TRAINING MODULE

Technology Facilitated Sexual and Gender-Based Violence, Gendered Online Hate Speech, Laws & Response Mechanisms

Centre for Equality and Justice

CitW

Design and layout by Know Us Art (Pvt) Ltd

Printed and published in February 2023.

For further information please contact:
Centre for Equality and Justice
37/2, Elibank Road, Colombo 05, Sri Lanka.
Tel/Fax: +94 11 2055404
email: srilanka.cej@gmail.com

ISBN 978-624-5847-26-6

LIST OF ABBREVIATIONS

CEDAW	Committee on the Elimination of Discrimination Against Women
CCID	Computer Crimes Investigation Division
CCU	Cyber Crimes Unit
CID	Criminal Investigation Department
TFSGBV	Technology Facilitated Sexual and Gender-Based Violence
DIG	Deputy Inspector General
GBV	Gender-Based Violence
GOHS	Gendered Online Hate Speech
IASC	Inter-Agency Standing Committee
IBSA	Image-Based Sexual Abuse
LGBTQI+	Lesbian, Gay, Bisexual, Transgender, Queer, and Intersex
MLA	Mutual Legal Assistance
NCII	Non-Consensual Intimate Images
NCPA	National Child Protection Authority
SGBV	Sexual Gender-Based Violence
SLCERT	Sri Lanka Computer Emergency Readiness Team
SLMA	Sri Lanka Medical Association
SOGIESC	Sexual Orientation, Gender Identity, Gender Expression and Sex Characteristics
UN	United Nations
UNFPA	United Nations Population Fund
WHO	World Health Organization
WIN	Women in Need

CONTENTS

Introduction

This module is the product of a 4-month research exercise facilitated by the Center for Equality and Justice (CEJ) with the aim of enriching the digital literacy of organizations and institutions responding to Technology Facilitated Sexual and Gender Based Violence (TFSGBV). In July 2025, edits were made to update this module and include new developments on TFSGBV.

2 Background :

Understanding Technology Facilitated Sexual and Gender Based Violence (TFSGBV) and Gendered Online Hate Speech (GOHS)

Broadly, TFSGBV is a form of sexual violence which is predicated on the gender of the victim and carried out online, while GOHS is a form of violence carried out online and is premised on hate which is manifested as bias towards a specific gender. Both, TFSGBV and GOHS, are distinct forms of violence that come within the umbrella term of Gender-Based Violence (GBV) and contain components of Sexual Gender-Based Violence (SGBV). As such, in order to understand TFSGBV and GOHS, we must first understand GBV and SGBV.

2.1 What is GBV & SGBV?

SGBV is a part of a large body of violence understood as GBV. GBV is physical and/or emotional (psychological) harm carried out through various actions which are directed towards a specific gender or gender minority. The Inter-Agency Standing Committee (IASC), the longest serving humanitarian coordination agency of the United Nations (UN), defines GBV as:

"Gender-based violence (GBV) is an umbrella term for any harmful act that is perpetrated against a person's will and that is based on socially ascribed (i.e. gender) differences between males and females."[1]

Types of GBV includes Sexual Violence, which is defined by the World Health Organization (WHO) in its World Report on Violence and Health as:

"Any sexual act, attempt to obtain a sexual act, unwanted sexual comments or advances, or acts to traffic, or otherwise directed, at a person's sexuality using coercion, by any person regardless of their relationship to the victim, in any setting, including but not limited to home and work."[2]

SGBV is therefore, any unwanted sexual act obtained or attempted to be obtained or committed against the victim without the victim's consent, using coercion that is carried out purely based on the sex or gender of the victim. These acts could include unwelcome comments of a sexual nature. Coercion includes use of force, blackmail, psychological intimidation, and various threats such as denying a job, causing physical harm, injury to family members or close associates etc.

[1] Jeanne Ward and Julie Lafrenière, Guidelines for Integrating Gender-Based Violence Interventions in Humanitarian Action: Reducing Risk, Promoting Resilience and Aiding Recovery. (: Inter-Agency Standing Committee 2015)

[2] Etienne G. Krug et al. (eds), World report on violence and health (World Health Organization, 2002).

SGBV can occur in both the private and public spaces and can be committed by known persons and unknown persons. Though SGBV is commonly considered as violence that is committed against women, it is also directed at men and persons of the LGBTQI+ community. SGBV plays out upon a power inequality, where the victim has less power (or is powerless in most circumstances when concerning children, women, refugees, persons of the LGBTQI+ community etc.) and the perpetrator or aggressor has the power.

