Addressing Online Violence Against Women and Girls in the Commonwealth Africa Region

The Role of Bystanders

The Commonwealth

Addressing Online Violence Against Women and Girls in the Commonwealth Africa Region

The Role of Bystanders

The Commonwealth

Foreign, Commonwealth & Development Office

Commonwealth Secretariat
Marlborough House
Pall Mall
London SW1Y 5HX
United Kingdom

www.thecommonwealth.org

Published by the Commonwealth Secretariat.

Contents

Acknowledgements

The Commonwealth Secretariat acknowledges with gratitude the financial support of the United Kingdom Foreign, Commonwealth & Development Office to the Commonwealth Cyber Capability Programme.

The Report on *Addressing Online Violence Against Women and Girls in the Commonwealth Africa Region: The Role of Bystanders* is part of a series, which investigates the culpability of online bystanders in violence against women and girls in the cyberspace.

The Report was authored by Andrew Nkunika, IT Law Practitioner at Messrs Nkunika and Chipeta Legal Practitioners, Zambia; Neema Iyer, Artist and Founder of Pollicy; and Nondumiso Nsibande, gender specialist South Africa.

The Series was prepared under the general guidance of Dr Tawanda Hondora, Adviser and Head of Rule of Law Section Governance and Peace Directorate (GPD). Dr Nkechi Amobi, Senior Research Officer, Cyber Capability Programme, GPD, led and co-ordinated the review and editorial process of the report. Ms Emma Beckles, Programme Officer, GPD, and Mr Shakirudeen Ade Alade, Programme Coordinator, GPD, provided valuable feedback while Ms Helene Massaka, Programme Assistant, GPD, provided logistical and administrative support.

The team is grateful to Mrs Elizabeth Bakibinga-Gaswaga, former Legal Adviser Rule of Law Section, GPD, for conceptualising this research project.

The team is also grateful for the constructive feedback received from internal reviewer, Mr Justin Pettit Human Rights Adviser, Governance and Peace Directorate.

Executive summary

This report provides a summary of the phenomenon of online violence against women in various African Commonwealth member countries and describes the legal frameworks and their limitations and the challenges these present. The report also makes suggestions on how to tackle these issues in order to find solutions to the problem of online violence against women and girls.

The report provides detailed individual country summaries. The report provides detailed summaries for the following countries are: Botswana, Cameroon, Eswatini, Ghana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Nigeria, Rwanda, Seychelles, Sierra Leone, South Africa, Tanzania, The Gambia, Uganda and Zambia. The report also covers the constitutional, legislative and administrative arrangements which support each country's ability to fight online violence and how they deal with online bystanders.

Cultural and traditional norms and practices play a role in creating the vulnerability of women and girls to online violence and its perpetuation against them. These practices have been found to promote discrimination and should be eliminated especially for young girls who face additional forms of gender violence. There is a need for the adoption of best practice in relation to the protection of women and girls from violence.

There are some capacity deficiencies among various law enforcement, judicial and administrative officers and these need to be addressed by increasing capacity and training. There are some capacity deficiencies among various law enforcement, judicial and administrative officers and these need to be addressed by increasing staff and training.

1. Introduction to online violence against women and girls

In today's increasingly digital society, more and more people are spending significant amounts of time in online spaces. As a result, users themselves are bringing pre-existing prejudices and beliefs directly into these platforms.

Online gender-based violence itself has been defined as an action facilitated by one or more people that harms others based on their sexual or gender identity or by enforcing harmful gender norms, which is carried out by using the internet or mobile technology (Iyer et al., 2020).

While several reports have looked into the motivation behind and the impact of online gender-based violence, particularly on women (Henry and Powell, 2005), the nature of third parties, also known as bystanders and described by some as secondary perpetrators, has seen less study.

This study aims to provide more context on the phenomenon of online violence as instigated or perpetuated by bystanders in a number of African countries – namely, Botswana, Cameroon, Eswatini, Ghana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Nigeria, Rwanda, Seychelles, Sierra Leone, South Africa, Tanzania, The Gambia, Uganda and Zambia. The report also provides more nuance on available legal provisions as well as the literature on and the institutional framework in these jurisdictions.

1.1. Prevalence of online violence against women

Globally, violence against women and girls (VAWG), more specifically intimate partner violence, is the leading cause of death and disability in women. It is estimated that one in three women and girls have experienced some form of VAW (WHO, 2018). Various studies conducted in this area have focused largely on offline violence, but there is growing evidence that the advent and uptake of technology have served as a double-edged sword for women (EIU, 2020; Fairbern, 2020). While technology facilitates access and opportunities, connecting people globally, it also serves as a breeding ground for abusers to target women and girls online. Although online violence against women and girls (OVAWG), including the terminology, is a growing area of study, there have been attempts by the United Nations and other institutions to define the concept . The common thread in the definitions is that it is 'action by one or more persons perpetrated against a person on the basis of their gender but utilising Information and Communication Technology' (UN Special Rapporteur on VAW, 2018; ICRC, 2020). In 2020, the Economist Intelligence Unit (EIU) completed a study on the global prevalence of OVAWG; its findings show that 85 per cent of women globally have witnessed harassment and online violence from among 4,561 women surveyed in 51 countries,[1] with younger women more likely to personally experience online violence.

The same study shows stark differences in the prevalence of OVAWG by region, with Africa and the Middle East respectively leading at 91 and 98 per cent of women witnessing harassment and online violence. It also reveals that women in countries with institutionalised gender inequalities are far more likely to experience online violence. While countries are making attempts to counter online violence through policy and law reform initiatives, these efforts are still in their early stages. Of interest in this study is that 85 per cent of respondents reported that they had witnessed OVAWG towards other women. Additionally, more than 54 per cent of the women who had experienced OVAWG knew the perpetrator.

It can be deduced from this study and other related studies, such as a study funded by the

1 See *Measuring the prevalence of online violence against women*. https://onlineviolencewomen.eiu.com

United Nations Educational, Scientific and Cultural Organization (UNESCO) on violence against women journalists (Posetti and Shabbir, 2020), that online and offline violence are connected and should be seen as a continuum (UN Special Rapporteur on VAW, 2018). The Special Rapporteur on VAW confirms that gender-based violence is often reproduced, amplified and, in some instances, redefined using information and communication technology (ICT). Undoubtedly, the internet has given rise to new forms of VAW.

1.2. Bystander interventions and theoretical underpinnings

Bystanders have been defined as persons who observe an act of violence or problematic behaviour but who are not its direct perpetrators or victims (Powell, 2011). The bystander effect, a situation whereby individuals in crowds choose not to intervene because no other persons are intervening, is the dominant explanation for why bystanders act the way they do.

Meanwhile, to combat the bystander effect, bystander intervention is an approach being pursued mainly in situations of offline violence (Fairbern, 2020). Institutions have focused on bystander intervention programmes aimed at training peers to intervene if they witness violence or assault (Senn et al., 2018). Bystander intervention refers to those witnessing, but not directly involved in, an event.

Others unpack the term to mean that the bystander notices the event, sees it as a problem requiring intervention and decides whether to take action and be a part of the solution and whether he or she has the capacity and skills to intervene (Banyard, 2011; Powell, 2011). In the context of online violence, this can be interpreted to mean that an online bystander identifies a problem, meaning that there is a level of awareness or an appreciation that there is a problem; assumes responsibility to act or has empathy towards the victim; and has the confidence to interrupt or speak out against the behaviour.

In a seminal piece of research in 1970, Latané and Darley formulated a theory to describe the bystander effect, involving three steps: audience inhibition – how the presence of other people inhibits bystander intervention because of the fear that other bystanders will negatively evaluate their behaviour; social influence – how the presence of others inhibits involvement when a bystander sees that no one else is helping; and diffusion of responsibility – how the psychological cost associated with non-intervention is reduced for individual bystanders.

In Africa, research conducted on the online bystander effect/intervention is based mainly on adolescents in campus settings. This is related to the exposure of this particular age range (14–29) to the use of technological facilities (Olasanmi et al., 2020). There is, therefore, a huge gap in research into the bystander effect in OVAWG in Africa, and into strategies to combat it.

In addition, most reports, laws and articles related to online violence focus on child sexual abuse and bullying among young people and adolescents, online or offline. While in many African countries the right to dignity and freedom from harassment is enshrined in the constitution, there is limited protection for women and girls, especially in online spaces. OVAWG is often trivialised, minimised and unpunished by the relevant authorities (Iyer et al., 2020). The laws that exist often bundle cybersecurity and cybercrime provisions together, with pornography and fraud thrown in under the same heading. Without a woman-centric evaluation during the preliminary processes of such law-making, partially attributable to the absence of women in legislative positions and in activism, laws end up insufficiently responsive to the needs of victims of OVAWG.

1.3. Why the term 'online bystander' may be problematic

The definition of the term 'bystander' in the context of OVAWG is problematic for several reasons:

- **Lack of clarity**. When using the word 'bystander', it is not clear whether a bystander is someone who simply views a piece of content or whether it is a secondary perpetrator of online violence, retweeting, sharing, disseminating or commenting on a problematic piece of information on a digital platform. The algorithms on several of these platforms are programmed to amplify information or content that people interact with, so even liking or commenting

on a post, whether in support or against, can further amplify the violence and retraumatise the victim.

- **Exoneration**. Using the term 'bystander' instead of secondary perpetrator removes blame from the person who takes action to like, share or comment on a piece of content, whereby, as previously explained, this serves to amplify the offending piece of content.
- **Everybody and nobody become the perpetrator**. It is difficult to identify who the primary or secondary perpetrators of violent acts are when carried out online due to the anonymity which cyberspace affords users. When content is shared through screenshots (within the same or on other platforms), likes, retweets and comments, etc., everyone and no one become the perpetrator. In a study conducted by Pollicy on online violence against women, up to 90 per cent of respondents were unaware of the identity of the perpetrator of the violence inflicted on them (Iyer et al., 2020).
- Regardless of the nomenclature that is used, the frequent absence of effective legal and regulatory frameworks to deal with this behaviour, however referred to, is the biggest problem facing jurisdictions. A lack of legal recognition means that enforcement and sanction for wrongful or criminal conduct tends to be absent. This vacuum in the law means that perpetrators of online violence tend to escape justice. Legal technicalities should not exist and should not be allowed to continue to exist once such legal loopholes or deficiencies have been identified.

1.4. Methodology and scope of the study

This report is a review of laws, policies and strategies used when dealing with cybercrimes, particularly on the topic of OVAWG and the bystander. This report is further supplemented by findings from interviews held with legal drafters and other relevant stakeholders working in the field of policy and law. The literature review focused on the aforementioned documents. There have been few studies conducted on OVAWG and, more importantly, on the online bystander.

2. Country analysis

2.1. Uganda

Under the Constitution of the Republic of Uganda, provision is made for the right to freedom of expression, gender equality, affirmative action for women and non-discrimination based on sex. Article 21 [(1) and (2)] under Chapter 4 of the Constitution explicitly sets out that no one may be discriminated against on the 'ground of sex, race, colour, ethnic origin, tribe, birth, creed or religion, or social or economic standing, political opinion or disability'. Article 24 provides for respect for human dignity and protection from inhuman treatment.

Constitution

Article 21 Equality and freedom from discrimination

(1) All persons are equal before and under the law in all spheres of political, economic, social and cultural life and in every other respect and shall enjoy equal protection of the law.

. (2) Without prejudice to clause (1) of this article, a person shall not be discriminated against on the ground of sex, race, colour, ethnic origin, tribe, birth, creed or religion, or social or economic standing, political opinion or disability.

In addition to the Constitution, the law regulating cyberspaces in Uganda is the Computer Misuse Act 2011. Sections 23, 24, 25 and 26 of this Act criminalise child pornography, cyber harassment, offensive communication and cyberstalking, respectively. However, the Act makes no mention of online bystanders and it fails to recognise or assign roles or culpability to bystanders in cybercrime. It also makes no specific mentions of OVAWG (Wagabaza, 2019).

Computer Misuse Act

23. Child pornography.

(1) A person who —

(a) produces child pornography for the purposes of its distribution through a computer;

(b) offers or makes available child pornography through a computer;

(c) distributes or transmits child pornography through a computer;

(d) procures child pornography through a computer for himself or herself or another person; or

(e) unlawfully possesses child pornography on a computer, commits an offence.

(2) A person who makes available pornographic materials to a child commits an offence.

(3) For the purposes of this section "child pornography" includes pornographic material that depicts —

(a) a child engaged in sexually suggestive or explicit conduct;

(b) a person appearing to be a child engaged in sexually suggestive or explicit conduct; or

(c) realistic images representing children engaged in sexually suggestive or explicit conduct.

