
- The definition of **sexual harassment** includes sending unwanted electronic communications of a sexual nature and protects against "outing" individuals based on their sexual orientation, gender, or gender expression.
- The revised definition of **electronic communications** in the context of harassment now encompasses digital audio, text, video, and images, as well as simulated and manipulated information. This expansion enables protection against the dissemination of non-consensual manipulated and deep fake images—videos or images altered to appear authentic.

This law reform process highlights the value of engaging with lawmakers on contemporary issues to ensure more meaningful protection against online harms.

4. DIGITAL SECURITY TACTICS

4.1. Personal protective techniques[31]

While no journalist should be responsible for preventing online violence or harassment against them, taking steps to manage one's digital profiles and making it more difficult for perpetrators to act against them can be an effective way to protect against such harms before they occur

- **Be conscious and cautious regarding the information you share with others**
  - Be careful not to give out your phone number, personal email address, identity numbers or location in both online and offline fora which could spread beyond your control and reach unintended audiences.
  - Be careful about not tagging your location in social media posts, at least until you have left it, and closely monitoring followers on personal accounts on which you may share more personal information.
  - Speaking to friends and family about not sharing images, videos, or other content online that provides sensitive information such as your location or your children's school.

[31] Much of the guidance provided here is courtesy of the Practical Guide for Women Journalists on How to Respond to Online Harassment, published by UNESCO, TrustLaw, the Thomson Reuters Foundation and the International Women's Media Foundation (accessible here).

Know what is out there and how to remove it

A quick online search of your name can be a useful tool to determine what information is currently available online about you and enable you to follow up with the hosts of any information you wish to have removed.

Keep in mind that once online, content can be rapidly shared, edited and stored on internet archive sites, so the most effective strategy is to prevent the information from getting online in the first place.

For more guidance see:

- The International Women's Media Foundation course, Keep it Private, which provides further guidance on how to protect one's data online,
- The Committee to Protect Journalists' (CPJ) detailed guide on how to remove data from the internet.

- **Consider the legal terms and conditions of the content you share:** Some social media and online platforms have conditions that enable the free use of any content posted online, enabling would-be attackers to reproduce or modify photos or other content you have shared online. Check the terms and conditions of the platforms you use and whether the settings on your account can be changed to prevent this kind of usage.

- **Secure all your accounts:** Online violence can sometimes take place through hacking or unauthorised access to your own accounts:

    - Protecting against these risks requires you to always use secure passwords which are regularly changed and saved in a secure password manager, use two-factor authentication (2FA) whenever possible, and be careful about sharing passwords with others.

    - Journalists should also educate themselves on phishing and malware to be able to identify such attempts and be careful to keep all software up to date, including browsers. Consider exploring encrypted email and document-sharing services as well as using encrypted messaging platforms.

    - One can also consider using Virtual Private Networks (VPNs) to mask your physical location and encrypt your connection to the internet, particularly when using public WiFi networks or networks shared with other people.

Account security tips

The Rory Peck Trust Digital Security Guide provides detailed guidance on account security along with Media Defence's Stay Safe Online Guide for Sub-Saharan African journalists.

4.2. Dealing with online violence

- It is important to emphasise the need to **document the messages** and communications you are receiving, both to share with others as well as in case of potential future legal action.

Documentation tips

See the IWMF's Know Your Trolls course for more information on how to identify the perpetrators of the abuse online and PEN America's guide on documenting online harassment here. While it may not be possible to document every incident of abuse, it can be important to capture the general trends as well as repeat offenders, any escalation over time, etc.

- Consider **reporting the abuse to your employer, family, friends**, and others who can provide support. Although this might be hard, it can be helpful to have others to lean on as well as to get advice from colleagues or others who may have experienced something similar.

Reporting tips

- See, for example, PEN America's guide on how to speak to your employer about online abuse.

- Consider **blocking the perpetrator**, logging off temporarily, or even closing your account in order to protect yourself from further violence.

- Do not hesitate to **seek psycho-social support** however it may be available. It is important to emphasise that although perpetrated online, such violence has very real and damaging real-world effects for its victims/survivors, and it is normal to experience these effects. Check whether your employer provides access to psycho-social support and consider reaching out to a professional who can assist.

Support tips

- See for example, CPJ's guide on protecting your mental health, Support tools for gender-based violence survivors, PEN America's Requesting and Providing Support, and Deconstruct: Online Gender Based Violence guidance on physiological support.

4.3. Reporting to online platforms

Another critical step in managing online violence which deserves further attention is reporting to the online platforms on which the content is shared. All platforms have standard terms of use, and if you can show that someone has violated those terms, you can have the content

removed and/or the person's account suspended or deleted, which prevents additional harm in future.

Support tips

- See PEN America's guide to reporting to platforms and Deconstruct: Online Gender Based Violence guidance on reporting to intermediaries for more detailed information about the requirements and steps for reporting content on each platform.

The difficulties of reporting to platforms

Unfortunately, many women journalists affected by this online violence report experiencing wholly ineffective responses from the digital platforms. Ferial Haffajee, an editor in South Africa, reported to UNESCO that she was "stonewalled" by Twitter (now X) when attempting to use the automated reporting system to report her abuse.[32]

Criticism has also gone further than individual cases to note that responses by the platforms are uneven, with proactive content moderation being notably poorer in countries outside of their major markets and in less prioritised languages due to a lack of contextual understanding and investment in content moderation capacity in their languages.[33]

For further guidance, as well as a list of other digital security resources, see the Practical Guide for Women Journalists on How to Respond to Online Harassment published by UNESCO, TrustLaw, the Thomson Reuters Foundation and the International Women's Media Foundation.

5. CONCLUSION

Digital attacks on journalists can occur in a wide range of formats, all with extensive impacts on a wide range of human rights that are protected and promoted by international human rights law. This module provides lawyers with a practical but introductory guide to considering strategies to counter and seek accountability for online violence against journalists, including through litigation, advocacy, and pre-emptive digital security tactics. Litigation can be a highly impactful way of security progressive jurisprudence and real remedies but is also most likely to be effective and successful when coupled with non-legal strategies such as public advocacy campaigns and efforts to improve the responsiveness of online platforms to such violence.

[32] UNESCO above 1 at p. 36.
[33] Id.