The root cause of SGBV has been identified as patriarchy and the traditional gender norms defined by generations of patriarchy. The power and sense of superiority entertained by males as a result of patriarchy and the primacy afforded to men within the framework of patriarchal gender norms encourages and prompts GBV. Most commonly, SGBV is carried out either to impose the traditionally identified roles and characteristics pertaining to men and women on biological males and females who reject or rebel against these gender norms or in order to control or punish women and persons with diverse sexual orientation, gender Identity, gender expression and sex characteristics (SOGIESC). As a result, SGBV is most often committed by men against women and persons with diverse SOGIESC. However, there are also instances where SGBV is committed by women in order to perpetuate patriarchal gender norms.[3] Therefore, SGBV targets women, persons with diverse SOGIESC, and feminized bodies who do not conform to these traditional notions or who need to be brought within the folds of the traditional norms.[4]

Victims subject to SGBV, women and girls as well as men and boys, suffer mental trauma leading to psychological problems and psychiatric illnesses, physical trauma such as injuries to the body and genitals, and health risks such as HIV-AIDS and Sexually Transmitted Diseases and infections. In addition, women and girls subject to SGBV also suffer particular health risks such as unsafe abortions (carried out in order to terminate unwanted pregnancies), complications from pregnancies (especially in young girls) and injuries to the reproductive system. In countries where discussions of sexual health are taboo and the national health care system is stretched, these risk factors also pose an additional strain on the national health care system and a more severe risk to the victims.

[3] Female Genital Cutting (FGC) or Female Genital Mutilation (FGM) is an excellent example of women committing SGBV in order to uphold patriarchal gender perceptions.

[4] It must be noted that men and boys too are not safe from SGBV. The IASC has identified GBV as occurring amongst men and boys as well: “The term ‘gender-based violence’ is also increasingly used by some actors to highlight the gendered dimensions of certain forms of violence against men and boys—particularly some forms of sexual violence committed with the explicit purpose of reinforcing gender inequitable norms of masculinity and femininity (e.g. sexual violence committed in armed conflict aimed at emasculating or feminizing the enemy). This violence against males is based on socially constructed ideas of what it means to be a man and exercise male power. It is used by men (and in rare cases by women) to cause harm to other males.”

2.2 What is TFSGBV?

Technology Facilitated Sexual and Gender-Based Violence refers to the online manifestations of SGBV. In other words, it refers to the sexist, anti-LGBTQI+ and misogynistic attacks, with a sexual connotation, that are carried out via technology, largely targeting women, girls and persons with diverse SOGIESC. TFSGBV is the use of digital tools such as social media and communication technologies to harass, bully, humiliate, frighten, coerce or in some way harm an individual by conducting activities through social media or information technology communication systems specifically targeting the particular individual. TFSGBV can even be perpetrated through analog or 'button' phones, through harassing or threatening calls and text messages.

There are three main types of digital platforms used in the perpetration of TFSGBV. These are social networks, media sharing platforms and messaging platforms. Social networks are platforms such as Facebook, which are used to connect with people and to share information, ideas and knowledge. Media sharing platforms, such as Instagram, are used to share media content such as photos and videos. Meanwhile, messaging platforms like WhatsApp are used primarily to communicate with each other, and provide facilities to send and receive text messages, and make voice and video calls.

TFSGBV is therefore the use of digital means (a digital platform) to commit any non-consensual sexual act or to obtain or attempt to obtain a sexual act, through coercion, based purely on the gender of the victim. The objective of this action may vary from revenge, to controlling the victim (most often a woman), and to causing embarrassment, shame, instilling fear etc.[5] As with SGBV the perpetrators of TFSGBV could be someone known to the victim, such as a close friend, relative, intimate partner, former intimate partner, a peer, or someone unknown.[6]

TFSGBV, for example, includes sending unwelcome messages with sexual connotations or explicit sexual messages through email or social media (cyber flashing); sending unwelcome messages of a sexual nature through social media, communication applications or text messaging (unsolicited sexting); using duress or coercion to obtain nude pictures or sexually explicit videos (sextortion); unauthorized distribution of intimate photos of a sexual nature or nude photos (image based sexual abuse); and creating fake profiles for the use of activities of a sexual nature in order to harass, bully, shame and threaten the targeted person.[7]

[5] 'Gender Based Interpersonal Cyber Crime' (UNODC, February 2020) <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/gender-based-interpersonal-cybercrime.html> accessed 05 March 2023.

[6] ibid.

[7] Ibid.

2.3 What is Gendered Online Hate Speech (GOHS)?

GOHS comes within the umbrella term of TFSGBV, which in turns comes under the umbrella term of GBV. GOHS encompasses communication expressed either by way of writing, speaking or through behaviour that attacks a person or groups of persons in a derogatory, humiliating and harmful manner because of their race, religion, gender or such other distinguishing and differentiating feature/s.

GOHS includes behavioural, verbal or written expressions which intend to vilify, humiliate, and/or incite hatred or violence against a person or group of persons on the basis of their sexual and/or gender identity. The root cause for GOHS is a hatred towards women and persons with diverse SOGIESC based on gendered norms and expectations, and the sense of power and superiority entertained by males (and accepted by some women) in this patriarchal society.

In Sri Lanka, sex workers, migrant workers, women politicians, women human rights defenders, other women and feminized people who have a public presence are more likely to be targets of GOHS. A lot of the time this 'hate' is misogynistic and is derived from the notion that these women are traversing gendered norms. For instance, sexual agency and public denouncement of the gendered status quo usually face retaliation through campaigns of hate speech.