(4) A person who commits an offence under this section is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

24. Cyber harassment.

(1) A person who commits cyber harassment is liable on conviction to a fine not exceeding seventy two currency points or imprisonment not exceeding three years or both.

(2) For purposes of this section cyber harassment is the use of a computer for any of the following purposes —

(a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent;

(b) threatening to inflict injury or physical harm to the person or property of any person; or

(c) knowingly permits any electronic communications device to be used for any of the purposes mentioned in this section.

25. Offensive communication.

Any person who willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right

of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor and is liable on conviction to a fine not exceeding twenty four currency points or imprisonment not exceeding one year or both.

26. Cyber stalking.

Any person who willfully, maliciously, and repeatedly uses electronic communication to harass another person and makes a threat with the intent to place that person in reasonable fear for his or her safety or to a member of that person's immediate family commits the crime of cyber stalking and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

Recommendations

While Uganda has passed several laws and policies with the aim of improving the status of women, including the National Action Plan on Women, the Gender Policy Act, the Domestic Violence Act and the Female Genital Mutilation Act, none focuses specifically on online and internet communications and the harms accompanying them. The exception is the Anti-Pornography Act 2014, which was passed to define and create the offence of pornography, to provide for the prohibition of pornography and to establish the Pornography Control Committee. However, the general, overarching nature of the provisions of this Act means it has often been used to punish women, despite them disproportionately being victims of non-consensual intimate image-sharing (WOUGNET et al., 2021).

This therefore points to the need to develop new legislation specifically providing for and addressing the needs of women online. This would require the unbundling of cybercrime and cybersecurity from the Computer Misuse Act and may necessitate the amendment of laws such as the Gender Policy Act and the Domestic Violence Act to include provisions expressly criminalising the use of digital technology to facilitate violence against women and girls.

In addition, although Section 24 of the Computer Misuse Act criminalises cyber-harassment, it is silent on the culpability of bystanders. Furthermore, while Section 24 (2) (c) provides that cyber-harassment also includes knowingly permitting the use of any electronic communications device for any of the purposes mentioned in the section, the provisions are unclear as to whether sharing, liking and commenting on – or even viewing and failing to report – cyber-harassment amount to actual commission of the crime. The Act will need to be amended to account for this deficiency.

2.2. Tanzania

Under the Constitution of Tanzania of 1977, as amended in 2005, there are explicit provisions regarding the basic rights and freedoms of Tanzania's citizens. From Article 12 to Article 32 under Part III of Chapter 1, the Constitution provides for the basic rights and duties of Tanzanian citizens including the right to equality, life and freedom of conscience.

Article 12 (1) of the Constitution provides that all human beings are born free and are all equal. Subsection (2) of the same article further provides that every person is entitled to recognition of and respect for his or her dignity. In addition, Article 13 (1) stipulates that all persons are equal before the law and are entitled, without any discrimination, to protection and equality before the law.

Under Article 9, the Tanzanian Constitution spells out as one of its objectives the protection of human dignity in accordance with the Universal Declaration of Human Rights.

Part II of Tanzania's Cybercrimes Act of 2015 (the law applicable to cyberspace regulation) spells out and criminalises a variety of acts that may be committed with the use of ICT. Sections 13 and 14 criminalise the publishing of child pornography and ordinary pornography. Sections 20 and 23 of the Act further criminalise the sending of unsolicited messages and cyberbullying, respectively. In a similar vein, Sections 26 and 27 criminalise attempts and conspiracies to commit any action defined as an offence under the Act.

Cybercrimes Act

14. (1) A person shall not publish or cause to be published through a computer system or through any other information and communication technology: (a) pornography; or (b) pornography which is lascivious or obscene.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction, in the case of publication of:

(a) pornography, to a fine of not less than twenty million shillings or to imprisonment for a term of not less than seven years or to both; and

(b) pornography, which is lascivious or obscene, to a fine of not less than thirty million shillings or to imprisonment for a term of not less than ten years or to both.

20. (1) A person shall not, with intent to commit an offence under this Act -
(a) initiate the transmission of unsolicited messages; (b) relay or retransmit unsolicited messages, or (c) falsify header information in unsolicited messages;

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than three million shillings or three times the value of undue advantage received, whichever is greater or to imprisonment for a term of not less than one year or to both. (3) For the purpose of this section, "unsolicited messages" means any electronic message which is not solicited by the recipient.

23. (1) A person shall not initiate or send any electronic communication using a computer system to another person with intent to coerce, intimidate, harass, or cause emotional distress.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine of not less than five million shillings or to imprisonment for a term of not less than three years or to both.

Recommendations

Unlike in Uganda, in Tanzania there are no specific laws aimed specifically at combating gender-based violence or VAW beyond the general provisions of the Constitution and other laws criminalising acts of violence in society. There is therefore a need to develop specific laws targeted at criminalising VAW in society. These would need to cover offline and online acts and related areas of VAW reflecting the advancement of technology adoption today.

The Tanzania Cybercrimes Act also does not define who a bystander is or the extent of their culpability under the Act, but Section 23 criminalises cyberbullying. It is unclear if Section 23 (1) refers solely to text or also to audio-visual messages when it mentions electronic communication, and if this includes sharing and liking as well. The Act therefore needs to be amended to reflect this.

2.3. Kenya

The rights accruable to Kenyan citizens are set out under Chapter 4 of the Kenyan Constitution of 2010, titled The Bill of Rights. Article 27 provides for equality and freedom from discrimination for men and women equally.

Sections 14–46 of Kenya's Computer Misuse and Cybercrimes Act 2018 criminalises child pornography, cyber-harassment and the unwanted distribution of obscene and intimate images, under Sections 24, 27 and 37, respectively.

Computer Misuse and Cybercrimes Act

27. Cyber-harassment

(1) A person who, individually or with other persons, willfully communicates, either directly or indirectly, with another person or anyone known to that person, commits an offence, if they know or ought to know that their conduct —
(a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property; or (b) detrimentally affects that person; or (c) is in whole or part, of an indecent or grossly offensive nature and affects the person.

(2) A person who commits an offence under subsection (1) is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both

37. Wrongful distribution of obscene or intimate images

A person who transfers, publishes, or disseminates, including making a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate or obscene image of another person commits an offence and is liable, on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both.

While Kenya has laws aimed at curbing violence against women, such as the Sexual Offences Act, the National Gender and Equality Commission Act and the Kenya National Commission on Human Rights Act, like the Computer Misuse and Cybercrimes Act these do not envisage the creation of new crimes carried out against women in digital spaces (Munyua, 2013).

Recommendations

There is a need to amend the provisions of the existing acts designed to address VAW to include novel, digital and technology-facilitated variations of existing acts of VAW such as cyberstalking, cyber-intimidation and cyber-assault.

In order to properly address potential acts of violence by online bystanders, the identity of persons described to be bystanders and their culpability needs to be properly delineated under these laws and under the Computer Misuse and Cybercrimes Act. This may necessitate an expansion of the provisions of Section 27 of the Act, which criminalises cyber-harassment. The wide variety of direct and indirect interactions made possible by technology in online spaces and on social media platforms makes it necessary for the Act to expressly spell out the scope of the crime.

2.4. Nigeria

Fundamental rights in Nigeria are set out under Chapter IV of the Constitution 1999 as amended. These rights include the right to life, privacy and dignity, among others.

In addition to these overarching provisions, Nigeria's Cybercrime (Prohibition, Prevention, etc.) Act 2015 outlines the offences of child pornography and cyberstalking as well as phishing and spamming.

In addition to the above, the Violence Against Persons (Prohibition) Act of 2015, applicable in the Federal Capital Territory and in states that have domesticated it, in addition to famously (re)defining rape as an act capable of commission by any person, thereby removing its definition as a gendered act, criminalises stalking and harassment. However, the provisions of the Violence Against Persons (Prohibition) Act are mainly applicable to offline settings and it is therefore ill-equipped to deal with OVAWG. Although the Act contains noteworthy provisions, including the notion of compensation for victims, these are accessible only by persons living in the 18 states where it has been domesticated (Ewepu and Eromosele, 2021).

Recommendations

Nigeria's federal system of government makes it extremely difficult to pass comprehensive and effective laws on the subject of OVAWG. While it is possible to pass a comprehensive law expressly criminalising online bystander violence and cyber variants of criminal offences at the national level, the semi-autonomous nature of states in Nigeria means that these need to be modified to make them applicable at the state level. This then creates an opportunity for state lawmakers to remove pertinent sections of each Act they consider undesirable, or not pass the law at all. To properly address this, there is a need to consider a constitutional amendment to bring the regulation of offences identified as disproportionately affecting women onto the exclusive list,[2] in response to their severity and in accordance with the fundamental human rights of women to dignity, privacy, public participation and freedom from discrimination and harassment. Another means to achieve this would be through strategic litigation aimed at establishing judicial precedent via court declarations on the need to place legislation on certain forms of violence, online and offline, that disproportionately affect minority groups such as women on the exclusive list.

Additionally, the provisions of Nigeria's Cybercrime Act have proven inadequate in dealing with acts of OVAWG such as revenge pornography, despite the broad sections that can generally be read to be applicable. The case of Attorney-General of the Federation v Olubunmi Ayan[3] is the only one on record resulting in the conviction of the defendant in a revenge pornography case. On the other hand, relevant sections of the Cybercrime Act, particularly Section 24, have achieved notoriety because of their use by the government to facilitate the arrest of journalists, leading to several human rights litigations to expunge and declare this unconstitutional (Babalola, 2020).

Cybercrime (Prohibition, Prevention, etc.) Act

. 24. Any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that -

2 The exclusive list refers to areas or sectors of governance over which only the federal government can make laws.

3 FHC/AD/17C/2017.

(a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or

(b) he knows to be false, for the purpose of causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent:

commits an offence under this Act and shall be liable on conviction to a fine of not more than N7,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.

(2) Any person who knowingly or intentionally transmits or causes the transmission of any communication through a computer system or network -
(a) 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;

(b) containing any threat to kidnap any person or any threat to harm the person of another, any demand or request for a ransom for the release of any kidnapped person, to extort from any person, firm, association or corporation, any money or other thing of value; or

(c) containing any threat to harm the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, to extort from any person, firm, association, or corporation, any money or other thing of value:

commits an offence under this Act and shall be liable on conviction--
(i) in the case of paragraphs (a) and (b) of this subsection to imprisonment for a term of 10 years and/or a minimum fine of N25,000,000.00; and

(ii) in the case of paragraph (c) and (d) of this subsection, to imprisonment for a term of 5 years and/or a minimum fine of N15,000,000.00.

(3) A court sentencing or otherwise dealing with a person convicted of an offence under subsections (1) and (2) may also make an order, which may, for the purpose of protecting the victim or victims of the offence, or any other person mentioned in the order, from further conduct which--
(a) amounts to harassment; or

(b) will cause fear of violence, death, or bodily harm; prohibit the defendant from doing anything described/specified in the order.

(4) A defendant who does anything which he is prohibited from doing by an order under this section, commits an offence and shall be liable on conviction to a fine of not more than N10,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.

(5) The order made under subsection (3) of this section may have effect for a specified period or until further order and the defendant or any other person mentioned in the order may apply to the court which made the order for it to be varied or discharged by a further order.

(6) Notwithstanding the powers of the court under subsections (3) and (5), the court may make an interim order for the protection of victim(s) from further exposure to the alleged offences.

The side-effect of the success of these cases is that there could be irreparable harm to the success of future cases against instances of OVAWG in Nigeria. The need for balance in terms of preserving human rights advocacy harmed by the overly broad application of the aforementioned Section 24 and maintaining the potential benefit of the section to women's rights online requires careful consideration. One way to maintain this balance is through the enactment of specific regulations targeting instances of OVAWG under the Act using specific terms, or the enactment of fresh legislation that would do so.

In the Act's current state, the additional criminalisation of bystander violence in cybercrime would further exacerbate injustice against persons who might have encountered online violence in social media spaces. New regulation is thus needed to properly delimit the scope of the existing legislation.

2.5. Rwanda

Under the Constitution of Rwanda of 2003, as amended in 2008, there are applicable provisions that outline the fundamental human rights and rights and duties of citizens. These are set out under Title II of the Constitution. Article 11 provides against discrimination based on ethnic origin, tribe, clan, colour, sex, region, social origin, religion or faith, opinion, economic status, culture and language, among others.

Rwanda also passed the Law on Prevention and Punishment of Cybercrimes in 2018, which criminalises several classifications of cybercrime. Section 4 specifically criminalises offences related to the content of computer and computer systems, such as the publication of pornographic material and cyberstalking, under Articles 34 and 35, respectively, albeit with no mention of the roles of bystanders despite the extensive provisions.

