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

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

TABLE OF CONTENTS

MODULE 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.