Apart from being a weapon to attack women and girls and persons with diverse SOGIESC, GOHS is also used to attack entire ethnic and religious groups. This is frequently used in Sri Lanka against the Tamil and Muslim communities where GOHS responses are racialized and ethnicized. It is also to be noted that these attacks are very often launched against female members of these ethnic and/or religious groups. In the recent spate of GOHS against the Muslim community, especially post Easter-bombings, one would notice that the attack is made on the feminized body and the female gender (such as the wearing of the hijab, sterilization tablets in kotturoti, female underwear causing sterilization etc). In circumstances such as these, GOHS does not only pose a threat to the physical safety of the individual. Instead, the entire group of persons who are symbolized by the individual or female image subject to GOHS is exposed to a security threat. For example, when memes of Muslim women wearing hijab with words displaying GOHS are circulated through social media, it incites hatred and suspicion towards the Muslim community as a whole, but more specifically against Muslim women, exposing them to a real risk of harm.

While many assume GOHS to be just harmful speech, in a context where the link between online expression and offline violence is well-established, GOHS is in fact dangerously capable of transcending to the offline space. This results in the hatred and humiliation spouted via digital platforms against religious or ethnic groups or persons with diverse SOGIESC being directed toward inciting people against these religious or ethnic groups and sexual minorities, thereby facilitating the physical manifestation of the online hate speech resulting in physical harm to these persons.

2.4 Prevalence of SGBV and Internet Penetration in Sri Lanka

In post war Sri Lanka, the prevalence of a culture of violence is unmistakable. A 2013 study conducted by Care International Sri Lanka on masculinities and GBV found that a majority of men related manhood to dominance and violence. It also found that being "tough" was understood to be manly and that there was greater acceptance, by both men and women, of masculinized violence and the use of male force. [8] This general acceptance of masculinity as being defined by dominance and violence, has become the foundation upon which violence against women occurs in Sri Lanka, leading to SGBV. In addition, years of war have created breeding grounds for ethno-nationalism, polarization of ethnic and religious communities, and militarization of the society, which has further compounded the severity of SGBV with intersections of ethnoreligious identity, caste, and class.

The study conducted by Care International Sri Lanka also found that 20% of men, aged 18 – 49, admitted to having perpetrated sexual violence on their intimate partner, whilst 6.2% of men admitted to subjecting a non-partner to sexual violence.[9] What is also evident is the systematic sexualization, objectification, violation and harassment of women and other feminized bodies within both public and private spaces in Sri Lanka. According to a survey conducted by the UNFPA in 2017, 90% of women and girls have been subjected to sexual harassment on public transport, [10] while 1 in 4 women (24.9%) over 15 years of age have been subject to sexual violence either by known or unknown persons.[11] Numerous research studies conducted over the years have proven that SGBV directed towards women does not escape any sector of society. A study conducted by the Sri Lanka Medical Association (SLMA) in 2011 found that women in the plantation sector, free trade zones and industrial sector are subject to SGBV at the workplace, whilst research conducted in institutions of higher education in Sri Lanka (State universities) found that both female and male students are subject to SGBV within the university structure and that SGBV was clearly prevalent in the system of ragging.[12]

[8] De Mel Neloufer, Peiris Pradeep and Gomez Shyamala, 'Broadening gender: Why masculinities matter?: Attitudes, practices and gender-based violence in four districts in Sri Lanka' (Care International Sri Lanka, 2013).

[9] ibid.

[10] Population Matters, 'Sexual Harassment on Public Buses and Trains in Sri Lanka' (UNFPA Policy Brief, March 2017) < https://srilanka.unfpa.org/sites/default/files/pub-pdf/FINAL%20POLICY%20BRIEF%20-%20ENGLISH_0.pdf > accessed 05 March 2023.

[11] Department of Census and Statistics. Women's Wellbeing Survey – 2019 (2020).

[12] Sri Lanka Medical Association (SLMA), Review of Research Evidence on Gender-Based Violence in Sri Lanka (2011); University Grants Commission (UGC), Center for Gender Equity and Equality & UNICEF, Prevalence of Ragging and Sexual and Gender-Based Violence in Sri Lankan State Universities (2022).

Within this culture of male dominance and violence which is perpetuating SGBV, TFSGBV also takes place and is largely facilitated by a majority of the population having access to the internet. As of January 2022, Sri Lanka's internet penetration rate stood at 56.3 percent of the total population at the start of 2024. Kepios analysis indicates that internet users in Sri Lanka increased by 460 thousand (+3.9 percent) between January 2023 and January 2024[13]. Furthermore, in Sri Lanka too, as has been observed globally, the lockdowns resulting from the COVID-19 pandemic has led to an increased use of internet and social media supported by the rapid adoption of smartphone usage. DataReportal reported that 98.8% of the social media users in Sri Lanka access it via smartphones and that out of the recorded 8.20 million social media users, 36.6% are female and 63.4% are male. It is also interesting to note that Sri Lanka has 32.29 million cellular mobile connections which is 149.9% of the population, indicating that one individual owns more than one mobile sim due to the unavailability of mobile number portability.

This rapid increase in smartphone usage is also contributing towards a sharp increase in TFSGBV. A combination of factors such as a lack of knowledge in data security, increased smartphone usage amongst teenagers, and a lack of regulation over online offences have given rise to increases in TFSGBV. Non-consensual intimate image (NCII) sharing, sextortion, doctored images and deep fakes,[14] and social media account impersonation are among the most common forms of TFSGBV observed in Sri Lanka. These incidents of TFSGBV occur predominantly on social media sites such as Facebook and Instagram, and messaging platforms like WhatsApp.