Cybercrime Law

Article 34: Publication of pornographic images through a computer or a computer system

Any person who:

1° publishes or causes to be published pornography through a computer system or through any other means of information and communication technology;

2° proposes, grooms or solicits, through a computer or a computer system or any network, to meet a child for the purpose of engaging in sexual activities with the child;

commits an offence.

Article 35: Cyber-stalking

Any person who, intentionally, uses a computer or a computer system to harass or threaten with the intent to place another person in distress or fear through one of the following acts when:

. 1° he/she displays, distributes or publishes indecent documents, sounds, pictures or videos;

. 2° in bad faith, he/she takes pictures, videos or sounds of any person without his/her consent or knowledge

. 3° he/she displays or distributes in a manner that substantially increases the risk of harm or violence to any other person;

. commits an offence.

Recommendations

In addition to unbundling cybersecurity and cybercrime provisions, there is a need to define the scope and role of the online bystander to be able to identify their responsibility in acts of OVAWG.

2.6. Ghana

Human rights protections and freedoms are highlighted under the Constitution of the Republic of Ghana 1992 as amended in 1996, specifically under Articles 12 (2) and 18 (2). Article 12 (2) provides that every person in Ghana, regardless of race, place of origin, political opinion, colour, religion, creed or gender, shall be entitled to the fundamental human rights and freedoms of the individual.

The Cybersecurity Act 2020 makes provision for the regulation of crime in cyber spaces as well as cybersecurity in the country. Sections 62 to 66 provide for the online protection of children by criminalising acts such as the cyberstalking of a child and the taking of indecent images of children. Sections 66 (1), 67 and 68 provide specifically for sexual crimes – namely, sexual extortion, the non-consensual sharing of intimate images, and threats to distribute prohibited images or visual recordings.

However, the Act remains silent on non-sexual variants of cyberbullying and harassment and makes no mention of a penalty awardable against bystanders.

Additionally, Section 123 of the Electronic Transacts Act 2008, provides that except as provided for in the Act, an offence under a law which is committed in whole or in part by use of an electronic medium or in electronic form is deemed to have been committed under that Act and the provisions of that Act apply with the necessary modifications. This provision ensures that the scope of the law relating to cybercrimes is extended to other offences which would otherwise not be captured when committed using electronic means. These may include offences relating to online violence against women and girls.

Recommendations

While it is commendable that the Act makes provision for the protection of children online, there is also a need for laws to adequately challenge the gendered nature of OVAWG. This could be done by unbundling the cybercrime and cybersecurity aspects present in the Act and further separating the parts designed to criminalise online violence

and child sexual abuse and OVAWG. Policy-makers should bear in mind while developing policies and laws that women are disproportionately victims of sexual abuse online. In addition, it is important to address non-sexual variants of cyber abuse, such as harassment and trolling. In designing laws targeting OVAWG, it is important to clarify the terms being used; in defining online bystander violence, it would be useful to clarify who such bystanders are and the extent of their culpability.

2.7. Zambia

Zambia's Constitution provides for protection from discrimination as well as protecting the rights of women and children.

Constitution

Article 23

23. (1) Subject to clauses (4), (5) and (7), no law shall make any provision that is discriminatory either of itself or in its effect.

(2) Subject to clauses (6), (7) and (8), no person shall be treated in a discriminatory manner by any person acting by virtue of any written law or in the performance of the functions of any public office or any public authority.

(3) In this Article the expression "discriminatory" means, affording different treatment to different persons attributable, wholly or mainly to their respective descriptions by race, tribe, sex, place of origin, marital status, political opinions colour or creed whereby persons of one such description are subjected to disabilities or restrictions to which persons of another such description are not made subject or are accorded privileges or advantages which are not accorded to persons of another such description.

(4) Clause (1) shall not apply to any law so far as that law makes provision --

(a) for the appropriation of the general revenues of the Republic;

(b) with respect to persons who are not citizens of Zambia;

(c) with respect to adoption, marriage, divorce, burial, devolution of property on death or other matters of personal law;

(d) for the application in the case of members of a particular race or tribe, of customary law with respect to any matter to the exclusion of any law with respect to that matter which is applicable in the case of other persons; or

(e) whereby persons of any such description as is mentioned in clause (3) may be subjected to any disability or restriction or may be accorded any privilege or advantage which, having regard to its nature and to special circumstances pertaining to those persons or to persons of any other such description, is reasonably justifiable in a democratic society.

Article 23 (4) (c) and (d) creates a loophole through which traditional practices may be used to discriminate against others, especially women and children.

Zambia recognises online bystanders as role occupants in cybercrime or cybersecurity. The Zambia Police Service has, on several occasions, detected online crime through devices and recordings from online bystanders. Zambia does not, however, have a formal policy framework for the recognition of online bystanders. Consequently, it has not published a national strategy and stakeholder map on online bystanders in cybercrime. It does have a National ICT Policy but this is outdated and needs to be replaced. The Zambia Information and Communication Technologies Authority is responsible for the enforcement of Zambia's cyber laws and for engagement with stakeholders on various issues, including cyberbullying and online protection, which also encompasses matters relating to online bystanders.

Zambia has put in place a number of cyber laws aimed at preventing crimes against women and children as special groups. The major law that Zambia has passed is the Cyber Security and Cyber Crimes Act of 2021. This law broadly covers cybercrime, including specific provisions relating to child online protection. The country therefore has in place laws that can be relied upon for the online protection of women and children although it lacks a specific framework for addressing online bystanders in the cyber environment. The Cyber Security and Cyber Crimes Act of 2021 provides as follows:

Cyber Security and Cyber Crimes Act

Prohibition of pornography

56. (1) A person shall not produce or participate in the production of pornography using a computer system.

(2) A person convicted of an offence under subsection (1) is liable, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or both.

(3) A person who knowingly —

(a) produces pornography for the purpose of its distribution for profit through a computer system commits an offence and is liable on conviction to a fine not exceeding one million penalty units or to imprisonment for a period not exceeding ten years, or to both; or

(b) offers, circulates, or makes available, pornography through a computer system commits an offence and is liable on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

Child pornography

57. (1) A person commits an offence if that person knowingly —

(a) produces child pornography for the purpose of its distribution through a computer system;

(b) sells or makes available any pornography to a child through a computer system;

(c) compels, invites or allows a child to view pornography through a computer system intended to corrupt a child's morals;

(d) offers or makes available child pornography through a computer system;

(e) distributes or transmits child pornography through a computer system;

(f) procures and obtains child pornography through a computer system for oneself or for another person;

(g) possesses child pornography in a computer system or on a computer data storage medium; or

(h) obtains access, through information and communication technologies, to child pornography.

(2) A person convicted of an offence under subsection (1) is liable to imprisonment for a period not less than fifteen years.

(3) Subsections (1)(d) to (h) do not apply to a person performing a bona fide law enforcement function.

Child solicitation

58. (1) A person commits an offence if that person —

(a) uses a computer system to meet a child for the purpose of committing a sexual related crime;

(b) communicates with a child through a computer system for the purpose of making it easier to procure the child to engage in sexual activity with that person;

(c) attracts a child for the purpose of making it easier to procure the child to engage in sexual activity with that person;

(d) attracts a child for the purpose of making it easier to procure the child to engage in sexual activity with another person; or

(e) recruits a child to participate in pornographic performances that is intended to be produced or recorded with or without the intent to distribute such material through a computer system or computer network;

(2) A person convicted of an offence under subsection (1) is liable to imprisonment for a period not exceeding fifteen years.

Obscene matters or things

59. (1) A person commits an offence under subsection (1) is liable to imprisonment for a period not exceeding fifteen years —
(a) makes, produces or has in the persons possession any one or more obscene, drawings, paintings, pictures, images, posters, emblems, photographs, videos or any other object tending to corrupt morals; or

(b) imports, conveys or exports, or causes to be imported, conveyed or exported, any such matters or things, or in any manner whatsoever puts any of them in circulation; or

(c) carries on or takes part in any business, whether public or private, concerned with any such matters or things, or deals in any such matters or things in any manner whatsoever, or distributes

any of them, or exhibits any of them publicly, or makes a business of lending any of them;

(d) advertises or makes known by any means whatsoever with a view to assisting the circulation of, or traffic in, any such matters or things, that a person is engaged in any of the acts referred to in this section, or advertises or makes known how, or from whom, any such matters or things can be procured either directly or indirectly through a computer system; or

(e) publicly exhibits any indecent show or performance or any show or performance tending to corrupt morals through a computer system.

(2) A person convicted of an offence under subsection (1) is liable to a fine not exceeding ten thousand penalty units.

(3) A prosecution for an offence under this section shall not be instituted without the written consent of the Director of Public Prosecutions.

Hate speech

65. A person who, using a computer system, knowingly without lawful excuse, uses hate speech commits an offence and is liable, on conviction, to a fine not exceeding five hundred thousand penalty units or to imprisonment for a period not exceeding two years, or to both.

The highlighted sections in the Cyber Security and Cyber Crimes Act may be applied to matters relating to online bystanders in relation to the matters specified in the respective provisions.

Zambia has been increasing its capacity-building for law enforcement to address the challenges and issues relating to online bystanders in the cyber environment. The training programmes undertaken tend to focus on child online protection and the protection of women against violence. However, no specific facilities and training programmes have been established to deal with issues arising from online bystanders in the cyber environment.

Zambia has not established relationships with service and application providers concerning online bystanders. The country does engage with stakeholders in the ICT sector relating to various themes on online safety. No awareness-raising activities have been held regarding cybercrime with a focus on online bystanders, which has for the most part remained an area of little focus because of its relative novelty as a subject of discourse. Zambia has developed interventions for child online protection but these also do not have a view to online bystanders. Zambia does not have in place targeted technical and infrastructure security to address issues related to online bystanders.

Recommendations

Although Zambia has laws partially addressing child online protection and the protection of women, the country lacks substantive legislation, regulations and procedures for online bystanders. There is a need for Zambia to enhance its legal framework by providing for specific good Samaritan legislation and for the enhanced protection of women online. Zambia also needs to establish formal channels for collaboration and co-operation of the various stakeholders to effectively address OVAWG and other forms of cybercrime. The country also needs to develop and publish a national strategy and stakeholder map on online bystanders in cybercrime.

More capacity-building of the various stakeholders involved in law enforcement, online protection and the adjudication of various cases brought before the courts and tribunals will ensure these stakeholders are fully competent to deal with the issues presented before them. This is critical especially when taking into account the possibility of litigation involving the various cyber laws in place in the country.

2.8. Sierra Leone

Sierra Leone has overcome many of the challenges it has faced in its post-war period and has been making strides in various areas of its development, including in ICT. The Office of National Security was established by Act of Parliament in 2002. The country has experienced various challenging security threats, especially related to the Internet and related domains. This in turn has prompted the development of improved responses to online threats at various levels.

The 1991 Constitution of Sierra Leone provides for protection from discrimination.

Constitution

27. Protection from discrimination

(1) Subject to the provisions of subsection (4), (5) and (7), no law shall make any provision which is discriminatory either of itself or in its effect.

(20) Subject to the provisions of subsections (6), (7) and (8), no person shall be treated in a discriminatory manner by any person acting by virtue of any law or in the performance of the functions of any public office or any public authority.

(3) In this section the expression "discriminatory" means affording different treatment to different persons attributable wholly or mainly to their respective descriptions by race, tribe, sex, place of origin, political opinions, colour or creed whereby persons of one such description are subjected to disabilities or restrictions to which persons of another such description are not made subject, or are accorded privileges or advantages which are not accorded to persons of another such description.

(4) Subsection (1) shall not apply to any law so far as that law makes provision —
(a) for the appropriation of revenues or other funds of Sierra Leone or for the imposition of taxation (including the levying of fees for the grant of licences); or

(b) with respect to persons who are not citizens of Sierra Leone; or

(c) with respect to persons who acquire citizenship of Sierra Leone by

registration or by naturalization, or by resolution of Parliament; or

(d) with respect to adoption, marriage, divorce, burial, devolution of property on death or other interests of personal law; or

(e) for the application in the case of members of a particular race or tribe or customary law with respect to any matter to the exclusion of any law with respect to that matter which is applicable in the case of other persons; or

(f) for authorising the taking during a period of public emergency of measures that are reasonably justifiable for the purpose of dealing with the situation that exists during that period of public emergency; or

(g) whereby persons of any such description as mentioned in subsection (3) may be subjected to any disability or restriction or may be accorded any privilege or advantage which, having regard to its nature and to special circumstances pertaining to those persons or to persons of any other such description, is reasonably justifiable in a democratic society; or

(h) for the limitation of citizenship or relating to national registration or to the collection of demographic statistics.

(5) Nothing contained in any law shall be held to be inconsistent with or in contravention of subsection (1) to the extent that it makes provision with respect to qualifications for service as a public officer or as a member of a defence force or for the service of a local government authority or a body corporate established directly by any law or of membership of Parliament.

(6) Subsection (2) shall not apply to anything which is expressly or by necessary implication authorised to be done by any such provisions of law as is referred to in subsection (4) or (5).

(7) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision whereby persons of any such description as is mentioned in subsection (3) may be subjected to any restriction of the rights and freedoms guaranteed by sections 18, 22, 24, 25 and 26 being such a restriction as is authorised by subsection (3) of section 18, subsection (2) of section 22, subsection (5) of section 24, subsection (2) of section 25 or subsection (2) of section 26, as the case may be.

(8) The exercise of any discretion relating to the institution, conduct or discontinuance of civil or criminal proceedings in any court that is vested in any person under or by this Constitution or any other law shall not be enquired into by any Court on the grounds that it contravenes the provision of subsection (2).

The constitutional provision relating to non-discrimination is generally similar to that of the other countries under review by virtue of the colonial heritage of these nations, and so the challenges with the provisions are similar, as are the solutions to these challenges.

Sierra Leone recognises online bystanders as role occupants in cybercrime or cybersecurity. This is evident from the fact that the process leading

up to the enactment of legislation on cybercrime included discussion on the protection of women and children online, and cyberbullying and online protection have been discussed in various other contexts as well. This recognition has, however, not been significant, as government policy in the area of ICT has focused mainly on public infrastructure and data as opposed to the protection of individuals, as seen in government policy towards cybersecurity and data protection.

The Sierra Leone Police has demonstrated a capacity to detect online crime using various investigative techniques. For example, police have been trained in various criminal investigation techniques and, with the enactment of the Cyber Security and Cyber Crimes Act of 2021, are learning to prosecute cybercrimes, which are a new type of crime.

Although Sierra Leone recognises online bystanders as role occupants in cybercrime and cybersecurity, the country does not have a formal policy framework for the recognition of online bystanders. Its draft National Cyber Security and Data Protection Strategy for the period 2017–2022 has various thematic areas and addresses a number of specific issues, including the protection of citizens online. Sierra Leone has not published a national strategy and stakeholder map on online bystanders in cybercrime but has continued to make efforts to develop more comprehensive strategies for the online protection of persons.

Sierra Leone's Cyber Security and Cyber Crimes Act of 2021 covers cybercrime broadly, including specific provisions relating to child online protection. These include measures relating to the protection of persons in cyberspace. The Act also provides for National Cyber Security Advisory Council, which is responsible for the implementation and development of national cybersecurity legal frameworks in Sierra Leone. The Act also provides for various offences, such as offences related to unauthorised access to computers, unauthorised access to a protected system, unauthorised data interception, unauthorised data interference, unauthorised system interference, misuse of devices, computer-related forgery, computer fraud, identity theft and impersonation, cyberstalking and cyberbullying, online child sexual abuse, and racist and xenophobic offences. The offences contained in the Act may to a great extent be used to deal with issues relating to online bystanders. Some of the specific provisions are as follows:

Cyber Security and Cyber Crimes Act

Cyber stalking and cyber bullying

35. (1) A person, including a corporation, partnership, or association, who individually or with another person, willfully and repeatedly communicates, either directly or indirectly, with another person, if he knows or ought to have known that his conduct -

(a) is likely to cause that person apprehension or fear of violence to him or damage or loss on his property; or

(b) detrimentally affects that person,

commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

(2) A person, including a corporation, partnership, or association, who knowingly or intentionally sends a message or other matter by means of a computer system or network that —

(a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or

(b) he knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent,

commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

(3) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act -

(a) for the purpose of preventing or detecting crime;

(b) in compliance of and in accordance with the terms of a judicial order issued or in exercise of any power under this Act or any law; or

(c) which is in the interest of the public.

Online child sexual abuse
38. (1) A person, including a corporation, partnership, or association, who, intentionally –

(a) possesses, distributes, produces, views, downloads, transmits, disseminates, circulates, delivers, exhibits, lends for gain, exchanges, barters, sells or offers for sale, lets on hire or offers to let on hire, prints, photographs, copies, provides location, requests for, offers in any other way, or makes available in any way child pornography through a computer system or storage data medium; or

(b) acquiesces a child's participation in pornography, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

(2) A person, including a corporation, partnership, or association, who intentionally poses, grooms or solicits, through any computer system or network, to meet a child for the purpose of -

(a) engaging in sexual activity with the child;

(b) engaging in sexual activity with the child

where-
(i) coercion, inducement, force or threat is used;

(ii) a recognised position of trust, authority or influence over the child, including within the family is abused; or

(iii) a child's mental or physical disability or situation of dependence is abused,

commits an offence and shall be liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

(3) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act intended for a bona fide scientific or medical research or law enforcement.

(4) For purposes of this section -
"child" means a person under the age of 18 years;

"child pornography" includes data which, whether visual or audio, depicts -

(a) a child engaged in sexually explicit conduct;

(b) a person who appears to be a child engaged in sexually explicit conduct; or

(c) realistic images representing a child engaged in sexually explicit conduct.

Sierra Leone has been increasing its capacity-building for law enforcement in order to address the challenges and issues related to online bystanders in the cyber environment. Training programmes have tended to focus on cybersecurity, child online protection and the protection of women against violence. No specific facilities and training programmes have been established on issues arising from online bystanders in the cyber environment.

Sierra Leone has established relationships with service and application providers concerning online bystanders and it does collaborate with various stakeholders on matters of cybersecurity and online protection generally. The country does engage with stakeholders in the ICT sector relating to various themes in the area of online safety. Sierra Leone has undertaken awareness-raising activities related to cybercrime and has developed interventions for child online protection – but not with a view to dealing with online bystanders. Sierra Leone does not have in place targeted technical and infrastructure security to address issues related to online bystanders. It also does not have advanced ICT infrastructure, and this poses a challenge in relation to infrastructure security.

Recommendations

The constitutional framework of Sierra Leone still leaves women vulnerable to exploitation and violence, given the patriarchal structure of the society. There is therefore a need to ensure discrimination against women is prevented through the implementation of legal and policy measures.

Sierra Leone needs to improve its ICT infrastructure in order to ensure that its cybersecurity profile and enforcement improve. Further, the country needs to increase its capacity-building for the various stakeholders so they can more effectively enforce existing laws relating to online protection. Sierra Leone needs to review its legal framework so it can deal with online bystanders specifically and protect women from online violence. The country also needs to develop and publish a national strategy and stakeholder map on online bystanders.

2.9. Mauritius

The Constitution of Mauritius, as with the other countries under review, provides for protection from discrimination. Article 16 specifically provides in part as follows:

> **Constitution**
>
> 16. Protection from discrimination
>
> (1) Subject to subsections (4), (5) and (7), no law shall make any provision that is discriminatory either of itself or in its effect.
>
> (2) Subject to subsections (6), (7) and (8), no person shall be treated in a discriminatory manner by any person acting in the performance of any public function conferred by any law or otherwise in the performance of the functions of any public office or any public authority.
>
> (3) In this section, 'discriminatory" means affording different treatment to different persons attributable wholly or mainly to their respective descriptions by race, caste, place of origin, political opinions, colour, creed or sex whereby persons of one such description are subjected to disabilities or restrictions to which persons of another such description are not made subject or are accorded privileges or advantages that are not accorded to persons of another such description.
>
> (4) Subsection (1) shall not apply to any law so far as that law makes provision
>
> (a) for the appropriation of revenues or other funds of Mauritius;
>
> (aa) for a minimum number of candidates for election to local authorities to be of a particular sex, with a view to ensuring adequate representation of each sex on a local authority;
>
> (ab) for a minimum number of candidates for election to the Rodrigues Regional Assembly to be of a particular sex, with a view to ensuring adequate representation of each sex in the Rodrigues Regional Assembly;
>
> (b) with respect to persons who are not citizens of Mauritius; or
>
> (c) for the application, in the case of persons of any such description as is mentioned in subsection (3) (or of persons connected with such persons), of the law with respect to adoption, marriage, divorce, burial, devolution of property on death or other like matters that is the personal law applicable to persons of that description.
>
> (5) Nothing contained in any law shall be held to be inconsistent with or in contravention of subsection (1) to the extent that it makes provision with respect to standards or qualifications (not being standards or qualifications specifically relating to race, caste, place of origin, political opinions, colour, creed or sex) to be required of any person who is appointed to any office in the public service, any office in a disciplined force, any office in the service of a local authority or any office in a body corporate established directly by any law for public purposes.
>
> (6) Subsection (2) shall not apply to anything which is expressly or by necessary implication authorised to be done by any such provision of law as is referred to in subsection (4) or (5).
>
> (7) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision whereby persons of any such description as is mentioned in subsection (3) may be subjected to any restriction on the rights and freedoms guaranteed by sections 9, 11, 12, 13, 14 and 15, being such a restriction as is authorised by section 9(2), 11(5), 12(2), 13(2), 14(2) or 15(3), as the case may be.
>
> (8) Subsection (2) shall not affect any discretion relating to the institution, conduct or discontinuance of civil or criminal proceedings in any court that is vested in any person by or under this Constitution or any other law.

Mauritius recognises online bystanders as role occupants in cybercrime or cybersecurity. Mauritius has an Anti-Cyber Threat Management System, which it implements through an online platform. The Mauritian authorities have demonstrated a capacity to detect online crime through devices and recordings from online bystanders. Mauritius does not have a formal policy framework for the recognition of online bystanders but developed a National Cybercrime Strategy for the period 2017–2019, although a new policy has not yet been

devised to replace it. Although Mauritius has not published a national strategy and stakeholder map on online bystanders in cybercrime, it has continued to make efforts to develop more comprehensive strategies for the online protection of persons.

The Computer Misuse and Cybercrime Act of 2003 broadly covers cybercrime, including specific provisions relating to child online protection. However, it requires updating on account of the technological challenges that have occurred since its passage. The country lacks a specific framework for addressing the issue of online bystanders in the cyber environment. Section 4 of the Computer Misuse and Cybercrime Act is the main section for use in dealing with online bystanders.

> **Computer Misuse and Cybercrime Act**
>
> (4) Access with intent to commit offences
>
> (1) Any person who causes a computer system to perform any function for the purpose of securing access to any program or data held in any computer system, with intent to commit an offence under any other enactment, shall commit an offence and shall, on conviction be liable to a fine not exceeding 200,000 rupees and to penal servitude for a term not exceeding 20 years.
>
> (2) For the purposes of this section, it is immaterial that -
>
> (a) the access referred to in subsection (1) is authorised or unauthorised;
>
> (b) the further offence to which this section applies is committed at the same time when the access is secured or at any other time.

Mauritius has been increasing its capacity-building for law enforcement in order to address the challenges and issues relating to online bystanders in the cyber environment. Training programmes have tended to focus on cybersecurity, child online protection and the protection of women against violence. No specific facilities and training programmes have been established for issues arising from online bystanders in the cyber environment. The Central Criminal Investigations Division of the Mauritius Police is responsible for investigating cybercrime.

Mauritius has established relationships with service and application providers concerning online bystanders and it does collaborate with various stakeholders on matters of cybersecurity and online protection generally. The country also engages with stakeholders in the ICT sector relating to various themes in the area of online safety. Mauritius has undertaken awareness-raising activities on the public internet and cybercrime. It has also developed interventions for child online protection but not with a view to online bystanders. The country suffers from the absence of targeted technical and infrastructure security to address issues related to online bystanders.

Recommendations

Mauritius' cyber laws are dated and have not been reviewed for a long time in order to keep it in line with technological changes. The provisions of the Act are largely archaic in relation to the advancement of technology. There is thus a need for the country to revise its laws so they can deal with online bystanders and also to bring them in line with rapid technological changes, to ensure the enhanced online protection of women and children.

Mauritius needs to enhance its technical and infrastructure capacity and to develop further interventions to ensure the protection of women and children against violence. The country further needs to build the capacity of the various stakeholders involved in the enforcement of the laws as well as adjudication so they can deal more effectively with issues relating to online bystanders. Mauritius further needs to develop and publish a national strategy and stakeholder map on online bystanders in cybercrime.

2.10. Malawi

Malawi has constitutional provisions for the protection of persons from discrimination. Specifically, Article 20 of the Constitution of Malawi provides as follows:

> *Constitution*
>
> *Equality*
>
> 20. (1) Discrimination of persons in any form is prohibited and all persons are, under any law, guaranteed equal and effective protection against discrimination on grounds of race, colour, sex, language, religion, political or other opinion, nationality, ethnic or social origin, disability, property, birth or other status.

(2) Legislation may be passed addressing inequalities in society and prohibiting discriminatory practices and the propagation of such practices and may render such practices criminally punishable by the courts.