Despite a growing awareness of TFSGBV and its impacts, glaring gaps in digital literacy, normalization of violence against women, and a culture of victim-blaming have eclipsed much of the mitigation efforts. TFSGBV persists at high frequencies among young, school-aged populations across the country, pointing to how it also alarmingly overlaps with the sexual exploitation of children online.

TFSGBV is the fastest growing form of gendered violence in Sri Lanka [15] with women and girl children being the most prominently targeted. A 2000 study by Women in Need found that 1 in 3 women knew a victim of some form of TFSGBV, a testament to how closely online and offline violence mirror each other and transpire from common gendered norms. A joint national research study conducted by the State Ministry of Women and Child Development, Word Vision, and Save the Children revealed that at least 28% of children have experienced some form of cyber-violence, which includes being exposed to 'indecent messages', while 20% of children have had an 'indecent' image of theirs shared on the internet without consent.[16]

[13] Simon Kemp, 'Digital 2024: Sri Lanka' (Datareportal, 23 February 2024) <https://datareportal.com/reports/digital-2024-sri-lanka > accessed 01 September 2025.

[14] Deep fakes are synthetic media in which a person in an existing image or video is replaced with someone else's likeness, by using AI.

[15] Dinithi Gunasekera, 'Online gender-based violence: The new normal of sexual harassment' (The Morning, 28 February 2021) < https://www.themorning.lk/online-gender-based-violence-the-new-normal-of-sexual-harassment/ > accessed 05 March 2023.

[16] Save the Ch ildren et al., Online Violence Against Children in Sri Lanka (March 2022) < https://srilanka.savethechildren.net/sites/srilanka.savethechildren.net/files/Online%20Violence%20Against%20Children%20in%20Sri%20Lanka.pdf > accessed 05 March 2023.

The number of reported cases of TFSGBV have steadily risen over the years,[17] with law enforcement agencies attempting to keep up with rising numbers in the face of increasing digital penetration, increased usage of newer platforms, and more recently, the COVID-19 pandemic. The most recent addition to enforcement mechanisms includes a Special Unit to tackle online child sexual exploitation content, [18] which was in response to a serious case of online child trafficking of a 15-year-old girl.[19]

The increasing popularity of messaging apps such as WhatsApp and Telegram have unfortunately allowed for extensive, covert networks for NCII and video sharing. The specific prevalence of such networks amongst schoolboys is well-documented, where young boys join and usually participate due to peer pressure, and engage in the systematic targeting of their female peers. The humiliation and degradation of women and girls appearing in these 'leaked' content are also rampant on social media. Meme culture has become an increasingly common way for social media users to find creative ways of harassing victims while evading the radar of community standards. Furthermore, social media and other digital tools also provide a platform, sometimes also protected by anonymity, for hate speech to be unleashed using the female as the object or against the LGBTQI+ community.

2.5 Human Rights Violations

It is also important to recognize that SGBV are serious violations of human rights. Numerous international covenants recognize the right to life, the right to be free from torture, inhuman or degrading treatment or punishment, the right not to be discriminated on the basis of gender, race, political opinion or sexual orientation (amongst others), the equal protection of the law, the right to express themselves freely and the right to a private family life, as human rights. The physical injuries, psychological trauma and discrimination women are subject to as a result of SGBV, and by extension TFSGBV and GOHS, have been recognized by the United Nations, the Council of Europe and other regional human rights protection systems as violating these human rights.[20] The Committee on the Elimination of Discrimination Against Women (CEDAW) has categorically recognized that SGBV violates, amongst others, womens' right to life, freedom from torture, cruel, inhuman or degrading treatment or punishment and the right to liberty and security of person.[21]

[17] Sumudu Chamara, 'Unsafe outside, unsafe online' (The Morning, 13 March 2022) <https://www.themorning.lk/unsafe-outside-unsafe-online > accessed 05 March 2023.

[18] Pavani Hapuarachchi, 'Special Police Unit to crack-down on Child Pornography' (Newsfirst, 29 July 2021) <https://www.newsfirst.lk/2021/07/29/special-police-unit-to-crack-down-on-child-pornography/ > accessed 05 March 2023.

[19] Bhavani Fonseka, 'The Growing Dangers of Online Sexual Exploitation of Children' (Groundviews, 20 November 2021) <https://groundviews.org/2021/11/20/the-growing-dangers-of-online-sexual-abuse-of-children/ > accessed 05 March 2023.

[20] Council of Europe, Explanatory Report to the Council of Europe Convention on Preventing and Combatting Violence Against Women and Domestic Violence (Council of Europe Treaty Series No: 210); UNGA, 'Discrimination and violence

[21] UN Committee on the Elimination of Discrimination Against Women (CEDAW), CEDAW General Recommendation No. 19: Violence against women, 1992 <https://www.refworld.org/docid/52d920c54.html > accessed 27 January 2023.