The Constitution additionally provides for the protection of the rights of women. Article 24 provides as follows:

Rights of women

(1) Women have the right to full and equal protection by the law, and have the right not to be discriminated against on the basis of their gender or marital status which includes the right -

(a) to be accorded the same rights as men in civil law, including equal capacity -

(i) to enter into contracts;

(ii) to acquire and maintain rights in property, independently or in association with others, regardless of their marital status;

(iii) to acquire and retain custody, guardianship and care of children and to have an equal right in the making of decisions that affect their upbringing; and

(iv) to acquire and retain citizenship and nationality.

(b) on the dissolution of marriage -

(i) to a fair disposition of property that is held jointly with a husband; and

(ii) to fair maintenance, taking into consideration all the circumstances and, in particular, the means of the former husband and the needs of any children.

(2) Any law that discriminates against women on the basis of gender or marital status shall be invalid and legislation shall be passed to eliminate customs and practices that discriminate against women, particularly practices such as -

(a) sexual abuse, harassment and violence;

(b) discrimination in work, business and public affairs; and

(c) deprivation of property, including property obtained by inheritance.

Malawi has in place institutional arrangements for the enforcement of its cyber laws and regulatory framework. These include the Malawi Communications Regulatory Authority, established under the Communications Act of 1998, which regulates Malawi's communications sector but focuses only on postal services, broadcasting and telecommunications.

Malawi does not formally recognise online bystanders as role occupants in cybercrime or cybersecurity. The Malawi Police Service is responsible for all criminal prosecutions in Malawi, including on cybercrime. Malawi has demonstrated a capacity to detect online crime through devices and recordings from online bystanders. Malawi lacks a formal policy framework for the recognition of online bystanders.

The Electronic Transactions and Cyber Security Act of 2016 broadly covers electronic commerce and cybercrime, including specific provisions relating to child online protection. The country lacks a specific framework for addressing issues related to online bystanders in the cyber environment.

Malawi has been increasing its capacity-building for law enforcement in order to address challenges but not related to online bystanders in the cyber environment. Training programmes have tended to focus on cybersecurity, child online protection and the protection of women against violence. No specific facilities and training programmes have been established regarding issues related to online bystanders in the cyber environment.

Malawi has not established relationships with service and application providers concerning online bystanders although it does collaborate with various stakeholders on matters of cybersecurity and online protection generally. The country does engage with stakeholders in the ICT sector on various themes relating to online safety. Malawi has not undertaken awareness-raising regarding the public internet and cybercrime with a focus on online bystanders.

Malawi has developed interventions for child online protection but not with a view to online bystanders, and the country suffers from the absence of targeted technical and infrastructure security to address issues related to online bystanders.

Recommendations

Malawi has laws that deal with ICT generally but the country needs to enhance its legal framework and its enforcement of online protection,

especially for women and children. Although a law is in place to deal with online matters, this is still insufficient regarding dealing with online bystanders. Malawi needs to enhance its training and capacity-building for law enforcement in order to effectively deal with matters of online protection and, specifically, matters of online bystanders. Malawi needs to develop and publish a national strategy and stakeholder map on online bystanders in cybercrime.

2.11. Cameroon

Cameroon is home to in excess of 250 ethnic groups, with different national languages, cultures and traditions. For administrative purposes, the country is considered bilingual, with French and English as the two official languages. The country also uses a dual legal system, which consists of civil and common law, with civil law practised largely by the French-speaking majority and common law by the English-speaking minority. Efforts to harmonise the two legal systems have been resisted by the proponents of the common law. Customary courts exist at the community level based on local laws and customs.

The Constitution of Cameroon in its Preamble provides for the various rights of the people, including protection from discrimination. It provides, among other things, as follows:

> **Constitution**
>
> *Preamble*
>
> We, the people of Cameroon,
>
> Declare that the human person, without distinction as to race, religion, sex or belief, possesses inalienable and sacred rights;
>
> Affirm our attachment to the fundamental freedoms enshrined in the Universal Declaration of Human Rights, the Charter of United Nations and the African Charter on Human and Peoples' Rights, and all duly ratified international conventions relating thereto, in particular, to the following principles:
>
> ...
>
> 13. no person shall be harassed on grounds of his origin, religious, philosophical or political opinions or beliefs, subject to respect for public policy;
>
> 25. the State shall guarantee all citizens of either sex the rights and freedoms set forth in the Preamble of the Constitution.

Cameroon as a jurisdiction presents various dynamics that make it susceptible to violence against women. Cameroonian women account for 52 per cent of the total population and are often discriminated against because of the patriarchal society in which they live. They suffer inadequate legal protection as a result of the structure of Cameroonian society which gives prominence to men generally at the expense of the rights of women and girls. Despite its ethnic diversity, Cameroon gives importance to local traditions. This widely affects Cameroonian women's situation, as traditions do not give as much protection as modern equality laws. Although Cameroon's Constitution upholds gender equality, there are several legal, social, religious and cultural obstacles to attaining this.

The dual system of civil and common law, along with customary law, which is highly patriarchal, makes it difficult to value equality. This widely affects the situation of women in the country. It also means that, when dealing with issues relating to online bystanders, the general attitude towards violence against women tends to be given less importance than it should. It has been further noted that the persistence of gender-discriminatory provisions in various laws, as well as the discriminatory customary law and the prejudices and stereotypical attitudes regarding the role of women and men in the family and society, encourages continuous violence against women (Moussi, 2020). All this is based on the conception of male superiority and female subordination, promoted by cultural and religious practices. Additionally, the legal, socio-economic and political status of women in Cameroon makes them increasingly vulnerable to high levels of violence .

Cameroon has an officially recognised national (and sector-specific) cybersecurity framework for implementing internationally recognised cybersecurity standards. The framework was developed by the National ITC Agency for government agencies. Cameroon does not formally recognise online bystanders as role occupants in cybercrime or cybersecurity. Cameroon has demonstrated a capacity to detect online crime through devices and recordings from online bystanders. However, it lacks a formal policy

framework for the recognition of online bystanders. Law No. 2010/012 of 21 December 2010 relating to cybersecurity and cyber criminality in Cameroon has some specific sections that may be related to online bystanders:

> *Law No. 2010/012*
>
> Section 75. (1) Whoever for financial gain, records or publishes images that undermine the bodily integrity of another person through electronic communications or an information system without the consent of the person concerned shall be punished with imprisonment for from 02 (two) years to 05 (five) years or a fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs or both of such fine and imprisonment.
>
> (2) This section shall not apply where such recording and publication fall under the normal exercise of profession aimed at informing the public on where they are carried out in order to be used as evidence in Court in accordance with the provisions of Criminal Procedure Code.
>
> Section 76. Whoever uses electronic communications or an information system to design, carry or publish a child pornography message or a message likely to seriously injure the self respect of a child shall be punished with imprisonment for from 5 (five) years to 10 (ten) years or a fine of from 5,000,000 (five million) to 10,000,000 CFA francs or both of such fine and imprisonment.
>
> Section 80. (1) Whoever for consideration or free of charge, uses electronic communications or an information system to publish, attach, record or transmit an image showing acts of paedophilia or a minor shall be punished with imprisonment for from 01 (one) to 05 (five) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both of such fine and imprisonment.
>
> (2) Whoever uses electronic means whatsoever to offer, provide or publish, import or export an image or picture portraying paedophilia shall be punished with the penalties provided in Subsection 3 above.
>
> (3) Whoever keeps an image or picture portraying paedophilia in an electronic communication network or an information system shall be punished with imprisonment for from 01 (one) to 05 (five) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both of such fine and imprisonment.
>
> (4) The penalties provided for in Subsection 3 above shall be doubled where an electronic communication network is used to publish an image or picture of a minor.
>
> (5) The provisions of this section shall equally apply to pornographic pictures showing minors.

Although Cameroon has not published a national strategy and stakeholder map on online bystanders in cybercrime, it has continued to make efforts to develop more comprehensive strategies for the online protection of persons. The country lacks a specific framework for addressing the issue of online bystanders in the cyber environment.

Cameroon has been increasing its capacity-building for law enforcement in order to address the challenges and issues relating to online bystanders in the cyber environment. Training programmes have tended to focus on cybersecurity, child online protection and the protection of women against violence. No specific facilities and training programmes have been established to deal with issues related to online bystanders in the cyber environment.

Cameroon has established relationships with service and application providers concerning online bystanders and it collaborates with various stakeholders on matters of cybersecurity and online protection generally. The country engages with stakeholders in the ICT sector relating to various themes in the area of online safety. Cameroon has not undertaken awareness-raising regarding the public internet and cybercrime with a focus on online bystanders. Cameroon has developed interventions for child online protection but not with a view to online bystanders, and the country suffers from the absence of targeted technical and infrastructure security to address issues related to online bystanders.

Concern over online bystanders by stakeholders in Cameroon has been expressed publicly. In one anecdotal example, the Commission on Human Rights and Liberties of the Cameroon Bar expressed its dismay regarding the proliferation of videos depicting acts of torture, bullying and humiliation on social media. In a press statement, the Commission advocated for an end to the

videos, which were mostly propagated by the perpetrators themselves (MMInfo, 2021):

'Whether it is the case of "Mamamdi Esther" in Nkomkana Yaoundé, the "Malicka" case, the unwholesome incursion of the Forces of Law and order in a private house at Douala Bonamoussadi, the rapes of the elderly in Ombessa, it is more or less torture and ill treatment prohibited by Article 3 of the Geneva Conventions of 1949 and its Additional Protocols of 1977.'

The ICT sector in Cameroon has evolved considerably since 2010, despite the persistence of a digital divide and affronts to freedom of expression online. The country's digital landscape was boosted by the launch in May 2016 of the National ICT Strategic Plan 2020, which recognised the digital economy as a driver for development. Relevant agencies governing the sector include the Telecommunication Regulatory Agency and the National ITC Agency, both under the mandate of the Ministry of Posts and Telecommunications.

These agencies are guided by key laws that govern ICT, including Law No. 98/014 of 14 July 1998 governing telecommunications and its amendment of 29 December 2005; Law No. 2010/013 of 21 December 2010 on e-communications and its amendment of April 2015; Law No. 2010/012 of 21 December 2010 on cybersecurity and cybercrime; and Law No. 2010/021 of 21 December 2010 governing e-commerce. Other legislation related to ICT includes Framework Law No. 2011/012 of 6 May 2011 on consumer protection; Law No. 2001/0130 of 23 July 2001 establishing the minimum service in telecommunications; and Law No. 98/013 of 14 July 1998 on competition, which governs all sectors of the national economy.

Recommendations

Cameroon should apply its dual legal system in a manner that ensures consistent protection of women and children against violence and cyberbullying in a consistent manner. Cameroon must continue to build on its officially recognised national sector-specific cybersecurity framework, which has been implementing internationally recognised cybersecurity standards through the framework developed by the National ITC Agency.

Cameroon should continue developing its legal framework to address contemporary online cyber challenges and devise more comprehensive strategies for the online protection of persons and to build increased capacity to protect people online, especially women and children.

2.12. Seychelles

The Constitution of Seychelles provides for protection from discrimination. Article 27 provides as follows:

> **Constitution**
>
> *Article 27*
>
> (1) Every person has a right to equal protection of the law including the enjoyment of the rights and freedoms set out in this Charter without discrimination on any ground except as is necessary in a democratic society.
>
> (2) Clause (1) shall not preclude any law, programme or activity which has as its object the amelioration of the conditions of disadvantaged persons or groups.

Seychelles does not formally recognise online bystanders as role occupants in cybercrime or cybersecurity. The country has demonstrated a capacity to detect online crime emanating from materials derived from devices such as recordings made by online bystanders, through the Police Strategic Plan 2017–2019. However, Seychelles lacks a formal policy framework for the recognition of online bystanders. Although Seychelles has not published a national strategy and stakeholder map on online bystander in cybercrime, it has continued to make efforts to develop more comprehensive strategies for the online protection of persons.

The Computer Misuse Act 1998 as amended in 2012 broadly covers electronic commerce and cybercrime, including specific provisions relating to child online protection. The country lacks a specific framework for addressing online bystanders in the cyber environment.

Seychelles has been increasing its capacity-building for law enforcement in order to address the challenges and issues relating to online bystanders in the cyber environment. Training programmes have tended to focus on cybersecurity, child online protection and the protection of women against violence. No specific facilities and training programmes have been established to deal with issues relating to online bystanders in the cyber environment.

Seychelles has not established relationships with service and application providers concerning online bystanders although it does collaborate with various stakeholders on matters of cybersecurity and online protection generally. The country does engage with stakeholders in the ICT sector relating to various themes in the area of online safety. Seychelles has not undertaken awareness-raising activities regarding the public internet and cybercrime with focus on online bystanders. Seychelles has developed interventions for child online protection but not with a view to online bystanders, and the country suffers from the absence of targeted technical and infrastructure security to address issues related to online bystanders.

Recommendations

The law of Seychelles needs to be updated to address issues relating to cybercrime and online protection, especially for women and children. Further, Seychelles needs to increase the capacity of law enforcement and other stakeholders to deal with cybercrime, specifically cyberbullying. The country also needs to develop policies and processes for the protection of online bystanders.

2.13. South Africa

South Africa has constitutional provisions for the protection of persons from discrimination. Specifically, Section 9 (1) of the Constitution provides that 'Everyone is equal before the law and has the right to equal protection and benefit of the law.' Section 9 (3) further adds that 'The state may not unfairly discriminate directly or indirectly on one or more grounds, including race, gender, sex, pregnancy, marital status, colour, ethic or social origin, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth.'

Legislation

The country passed the Cybercrimes Bill into law on 1 June 2021. The Cybercrimes Act seeks to create offences that have a bearing on cybercrimes. Part II explicitly addresses the issue of violence perpetrated against a group of persons/person, dealing with malicious communications, which includes violence on the basis of a person's gender. To be specific, the definitions section of Part II provides for two important definitions relevant to the study:

Cybercrimes Act

> Section 13. Definitions
>
> 'Group of persons' means characteristics that identify an individual as a member of a group, which characteristics include without limitation, race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language, birth or nationality;
>
> ...
>
> 'Violence' means bodily harm.

Section 14 of the Act makes it an offence to disclose a data message with the intention to incite violence or damage to property; to be specific, the section provides that:

> Section 14. Data message which incites damage to property or violence
>
> Any person who discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to
>
> incite —
>
> (a) the causing of any damage to property belonging to; or
>
> (b) violence against, a person or a group of persons, is guilty of an offence.

Section 15 deals with data messages that threaten persons with damage to property or violence. It specifically provides that:

> Section 15. Data message which threatens persons with damage to property or violence
>
> A person commits an offence if they, by means of an electronic communication service, unlawfully and intentionally discloses a data message, which —
>
> (a) threatens a person with —
>
> (i) damage to property belonging to that person or a related person; or
>
> (ii) violence against that person or a related person; or
>
> (b) threatens a group of persons or any person forming part of, or associated with, that group of persons with —

(i) damage to property belonging to that group of persons or any person forming part of, or associated with, that group of persons; or

(ii) violence against the group of persons or any person forming part of, or associated with, that group of persons, and a reasonable person in possession of the same information, with due regard to all the circumstances, would perceive the data message, either by itself or in conjunction with any other data message or information, as a threat of damage to property or violence to a person or category of persons contemplated in paragraph *(a)* or *(b)*, respectively.

Section 16 deals with the disclosure of data with intimate messages. This provision makes it an offence to disclose, unlawfully and intentionally, a data message with intimate images without the consent of the person to whom the images belongs. It defines 'intimate messages' to include any real or simulated depiction in which a person is nude or their genital organs or anal area is displayed, including breasts in instances where a person identifies as female, transgender or intersex, in a manner that violates the sexual integrity of the person involved or constitutes sexual exploitation.

Section 17 extends to persons who attempt, conspire, aid and abet, incite, instigate, command or procure the services of someone else to commit the above offences, who will thus be deemed in contravention of the Act. Although these provisions do not explicitly address the issue of the online bystander, offenders of this nature may be deemed to be in contravention of the Act's provisions by implication and subsequently prosecuted; however, the element of intent would have to be established.

The Act also provides for recourse for persons who have been violated under the provisions of this Act. To be specific, Section 20 provides for complainants to apply for protection orders pending the finalisation of a criminal case in instances where a criminal charged has already been lodged with the South African Police Services.

Section 20. Order to protect complainant pending finalisation of criminal proceedings

(1) A complainant (hereinafter referred to as the applicant) who lays a charge with the South African Police Service that an offence contemplated in section 14, 15 or 16 has allegedly been committed against them, may on an ex parte basis in the prescribed form and manner, apply to a magistrate's court for a protection order pending the finalisation of the criminal proceedings to —
(a) prohibit any person to disclose or further disclose the data message which relates to the charge; or

(b) order an electronic communications service provider whose electronic communications service is used to host or disclose the data message which relates to the charge, to remove or disable access to the data message.

To support this application, the Act places a duty on electronic communications service providers to supply the information required for the prosecution of the alleged offence. Through this provision, the Act empowers a member of the South African Police Services with practical mechanisms to enable them to obtain the required evidence to facilitate a protection order application against the perpetrator. The issuance of a protection order by the court would be in accordance with Section 9 (4) of the Protection from Harassment Act 2011, which gives the court powers to issue a protection order if it finds, on a balance of probabilities, that the respondent engaged in harassment.

The Protection of Personal Information Act of 2013, which came into effect on 30 June 2021, aims to protect personal information in processing by both public and private bodies. Section 26 of the Act is relevant for this study as it prohibits the processing of personal information concerning the religious or philosophical beliefs, race, health or sex life of a data subject. Similarly, the Act prohibits the sharing/resharing of information on a person's sex life, or even their private contact details, especially in recognition of recent targeting of women journalists by political parties. This Act can thus be interpreted to include persons such as bystanders who reshare personal information on a person's sex life. Such resharing of personal information would constitute a contravention of the provisions in the Act.

Sections 20 and 55 make provision for enforcement mechanisms and give powers to the police to investigate matters of this nature, and more importantly mandate the national commissioner to designate an officer to be known as the point of contact, charged with investigating commissions of offences as stipulated in the Act. In addition to this,

Section 55 places an obligation on the minister of police to 'establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes'. This includes providing accredited training to police officials on aspects relating to this. Section 55 (3) (a) also mandates the minister to report to parliament on an annual basis cases that have been reported to the police and resulted in criminal prosecutions. In line with the Act, the South African Police Service has established a Cybercrimes Unit, tasked with investigating cybercrimes. The Unit has published awareness-raising material on its webpage on cybercrime prevention, including on crimes against children and abuse, but it remains unclear whether it has engaged in awareness-raising on online bystanders.[4]

Overall, the Act, while containing important provisions relating to online violence against women, is in its infancy in terms of implementation.

National policies and strategies

South Africa's National Strategic Plan on Gender Based Violence and Femicide aims to address the various forms of violence that are prevalent in the country. Its development followed protest by women and gender non-conforming persons calling on the South African government to prioritise VAWG. The Plan recognises OVAWG and draws its definition of this from the United Nations Special Rapporteur's Report on VAW of 2018. Its prevention pillar makes certain assumptions on how prevention can be tackled. These include communities being ready and willing to harness their individual and collective resources to stop VAWG. Although this does not specifically refer to digital communities, an inference can be drawn that includes both offline and online bystanders. The Plan prioritises raising awareness on OVAWG; there is an opportunity to conduct further research in this area.

The National Cybersecurity Framework 2015 seeks to centralise co-ordination on cybersecurity activities, develop skills and conduct research, and promote a culture of cybersecurity. It establishes a cybersecurity hub that serves to co-ordinate interactions between the private sector, government and civil society on cybersecurity threats; disseminate information on cybersecurity developments; and engage in awareness-raising campaigns and research initiatives. Section 14 of the Policy emphasises the importance of building a cyberculture whereby users are informed of the risks of cybersurfing, through initiating awareness-raising programmes and working with civil society organisations on outreach programmes. The scope of application of the Policy is broad; it can be implied that, as more developments on cybercrimes such as violence against women are defined, then awareness-raising on matters such as the online bystander will take place. This is also in light of the developments of case law on issues of violence against women perpetrated online. Currently, there are no known awareness-raising initiatives on the online bystander.

Case law on online violence against women and girls

Given that this is a developing area of study, there is limited case law with regard to the issue of online bystanders. One specific case is that of *Brown v Economic Freedom Fighters*, in which the court found a political partly liable for online harassment experienced by a journalist, having instigated its members to incite violence against the applicant. To be specific, in 2019, the South Gauteng High Court ruled that the failure of the political party to condemn the harassment violated the Electoral Code. The party leader had tweeted a message with the personal contacts of the journalist, which had resulted in the party supporters threatening the journalist with rape and other forms of harassment. In delivering its ruling, the court held that in adhering to and upholding the rights of women, political parties had a duty under the Act to take reasonable steps to condemn and stop such harassment.[5] At the time, the Cybercrimes Act had not been passed into law; however, this case remains significant in setting a precedent on OVAWG and on how formations such as political parties can be held liable when instigating or perpetuating this crime.

Training/awareness-raising on online violence against women and girls

It remains unclear whether targeted training for duty-bearers and stakeholders on online bystanders and violence against women has taken place. However, the United Nations Children's Fund South Africa together with partners has implemented an awareness programme on online

4 www.saps.gov.za/alert/cybercrime_prev_tips.php

5 ZAGPJHC 166.

violence against children. This programme aimed at strengthening children's online safety in the country and was implemented between May 2018 and August 2021.[6]

Recommendations

The Cybersecurity Act is a progressive piece of legislation that will be critical to addressing OVAWG. However, it has missed an opportunity to define what a perpetrator is. It will thus be left to the courts to interpret whether a perpetrator includes an online bystander as defined by the Commonwealth.

One option is to amend some provisions of the Act to expand on the definition of a perpetrator and also on the various forms of OVAWG. As mentioned earlier, the advent of technology has introduced new forms of violence that are not encapsulated in current definitions of violence against women in law, for example cyberbullying, cyberstalking, etc.

2.14. Botswana

The Constitution of Botswana provides for protection from discrimination. To be specific, Article 15(1&2) prohibits discriminating against any person only on the basis of any one or more of the aspects such as race, tribe, place of origin, political opinions, colour, creed, or sex.

The article defines the term "discriminatory" as meaning affording different treatment to different persons, attributable wholly or mainly to their respective descriptions by race, tribe, place of origin, political opinions, colour, creed or sex whereby persons of one such description are subjected to disabilities or restrictions to which persons of another such description are not made subject or are accorded privileges or advantages which are not accorded to persons of another such description.

Botswana's Cybercrime and Computer Related Crimes Act of 2018 repeals the Cybercrime and Computer-Related Crimes Act of 2007. It seeks in its Preamble to combat cybercrime and repress criminal activities perpetrated through computer systems and facilitates the collection of electronic evidence. Although the Act does not have provisions that specifically address the issue of online bystanders, there are important clauses that relate to child pornography. For example, Section 19 of the Act criminalises the publication, production and possession of child pornography material. It defines child pornography to include 'material that visually depicts a child engaged in sexually explicit conduct, including a person who appears to be engaged in sexually explicit conduct and the depiction of realistic images representing a child engaged in sexually explicit conduct'. Section 20 deals with the publication of sexually explicit material; it makes it an offence to publish private sexual photographs without the consent of the person who appears in the photograph or films with intent to cause distress. However, both sections are limited in their scope of application, particularly to online bystanders, as they require that intent be proven for contravention.

Botswana's Cybersecurity Strategy seeks in its Mission Statement to protect information infrastructure and build capacity capabilities to prevent and respond to cyberthreats. It was informed by a cybersecurity assessment conducted in 2012, with the support of the International Telecommunication Union, which found, among other issues, that cybersecurity needed to be allocated sufficient priority in policy-making, including through building the capacity of various stakeholders such as the judiciary, financial institutions and service providers to handle cybersecurity. Although the Strategy was developed prior to the enactment of the Cybercrime and Computer Related Crimes Act 2018, it recognises the existence of threats in cyberspace, which include revenge porn and child pornography. However, it fails to recognise the full spectrum of the various forms of violence against women that occur in cyberspace.

The Strategy presents opportunities to build knowledge on OVAWG and the online bystander, through its Strategic Objectives 2 and 3, which seek to enhance capacities and capabilities to reflect everchanging technical knowledge and requirements, including collaborating more with academia. Specifically, Strategic Objective 3 seeks to protect children and other vulnerable groups against cyberthreats. Key actions proposed include conducting outreach programmes and awareness-raising targeted at the general public to foster a culture of safe practices.

There is currently no evidence of training that has taken place on the subject matter of this report.

6 See https://www.end-violence.org/grants/unicef-south-africa

Recommendations

Contravention of the Cybercrime and Computer Related Crimes Act requires that intent is established on the part of the perpetrator; the same would apply in the case of the online bystander. Who constitutes a perpetrator would similarly require judicial interpretation unless an amendment is made in the Act to define this.

As in other jurisdictions, public education on the contents of the Act will be necessary to raise awareness on OVAWG.

2.15. Eswatini

Article 20 of the Constitution of Eswatini provides for equality before the law and states :

> 20(1) All persons are equal before and under the law in all spheres of political, economic, social and cultural life and in every other respect and shall enjoy equal protection of the law
>
> 20(2) For the avoidance of any doubt, a person shall not be discriminated against on the grounds of gender, race, colour, ethnic origin, tribe, birth, creed or religion, or social or economic standing, political opinion, age or disability

The Computer and Cybercrime Act of 2013 was passed into law in March 2022. The Act seeks to criminalise offences committed against, and through the usage of computer systems and electronic communications networks, to provide investigation and collection of evidence for computer and network related crimes (see preamble).