The United Nations has also recognized SGBV committed against the LGBTQI+ community as a violation of their human rights.[22] An obligation and duty cast upon the State through international legal obligations and the United Nations framework encourages them to proactively and consciously ensure the protection of the rights of women and similarly the rights of LGBTQI+ persons. As such, States must, at the very least, ensure equal protection of the law by setting up legal mechanisms to bring perpetrators before the law and to prevent the occurrence of SGBV.

The constitution of Sri Lanka in its Fundamental Rights chapter recognizes a person's right to be free from torture, inhuman, degrading treatment or punishment and the right to equal protection of the law. Where the State fails to enact effective laws, or fails to investigate and prosecute persons committing SGBV activities such as, but not limited to, subjecting a victim to fear for their safety or the safety of relatives or friends, causing psychological trauma, distributing intimate photos without consent, obtaining sexual favours under duress or coercion through digital platforms, the State has failed to ensure equal protection of the law and the right to be free from torture, degrading or inhuman treatment or punishment.

3 Types of TFSGBV

3.1 Non-Consensual Intimate Image (NCII) Sharing leading to Image-Based Sexual Abuse (IBSA) (Commonly called 'Revenge Pornography')

The advent of social media has monumentally changed the ways in which we communicate and build relationships, and this extends to romantic and sexual relationships. However, a general lack of awareness of cyber safety and consent has resulted in online platforms becoming hotbeds for the creation, sharing, and dissemination of NCII and videos.

[22] UN Human Rights Office of the High Commissioner, Born Free and Equal: Sexual Orientation, Gender Identity and Sex Characteristics in International Human Rights Law (2nd edn, United Nations 2019).

Activists and law enforcement concur that NCII sharing is the most extreme form of TFSGBV in Sri Lanka. The term ‘revenge pornography’ is rapidly being phased out due to its implication of victim-blaming and the presumption that the violence prerequisites an intention to exact revenge. Furthermore, revenge porn is not the only intention of NCII sharing. NCII sharing, which leads to IBSA, also includes the threat of sharing intimate or compromising images as much as the actual sharing of these images online. Motives for NCII sharing (or IBSA) also include blackmail or extortion to obtain sexual favours and monetary gain from the victim, voyeurism, sexual gratification and control.[23] Other forms of NCII sharing leading to IBSA is “up-skirting”, which is taking an image up a woman’s skirt, or “down-blousing”, which is taking a photo of a woman down her blouse, and circulating or publishing these images on digital platforms. In addition, NCII sharing and IBSA occur through the secret filming or taking of photos in public or private places via hidden cameras and “cyber-flashing”, which is exposing oneself by sending images on digital platforms.

In Sri Lanka, a significant amount of online NCII sharing is the outcome of a soured romantic or sexual relationship, and frequently targets women and girls. Cases of people building purely online relationships only to later have their NCII shared by individuals on the other side of the screen have also been reported in Sri Lanka. In cases like this, the overarching goal is the sexual exploitation of the victims. The broad observation made here relates to the weaponization of sexuality to cause reputational and psychological harm to the victim.

3.2 Morphing - Doctored Images/Videos

Another common form of TFSGBV is “Morphing”, where an image of the victim’s face is superimposed onto the bodies of others. Generally, this involves the digital morphing of the faces of a victim onto nude torsos and creating obscene images, thereby humiliating and defaming the victim. TFSGBV in the form of morphing also includes the creation, proliferation, or threats of proliferation of morphed images and videos. The development of face morphing software programs has intensified the reputational harm and psychological trauma caused through morphing. Software applications such as ‘deep fake’ video creation, which uses a machine-learning algorithm to replace the faces in videos, has made morphing increasingly easy over time, with such manipulated videos even being released onto commercial pornography sites. As discussed, doctored images and videos are mostly used to cause reputational harm to victims, with financial motivations either being absent or largely a secondary aspect.

[23] Gender Based Interpersonal Cyber Crime’ (UNODC, February 2020) <https://www.unodc.org/e4j/en/cybercrime/module-12/key-isues/gender-based-interpersonal-cybercrime.html > accessed 05 March 2023.

3.3 Doxxing

Doxxing (also known as doxing) refers to “unauthorized personal information exposure” online. It is the online publishing of actual private and confidential information and/or information identifying a person, such as personal phone number, work phone number, workplace, home address, photo, family information and even financial information without the consent of the owner of such information (the victim).

Doxing is carried out usually with an intention of threatening, bullying or causing or inciting harm to the victim. The motivation for doxing is either to exact revenge, is a result of online vigilante, body shaming or directed in the form of an attack on someone whose opinions/beliefs are considered intolerable. A common form of this occurring in Sri Lankan cyberspace is the sharing of contact information (and sometimes the workplace) of women and girls along with their photograph. This is usually accompanied with a description of the woman projecting her in a compromising, humiliating or derogatory situation and inviting the public to contact her. This harassment not only defames the woman/girl and causes her mental trauma, but also leads to her being sexually abused.[24] However, this does not mean that the victims of doxxing are exclusively women and girls. It must be noted that doxxing can happen to anyone, regardless of gender or sexual orientation. Given that doxxing exposes private details such as workplace, home and other personal information, which can be used to track down the victim, it can also lead to physical harassment and physical harm to the victim.

‘Outing’ is also a form of doxing that targets the LGBTQI+ community. It involves the publishing of someone’s sexual orientation and gender identity, sometimes along with private information. This could have grievous consequences due to prevailing negative attitudes towards the LGBTQI+ community within Sri Lanka that have led to transphobic and homophobic attacks against them.

3.4 Sextortion

Sextortion is a form of cyber blackmail that constitutes a form of sexual exploitation. This involves the perpetrator threatening to release private, personal, and at times compromising information including but not limited to explicit private images, videos and/or conversations of the victim, if the victim does not provide the perpetrator with his demands, which are usually sexual favours, nude photos, videos and money. A perpetrator carrying out sextortion threatens to release explicit or intimate content with family, friends, employers

[24] A common form of doxing is publishing the photo along with the phone number of the female projecting her as a sexual worker or masseuse and inviting persons to call her for “appointments”.

or other persons known to victims, there by threatening the victim with humiliation, embarrassment and defamation of their character. As such, the aim is to isolate and manipulate the victim by weaponizing the stigma caused by TFSGBV and the fear of losing close familial, social, and communal ties that the victim cherishes.

3.5 Fake Profiles and Impersonation

Anonymity online is a double-edged sword. It can be a safe haven for those that do not wish to have a public presence or digital footprint online. Unfortunately, within the context of CSGBV, fake profile creation and impersonation have presented a seriously troubling pattern of behaviour in Sri Lanka's cyberspace.

The most common forms of these patterns include the creation of social media fake profiles using images and/or personal details of a victim and impersonating them online. The perpetrator will use personal information of the victim, which is obtained either by searching for the victim's social media accounts or which the perpetrator is already privy to through an intimate relationship with the victim, to create a fake social media profile of the victim. The perpetrator will thereafter proceed to send friend requests to the victim's friends and family. After adding them to the fake profile, the perpetrator will share defamatory content created by the perpetrator as well as private images, intimate images and videos of the victim in the fake profile, causing humiliation, embarrassment, defamation of character and sometimes leading to the victim losing family relationships and friendships. In addition, the perpetrator will attempt to seek financial gain by requesting money from the friends and family added to the fake profile. These fake profiles are also created exclusively to share NCII and engage in other forms of sexual exploitation such as doxing and morphing, effectively avoiding accountability both online and offline.

Another dimension of fake profiling, is when a perpetrator, for purposes of anonymity, creates a fake profile using images from the social media pages of an individual, sometimes under a name that is not of the person to whom the images belong to. These types of fake profiles are created most often to groom and lure children, young adults and women into sexual activity, which leads to sexual abuse both offline and online. In addition fake profiles, relying on the safety of anonymity, are used to request money by resorting to coercion or duress.

4 Objective of the Module

This module is situated within the aforementioned context and is derived from a 4-month assessment of current mechanisms set in place to report and respond to TFSGBV. It intends to highlight the functions of key State law enforcement agencies and non-State organizations that are crucial points in the pipeline and to identify the gaps in the process of accessing justice for victims.

Since the victimhood of TFSGBV is significantly gendered, a central question of the assessment was whether these institutions had a gendered approach to TFSGBV - either codified or entrenched through conscious practice. Investigation into what institutions understood to be a gendered approach, what factors were considered when such an approach was designed, and the barriers to the successful execution of approaches were also considered.

The other focus of this module is to review the digital literacy of key stakeholders. As technology is the foundation on which malpractices take place, uplifting the technological capabilities of the key stakeholders will predictably have a direct impact on preventing and remedying GOHS and TFSGBV, and thereby improve responses. With hate speech targeting females or persons with diverse SOGIESC, the online environment has become unsafe and dangerous for women, girls and persons with diverse SOGIESC. It must also be kept in mind that hate speech, which is abusive, offensive and angry, is directed at women and girls where specific ethnic groups and religions are targeted.

In preparation for this module, desk research was conducted to identify the key stakeholders who respond to TFSGBV in Sri Lanka in capacities including, but not limited to, technical support, legal aid, psychosocial assistance, and research and training. Following this preliminary mapping exercise, two focus group discussions were conducted involving these stakeholders. These consultations were instrumental in identifying the ground realities of responding to TFSGBV and the manifest gaps in the existing mechanisms.

4.1 Key Observations

The Computer Crimes Investigation Division (CCID) attached to the Criminal Investigation Department (CID) is the premier law enforcement organ that deals with technology-related and social media-related crimes, which includes all forms of TFSGBV.

The Children and Women's Bureau attached to the Sri Lanka Police is also a key organ within the law enforcement institution responding to cases of TFSGBV, often in tandem with the CCID.The Bureau also responds to child sexual exploitation that happens online. A dedicated Bureau desk can be found at 44 Police divisions in the country recording and investigating SGBV cases.

Aside from the CCID and the Bureau, the response apparatus is composed of several civil institutions and non-governmental organizations, working in areas including research, legal aid, support services, technical assistance, as well as working directly with law enforcement.

4.2 Desk research

Preliminary desk research was conducted from October to December 2021 to map out the organizations and institutions that compose the TFSGBV response apparatus in Sri Lanka.