Although the Act's interpretation section does not explicitly provide a definition for what constitutes OVAWG, nor create a positive duty on the online bystander to take action to address VAW, it makes provision in Section 14 (1) for sexual exploitation through child pornography. This is defined to include a child engaged in sexually explicit conduct and images representing a child engaged in sexually explicit conduct.

Section 28 makes provision for what is termed 'harassment utilising means of electronic communications'. It provides that:

> A person who intentionally and without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intention to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system, to support hostile behaviour, commits an offence and is liable, on conviction, to a fine not exceeding one hundred (1) thousand Emalangeni or to imprisonment for a period not exceeding five (5) years or both.

As mentioned earlier, the Act does not provide a definition of VAW but certain acts, such as the one defined in the above section, can be interpreted to constitute acts of violence, although this is not explicit. Section 30 (1) addresses persons who aid or abet persons or carry out any act in furtherance of a crime, who are seen to commit an offence in terms of the Act.

Section 49 provides that:

> Except as provided for in this Act, any offence under any Act which is committed in whole or in part through the use of a computer, electronic device or in electronic form is deemed to have been committed under that Act and the provisions of that Act shall apply with the necessary modification to the person who commits the offence.

This section can be read together with the Sexual Offences and Domestic Violence Act 2018, which creates criminal offences relating to violence against women. It can be interpreted to mean that violence against women offences committed under the Sexual Offences and Domestic Violence Act using technologies such as computers and social media will be deemed to have been committed under this Act. Penalties will apply under the Sexual Offences and Domestic Violence Act.

The Computer and Cybercrime Act's Section 14 on child pornography, which makes it an offence to produce, offer, distribute or procure or knowingly obtain or access child pornographic material through ICT, extends to the online bystander who reshares information obtained through such a platform.

The Sexual Offences and Domestic Violence Act 2018 makes it a criminal offence to distribute child pornography and addresses the issue of sexual harassment and domestic violence. Although this law is limited because it does not explicitly define the online violence, it can be interpreted to mean

that violence, in whatever form as covered by this law, is an offence regardless of the platform used.

The country has also adopted the National Cybersecurity Strategy 2020–2025, whose vision is a safe, secure and resilient cyberspace in the country. This establishes various institutional frameworks to address the issue of cybersecurity broadly. These include the National Cybersecurity Agency, which has been tasked with, among other duties, collecting information on cybersecurity concerns, including conducting a national study on cybercrimes. Although the Strategy recognises that the country still needs capacity support in understanding cybersecurity and keeping abreast of security issues, it is unfortunately silent on the issue of OVAWG.

Credence must be given to the emphasis placed by the Computer and Cybercrime Act on public education and awareness on cyber threats. While there is currently no case law in the country on this subject matter, it is clear that, with more public awareness on these types of crimes, the public will be more sensitised to the seriousness of cybercrime and be able to seek recourse using the law.

Recommendations

It is clear from the above that Sections 28 and 30 of the Computer and Cybercrime Act as implied include the online bystander; however, an opportunity exists to revise provisions to bring clarity on persons who constitute a bystander and the liability attached to such actions.

The following recommendations are proposed:

It is recommended that Computer and Cybercrimes Act be amended to:

- define in the Act who constitutes 'a person' as stipulated in Section 28;
- include in the Act the various forms of OVAWG as acts that constitute an offence;
- alternatively, amend the Sexual Offences and Domestic Violence Act to include these types of online violence and the online bystander, although changes to the Computer and Cybercrimes Act are preferred;
- include in the Computer and Cybercrimes Act provisions such as on the non–consensual sharing of personal information as offences.

It is imperative that the country undertakes studies on OVAWG and also engages in awareness-raising on online violence with various stakeholders. There is currently no evidence of any capacity-building undertaken on OVAWG and the duties or obligations of the bystander. There is, however, recognition that this is a growing area of work and the effective enforcement of the Act will require that officers are well equipped with the knowledge and understanding required to effectively respond.

2.16. Lesotho

In Lesotho, the Computer Crime and Cybersecurity Bill 2021 has been approved by parliament and is yet to be further approved by senate and assented by the King of Lesotho. The Bill aims to combat computer crimes and provides for punitive measures, as well as establishing mechanisms such as the National Cybersecurity Advisory Council and a Cybersecurity Incidence Response Team tasked with managing cybersecurity in Lesotho. The Bill itself does not address the issue of online bystanders but it does contain important provisions on various forms of violence against women and child pornography.

Section 33 deals with the non-consensual distribution of intimate images. It provides that:

> A person who makes available, broadcasts or distributes by means of a computer system, a data message of an intimate image of an identifiable person knowing that the person depicted in the image did not given his consent, or its broadcasting and distribution commits an offence and is liable, on conviction to a fine.

Section 33 (2) defines intimate images as a visual depiction of a person made by any means – (a) under circumstances that give rise to reasonable expectation of privacy and (b) in instances in which the person is nude, or exposing his genital organs or anal region, or in the case of a female, her breast.

While this provision is progressive and does address a form of violence against women, and by implication it extends to the online bystander, the element of 'consent' would need to be proven in a court of law. Section 40 of the Bill similarly addresses acts of harassment and other forms of violence, which include those perpetrated on the basis of a person's gender by making it an offence to 'intentionally and without lawful

excuse initiate electronic communication with intent to coerce or intimidate, harass, abuse or cause emotional distress or initiates offensive and obscene communication with intent to disturb peace commits an offence'. This section applies to initiators of the act; however Section 42 of the Bill further provides for instances where a person aids, abets or does any act preparatory or in furtherance of the commission of an offence to be held liable. It can be implied that this provision relates to online bystanders as persons who may further the commission of such acts either intentionally or without intent.

In the absence of an Act of parliament on the above matter, the Domestic Violence Act of 2008 applies in instances where online violence has been perpetrated by a person with whom the complainant/victim is in a domestic relationship. This legislation is limited in its scope and would not apply to persons who are not in a domestic relationship. Other applicable laws would include the following:

- the Sexual Offences Act 2003, which consolidates all sexual offences and prescribes sentences for offences;
- the Anti–Human Trafficking Act 2011 in. instances of trafficking; Section 4 (b) is particularly relevant for this study because it holds liable persons who aid, facilitate, organise or encourage other persons to engage in trafficking. Section 6 (d) expands on this issue and extends to online bystanders, it provides that:

A person who advertises, publishes, prints, broadcasts, distributes by any means including the use of ICTs and the internet that promote trafficking commits an offence and shall be liable to the same penalties as those of person commits an offence as if they committed the offence of trafficking.

- the Penal Code 2010, which covers issues such as assaults, threats and sexual offences against children.

These laws would apply in instances where such crimes have been committed but would not extend to the online bystander where this person is aware of the commission of such an act but does nothing about it. Arguably, the resharing of child pornographic content would constitute an offence under the Sexual Offences Act 2003.

Recommendations

Lesotho should pass legislation dealing with cybercrimes and incorporate, in its interpretation section, a definition of OVAWG. Similarly, the definition of a perpetrator must include and should extend to the online bystander.

2.17. Namibia

Article 10 of the Constitution of Namibia makes provision for equality and freedom from discrimination. This Article provides that "All persons shall be equal before the law. No persons may be discriminated against on the grounds of sex, race, colour, ethnic origin, religion, creed or social or economic status".

The Internet Society Namibia Chapter reveals that cybercrimes, in this case OVAWG, is rife, the most prevalent form being revenge porn. Namibia is in the process of finalising its cybercrime legislation. The country has also passed a number of laws to address violence against women; these include the following:

- The Combatting of Domestic Violence Act 2003 seeks to provide redress for persons experiencing various forms of violence. Its scope of application is limited to persons in a domestic relationship.
- The Combatting of Rape Act 2000 addresses various forms of sexual offences and prescribes minimum sentences for rape. This law also deals with child protection issues, rape and the distribution and publication of child pornography

In relation to institutional mechanisms, the country's Ministry of Gender and Child Welfare Unit has the objective of ensuring the empowerment and protection of children. Women and Child Protection Units were established in 1991 to provide protection to victims of violence. More recently, the government has recommitted to strengthening the enforcement of laws in light of escalating levels of violence against women and children. It remains unclear whether the mandate of these units extends to online violence.

Recommendations

In the absence of legislation on cybersecurity, and more specifically provisions on OVAWG and on the bystander, an opportunity remains for the

country to address the duties and responsibilities of the online bystander in relation to VAW. The Commonwealth Secretariat has previously conducted a workshop with government officials on cybersecurity, which recognised that the country was lacking in knowledge in this area.

Overall, current laws are not sufficient with respect to the issues being studied here.

2.18. Mozambique

The country is currently in the process of developing cybersecurity legislation; in its absence, there are a number of laws to address violence against women and the protection of data regardless of the platform on which it takes place. These include:

- The Constitution guarantees rights to equality and non-discrimination (Article 36). It also entitles citizens to the protection of their private life, including granting the protection of a good name, reputation and public image. It also recognises the need to legislate on the protection and use of computerised personalised data.
- The Domestic Violence Act 2009 provides protection to persons experiencing or at risk of experiencing violence; however, this is limited to persons in a domestic relationship.

Mozambique's Cybersecurity Strategy 2017–2021 aims at adopting measures that guarantee a safe online environment. Specific Objective covers strengthening information-sharing among stakeholders to ensure a timely response to cybersecurity threats – this includes the judiciary, law enforcement and various service providers. This also includes developing an online platform with updated information on cybersecurity threats, vulnerabilities and incidents in a bid to foster trust. However, there is currently no evidence of the establishment of such a platform. Specific Objective 9 envisions investing in research and development on cybersecurity, in the understanding that there is a dearth of knowledge in this area. In this, it provides for collaboration between academia, the private sector, etc. In addition, the Strategy recognises the importance of training stakeholders, including assessing levels of awareness on cybersecurity among the public.

While the Strategy contains important provisions aimed at dealing with cybersecurity threats – although it is silent on issues related to women's safety and security – the extent of its implementation remains unclear.

Recommendations

Overall, Mozambique is in the early stages of responding to cybersecurity threats – and there is limited evidence of efforts to curb such threats. In light of this, it is recommended that:

- Mozambique fast-track the process of developing a law to respond to cyber threats, including a consultation process with experts on OVAWG to enable the development of strong legislation responding to the various manifestations of VAW.
- Drafters of this law strongly consider explicitly incorporating the role of the online bystander in the text of any law.
- The government engage in continuous knowledge-building and public awareness-raising on cybersecurity.

2.19. The Gambia

The Gambia is an Islamic nation that applies Sharia law. The Constitution provides a fundamental legal framework for the protection of the rights of the people.

Constitution

17. Fundamental rights and freedoms

(1) The fundamental human rights and freedoms enshrined and in this Chapter shall be respected and upheld by all organs of the Executive and its agencies, the Legislature and, where applicable to them, by all natural and legal persons in The Gambia, and shall be enforceable by the Courts in accordance with this Constitution.

(2) Every person in The Gambia, whatever his or her race, colour, gender, language, religion, political or other opinion, national or social origin, property, birth or other status, shall be entitled to the fundamental human rights and freedoms of the individual contained in this Chapter, but subject to respect for the rights and freedoms of others and for the public interest.

Although the Constitution protects the rights of citizens generally, it still has shortcomings in relation

to the rights of women. For example, Section 33 (5) (c) provides that the prohibition of discrimination does not apply in respect of adoption, marriage, divorce, burial and devolution of property upon death (Amnesty International, 2017). Additionally, VAW in The Gambia remains a grave concern. The Women's Act No. 12 of 2010 enforces the protection of women's constitutional rights, including human rights, health, protection from discrimination and special measures supporting women (Pomerantz, n.d.).

The principal legislation in The Gambia for the regulation of information technology is the Information and Communications Act of 2009, which attempts to comprehensively address the rapid evolution and convergence of technologies in the country. The Act covers themes such as protection against child pornography, penalties for reprogramming telecommunication and personal data protection. There has been some training for law enforcement in The Gambia, under the auspices of the Gambia Cyber Security Alliance, which collaborated with Northampton University in December 2020 to conduct cybersecurity and cybercrime training for the Tallinding Police Department for a period of one month. The training was prompted following observations emerging from news and defamatory matter emanating from WhatsApp groups (Cham, 2020). It aimed to enhance the ability and efficiency of officers in terms of cybersecurity as well as to equip and prepare them for cybercrime incidents.