The mapping exercise identified 18 key bodies that engaged in several different forms of responses to TFSGBV. The data collection was a combination of primary input from representatives of the organizations and secondary research based on publicly available information.

The following information about each organization was gauged:

- The forms of TFSGBV each organization responded to,
- The response mechanisms deployed,
- The process of responding to a TFSGBV case,
- Training or specialization for responders/employees including, but not limited to, digital literacy and gender sensitization,
- Knowledge of data privacy, archiving, and recordkeeping,
- Barriers to responding to TFSGBV and/ or pursuing formal methods of justice and relief, and
- Language capacity and accessibility.

NCII/video sharing, cyber sexual exploitation and abuse, sextortion, and cyber harassment (including GOHS) were identified as the forms of TFSGBV most encountered and responded to. Threats were also identified by 4 organizations as incidents that they responded to.

With regards to response mechanisms, legal aid was the most commonly offered response mechanism. Nine organizations also confirmed that they provided further assistance with regards to the legal process, including help with filing a complaint and following up.

Nine organizations also confirmed that technical support was available for victims. This included helping with adjusting privacy settings on social media apps, blocking and removing fake profiles that impersonate or attempt to defame them, and bringing complaints to social media companies to get harmful content removed. Interestingly, only 4 organizations provided all three of these services.

14 of the organizations have trilingual accessibility for all services. Nine out of 18 organizations had some form of formal training for staff in one or more of the following: digital literacy, gender sensitization, and psychosocial support provision. However, only 3 organizations had the capacity to provide in-house psychosocial support for victims, with a single organization stating that a formalized procedure was instated to refer victims to external organizations that provided such services.

It was interesting to note that many of the institutions also provided digital security and gender sensitization workshops and training programs. A majority of this was either catered to women and girls or was inadvertently attended predominantly by women and girls. Only 1 of the organizations surveyed consciously worked with war-affected women and widows.

4.3 Focus Group Discussions (FGDs)

Following the desk research, two focus group discussions (FGDs) were conducted with the purpose of gaining more in-depth insight into the current scope of work responding to TFSGBV, and to identify whether a gendered approach is adopted within their response apparatus. The FGDs were also instrumental in establishing the baseline measure of digital literacy of organizations to inform the relevant component of this module.

4.3.1 FGD 1 - Public institutions

The first focus group consisted of representatives from law enforcement agencies and civil institutions including Sri Lanka Computer Emergency Readiness Team (SLCERT) and the National Child Protection Authority (NCPA). The primary objective of this discussion was to gather information on the approach of key State institutions working on cyber security, women's and children's affairs, and computer crimes, in relation to incidents of TFSGBV and GOHS.

The insights gained through this discussion about the current situation of TFSGBV in Sri Lanka, with regard to law enforcement, are as follows:

- The most frequent form of TFSGBV reported is the sharing of NCII and videos. A majority of the cases involved a perpetrator and complainant who were formerly in a romantic or sexual relationship. The motive of revenge was present in most cases.

- A majority of these complaints also included threats and/or attempts of sextortion with the perpetrator demanding more sensitive content, sexual favours and money. The most frequently sought assistance was the removal of compromising images/videos/content from platforms.

- While a financial motive was rare in sextortion cases involving former partners, the monetization of non-consensual intimate material has rapidly increased, with perpetrators selling such content on commercial pornography sites and social media pages.

- There is heavy stigma and victim-blaming surrounding complainants, especially from immediate family. This is acute in cases of non-consensual intimate material sharing and sextortion.

- Alarmingly, the hostility is also evident in cases with minor complainants. One of the respondents shared a case where a 13-year-old girl submitted a complaint alleging a perpetrator had held her at knife point and taken compromising photos of her. However, upon further investigation, it was discovered that she had voluntarily sent the photos to the perpetrator who was now using the images to ‘sextort’ her. The minor had not revealed the full truth for fear of being reprimanded or shunned by parents. The respondent noted that this case was an illustration of how stigma leads to victims not coming forward in full, often concealing details to avoid further traumatic treatment from close networks, which then impede investigation processes.

- A chronic lack of awareness about TFSGBV and available response mechanisms is ever-present, especially in rural areas and outside the Colombo District. In the event that the victim is a minor, the lack of awareness about response mechanisms on the part of the parents or adult guardian causes setbacks in terms of harm reduction.

- When complaints arrive at law enforcement agencies it is often ‘too late’. The reluctance to come forward due to fear of being ostracized and the lack of awareness about what to do are the main factors for these delays. Technical difficulties in retrieving data and evidence from devices also arise due to such delays or because complainants accidentally tamper with the device/evidence.

- The prevalence of TFSGBV has risen steadily over the years, with an astronomical leap between the years 2019 and 2020 (due to COVID-19). Those between the ages of 13 - 25, often girls and women, are most vulnerable. Most complaints received are from school-going children.

- Unemployed, stay-at-home women and children of migrant workers are also highly vulnerable groups. It was noted that women who spend a majority of the time in the household during the day are more likely to spend larger amounts of time on social media, and often become victims of TFSGBV and even financial scams.