The Gambia does not formally recognise online bystanders within its legal framework and the country has not undertaken awareness-raising activities on the public internet and cybercrime with a focus on online bystanders, despite the capacity-building work of the Gambia Cyber Security Alliance.

Recommendations

The Gambia needs to revise and implement its legal framework to ensure the greater protection of women, especially because of the way in which women are perceived under Sharia law. The country also needs to enhance its capacity to implement laws relating to online protection of women and children.

The Gambia needs to ensure that it implements policies for online bystanders and builds further capacity for law enforcement and stakeholders to collaborate in dealing with cybercrime.

3. Recommendations

3.1. Areas for policy and legal reform (improvements)

The analysed jurisdictions should put in place legal frameworks that ensure accountability of online bystanders, such as 'bad Samaritan' laws. Some of the jurisdictions have attempted to incorporate the various international instruments such as the Budapest Convention on Cybercrime into their domestic legal frameworks. However, important aspects of jurisdiction such as the extraterritorial application of domestic laws of various jurisdictions examined have proved to be important in order to effectively deal with the challenges associated with online bystanders. Additionally, a number of the jurisdictions under analysis have implemented provisions for international cooperation in relation to cybercrime generally as this is invaluable as a tool for effective law enforcement related to online violence against women and girls (OVAWG)

Although the countries analysed are generally signatories to the Convention on the Rights of the Child (CRC), they are yet to fully implement its provisions and those principles contained in the Lanzarote Convention which affords protection to children from sexual abuse and exploitation. A number of the countries have specifically criminalised online child pornography and other forms of abuse of children in line with the principles and provisions of the Lanzarote Convention. There are still a number of provisions which have to be implemented in relation to the protection of children from sexual exploitation.

Cultural and traditional practices that are harmful to women and encourage discrimination against women should be eliminated. In addition to eliminating these practices, the principles set out in the Istanbul Convention to help prevent and combat violence against women and domestic violence need to be implemented in order to ensure that women are protected from violence both in the real world and online.

Legal and constitutional frameworks that leave room for discrimination should be revised in order to ensure that both genders receive equal treatment.

There is a need for enhanced capacity-building for law enforcement and for judicial officers in matters relating to online bystanders.

3.2. Specific recommendations for the Commonwealth

Adoption of Best Practice

Best practice as contained in the various international instruments such as the Budapest Convention, Lanzarote Convention and the Istanbul Convention need to be incorporated into the legal frameworks. Deliberate efforts should be made through the development of Commonwealth model laws and other interventions to ensure that the legal frameworks consisitently apply the best possibe legislative provisions for the protection of women and girls against online violence.

Common law

In improving bystander intervention in online spaces, certain principles available under common law, which are aimed at rewarding or punishing actions or omissions wherever a prior relationship can be established or not, could be useful. The existence of these legal principles under common law is particularly useful given the colonial history under British rule shared by most of the countries listed in this study, which extends to the development of their legal system and jurisprudence.

Bad Samaritans laws

A bad Samaritan is defined as a person 'who by inaction allows another to suffer a harm' (Klepper, 1993). According to Klepper, under common law, the following elements pertain to the bad Samaritan principle: actual intention, wantonness, criminal negligence, malice and knowledge. The following features have also been described as necessary in order to ascertain who a bad Samaritan is (Feinberg, 2003):

- a stranger standing in no 'special relationship' to an endangered party,
- who omits to do something – e.g., warn of unperceived peril, attempt a rescue, call the emergency services,

- which she could have done without unreasonable cost or risk to herself or others,
- as a result of which the endangered party suffers harm or an increased degree of harm, and
- who for these reasons is morally blameworthy.

Generally, under criminal law, two elements need to be satisfied to establish guilt and ensure a conviction: the *acteus reus,* which is the guilty act, for instance the act of murder or rape itself, and the *mens rea,* the guilty mind or intention to commit those acts. The *acteus reus* consists of acts of commission and, in the case of the bystander, omission. Where a person refuses to commit an act, intentionally or wantonly or negligently/recklessly or with malice or with knowledge, this constitutes or ought to constitute a certain culpability.

Negligence

Negligence may be actionable as either a civil or a criminal cause of action. Civil negligence or the tort of negligence occurs where there is a loss resulting from a breach of a duty of care, such as when a medical professional improperly discharges his or her duty towards a patient, or when a beverage company produces food unfit for consumption, as was the case in the *locus classicus* case of *Donoghue v Stevenson*.[7]

Criminal negligence goes a step beyond the tort of negligence. It occurs when an individual acts with such disregard or indifference to human life that he or she creates a risk of great bodily injury or death to those around him of which a reasonable person ought to be aware.

In the case of online bystanders, it may be difficult to establish a pre-existing duty of care between a victim of online violence and online bystanders, and therefore the probability of success of a civil action may be slim. However, in cases where the refusal to intervene may be reasonably expected to result in suicide, bodily harm or violence, it is possible to argue for a law criminalising the refusal to take action in the instance of where a bystander takes no action.

It is also important to note the risks involved in enacting bystander laws, taking into account the approach to internet regulation taken by many African governments. There is a need to properly weigh the value of this law to prevent the unfair targeting of journalists, members of civil society and their followers online by the government.

Meanwhile, beyond online social media users, the principle may be used to compel social media moderators who benefit from user engagements on their websites to better moderate and monitor the activities on their platforms.

Good Samaritan laws

Good Samaritan laws refer to laws that encourage, by granting legal protection to people who offer aid to persons in need. Typically, these laws protect good Samaritans from litigation because of the charitable acts and services they provide, in order to encourage good neighbourliness.

In contrast with bad Samaritan laws, which consist of duties to rescue or report and punish a failure to do so, good Samaritan laws seek to encourage or incentivise providing assistance to persons in need.

In relation to OVAWG, this would involve improving the ability to report and monitor these incidents to online moderators and civil authorities. It also involves the option to report anonymously or the de-identification of personal data easily traceable to reports.

7 (1932)A.C 562.

4. Conclusions

It is evident that the countries reviewed in this report do not have the necessary infrastructure to deal with online violence against women and girls and online bystanders and there is a need for a review of the current legislation.

Although the constitutional frameworks of the countries generally provide protection of human rights, they do, in some instances, perpetuate discrimination against women and girls.

The countries are at different points regarding the necessary legislation and their ability to deal with online bystanders. However, all the countries are making efforts to ensure adherence to best practice to protect women and girls from online violence effectively.

References

Amnesty International (2017) 'Human Rights Priorities for the New Gambian Government'. 28 April. www.amnesty.org/fr/wp-content/uploads/2021/05/AFR2761232017ENGLISH.pdf

Cham, J. (2020) 'Gambia: GCSA Trains Tallinding Police on Cyber Security, Cyber Crime'. *The Point*, 14 December. https://allafrica.com/stories/202012150266.html

Banyard, V.L., E.G. Plante and M.M. Moynihan (2005) *Rape Prevention Through Bystander Education: Bringing a Broader Community Perspective to Sexual Violence Prevention*. Washington, DC: US Department of Justice.

Babalola, O. (2020) 'ECOWAS Court Judgment Compelling Nigeria to Repeal or Amend Its Cybercrime (Prohibition, Prevention, E.T.C) Act of 2015'. *This Day*, 3 September. www.thisdaylive.com/index.php/2020/09/03/ecowas-court-judgment-compelling-nigeria-to-repeal-or-amend-its-cybercrime-prohibition-prevention-e-t-c-act-of-2015/

Ewepu, G. and F. Eromosele (2021) 'Sexual Violence: CSOs Demand 18 States to Domesticate CRA, VAPP Acts'. *Vanguard*, 7 June. www.vanguardngr.com/2021/06/sexual-violence-csos-demand-18-states-to-domesticate-cra-vapp-acts/

Feinberg, J. (2003) *The Moral Limits of the Criminal Law Volume 1: Harm to Others*. Oxford: Oxford University Press.

Iyer, N., B. Nyamwire and S. Nabulega (2020) 'Alternate Realities, Alternate Internets African Feminist Research for a Feminist Internet'. Report by Pollicy for the APC Feminist Internet Research Network Project.

Klepper, H. (1993) 'Criminal Liability for the Bad Samaritan'. *Public Affairs Quarterly* 7(1), January.

Latané, B. and J. Darley (1970) *The Unresponsive Bystander: Why Doesn't He Help?* New York: Appleton-Century Crofts.

MMInfo (2021) 'Cameroon Bar Commission Denounces Rising Cyber Bullying, Seeks Sanctions for Perpetrators'. 14 July. https://mimimefoinfos.com/cameroon-bar-commission-denounces-rising-cyber-bullying-seeks-sanctions-for-perpetrators/

Moussi, C.A. (2020) 'Violence Against Women in Cameroon: An Unchecked Phenomenon'. *SVRI Blog*, 3 November. www.svri.org/blog/violence-against-women-cameroon-unchecked-phenomenon

Munyua, A. (2013) 'Kenya - Women and Cyber Crime in Kenya', in Finlay, A. (ed.) *Women's Rights, Gender and ICTs.* Global Information Society Watch 2013. Association for Progressive Communications and Humanist Institute for Cooperation with Developing Countries.

Olasanmi, O., Y. Agbaje and M. Adeyemi (2020) 'Prevalence and Prevention Strategies of Cyberbullying among Nigerian Students'. *Open Journal of Applied Sciences* 10: 356–357.

Pomerantz, R.()n.d. 'Prioritizing Women's Rights In The Gambia'. https://borgenproject.org/womens-rights-in-the-gambia/

Posetti, J. and N. Shabbir (2020) *The Chilling: A Global Study of Online Violence Against Women Journalists.* Washington, DC: ICJF.

Powell, A. (2011) *Review of Bystander Approaches in Support of Preventing Violence Against Women*. Melbourne: Victorian Health Promotion Foundation.

Senn, C., J. Hollander and C. Gidycz (2018) 'What Works? Critical Components of Effective Sexual Violence Interventions for Women on College and University Campuses', in Orchowski, L. and C. Gidycz (eds) *Sexual Assault Risk Reduction and Resistance*. Amsterdam: Elsevier.

Wagabaza, O. (2019) 'Why Online Violence Against Women is Persistent in Uganda Despite Existing Laws and Policies'.*Arise*, Issue 67, November. www.kas.de/documents/280229/4616563/ARISE+Issue+67.pdf/e9c420c2-7267-e348-f9bd-0e5eb99c58cc?version=1.2&t=1605608816734

WOUGNET (Women of Uganda Network), Association for Progressive Communications, Collaboration on International ICT Policy for East, Southern Africa (2016) *Women's Rights and the Internet in Uganda.* Stakeholder Report, Universal Periodic Review 26th Session, Uganda. Kampala: Association for Progressive Communications.

Appendix A Online Violence Against Women Country Status

Country analysis	Uganda	Kenya	Nigeria	Rwanda	Ghana
Does the country recognise online bystanders as role occupants in cybercrimes?	No	No	No	No	No
Has the country/jurisdiction published an online bystander on cybercrime national strategy?	No	No	No	No	No
Has the country put legislation or regulations that address online bystanders in the cyber environment?	No	No	No	No	No
Are there are any training programmes/facilities to address issues arising from the online bystander?	No	No	No	No	No
Are there any relationships established with service providers concerning the online bystander and any public awareness?	No	No	No	No	No
Is there technical and infrastructure security to address issues relating to the online bystander?	No	No	No	No	No
					No

Country analysis	Zambia	Sierra Leone	Mauritius	Malawi	Cameroon	Seychelles	The Gambia
Does the country recognise online bystanders as role occupants in cybercrimes?	No	No	No	No	No	No	No
Has the country/ jurisdiction published an online bystander on cybercrime national strategy?	No	No	No	No	No	No	No
Has the country put legislation or regulations that address online bystanders in the cyber environment?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are there any training programmes/ facilities to address issues arising from the online bystander?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Are there any relationships established with service providers concerning the online bystander and any public awareness?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Is there technical and infrastructure security to address issues relating to the online bystander?	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Country analysis	South Africa	Eswatini	Botswana	Lesotho	Mozambique
Does the country recognise online bystanders as role occupants in cybercrimes?	Yes	No	Yes	No	No
Has the country/jurisdiction published an online bystander on cybercrime national strategy?	No	No	No	No	No
Has the country put legislation or regulations that address online bystanders in the cyber environment?	Yes, but not very specific	Yes	Yes	No	No
Are there are any training programmes/facilities to address issues arising from the online bystander?	No	Not clear	Not aware of these	No	No
Are there any relationships established with service providers concerning the online bystander and any public awareness?	Key initiatives led by UNICEF, Save the Children and government on online child violence	No	Yes	No	Not clear
Is there technical and infrastructure security to address issues relating to the online bystander?	No	yes	No	No	No

Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

thecommonwealth.org

The Commonwealth

D19114