- The lack of adequate adult supervision was a contributing factor to the high prevalence of TFSGBVagainst children of migrant workers. Respondents noted that these children were often left in the care of secondary guardians such as grandparents, whose knowledge on digital safety and/or response mechanisms to TFSGBV are likely to be extremely low.

- Due to the closure of schools during COVID-19 and due to the limitation imposed on socialization as per health protocols, children spent more time online without proper knowledge on cyber safety. The use of WhatsApp groups for school-related communication without sufficient know-how on digital safety has posed a significant problem of other adults posing as children or parents gaining access to these groups. Perpetrators gather open-source information such as contact details and photographs of minors, which are used to harass, blackmail, and even sextort minors.

- Men and boys are also subjected to TFSGBV, but it is spoken about less in Sri Lanka. A specific trend that has emerged in recent times includes women initiating sexual conversations, including video calls, with men, and later using the explicit exchanges to blackmail the men.

- The lack of comprehensive sexual and reproductive health and consent education contributes to minors and women being more vulnerable to TFSGBV. The coinci-dence of natural sexual curiosity during adolescence with access to a digital device often happens without any comprehensive knowledge on digital literacy, cyber security and consent.

- Respondents also stressed the importance of protecting the mental and emotional wellbeing of the affected party and their family, especially where the victim is a minor. Inadequacies in gender-sensitivity training and the overarching dismissive attitudes towards psychosocial services have made implementation difficult. The need for a more gender-sensitive judicial process was also raised to avoid victims being traumatized.

- Despite the availability of help desks across the island, the ease of accessibility for reporting is still limited outside Colombo, often affecting the exact areas where women and girls are most vulnerable.

- With regards to institutional knowledge base and capacities, the consensus was that while progress has been made in recent times there was still a broad lack of awareness about cybercrimes, TFSGBV and the legal context both within the police and other branches of State institutions operating outside of the capital, Colombo.

- Further barriers to ensuring effective responses included an inadequacy of specialized personnel (for areas such as information systems and forensic auditing) and the lack of knowledge amongst judicial officers and court systems about forensic data. The lack of up-to-date technology and devices available to law enforcement and other public institutions were also noteworthy barriers.

- The number of people employed to handle complaints at the public access call centers and hotlines designated for TFSGBV was inadequate. A coordination and communication gap between institutions was also recognized as a barrier to ensuring effective, streamlined responses to TFSGBV cases. Furthermore, a lack of awareness on the newer methods of reporting and responding also has detrimental effects on victims getting justice.

Gendered Approach

The respondents maintained that young girls and women were most likely to be the victims of TFSGBV, noting that the culture of victim-blaming was rather pervasive. With regards to how this informed their approach to cases, law enforcement agents pointed to the recently established online complaint service available through the Sri Lanka Police website.

They mentioned that this would alleviate the need for victims to visit a Police Station in person and record a complaint - a process that can be difficult, intimidating, and at times traumatizing. The subsequent internal process of handling the complaint has been streamlined to reduce congestion. This service is available in all three languages and complainants will be directed to the next steps by the local Police Station. Pursuing legal action is an option, and these online cases will be directed to the appropriate authority while the IT desk of the respective Police Station would be notified to provide preliminary technological assistance where required.

4.3.2 FGD 2 - Civil Society

The second FGD consisted of members of non-governmental civil society organizations that specifically responded to TFSGBV. Broadly, these organizations provided a plethora of services to victims of TFSGBV including legal aid, assistance with police reporting, technical assistance, and training and awareness programs.

Preliminary discussions established the following aspects with regards to the current context of TFSGBV in Sri Lanka:

- Non-consensual intimate image sharing was the most commonly reported form of TFSGBV. The perpetrator is often a male, a former partner or a jilted lover, who has an intention of exacting revenge, and/or causing reputational harm to the victim. Sextortion may also follow, usually demanding more material or sexual favours.

- The creation of fake profiles on Facebook intended to cause reputational harm and harass women and girls has been on the rise in recent times. This has reached the threshold for cyberstalking in some cases where perpetrators continue to spawn newer profiles and continue a relentless campaign of harassment. These campaigns may also involve sextortion and threats against the victim.

- Offline disagreements and sexual harassment may manifest online as harassment campaigns, including with the use of the victim's images and identifying information. Further, incidents have been reported where male colleagues resort to such cyber harassment often using fake profiles when offline sexual advances have proved futile in workplaces.

- Women and girls are most vulnerable to TFSGBV. Girl children and teenagers were specifically susceptible due to the disparity between increased access to smart phones and comprehensive digital literacy education.

- Cultural stigma about sexual violence and sexist notions about women and girls using the cyberspace combine in a dangerous way. Victims feel immense shame and are fearful of friends and family being privy to the violence committed against them. The fear of parents finding out is especially acute in younger women and girls due to potential reprisals and fear of ostracization from communities and support networks.

- Despite the existence of emergency hotlines, accessing services through these have proven to be difficult for some. Many victims approach civil society organizations when the public institutions have been unable to provide satisfactory redress or advice.

- While most victims seek assistance with removing content that targets them, the demand for legal advice remains at high levels. Despite this, victims are extremely reluctant to follow a formal legal procedure against perpetrators or even to receive some form of relief through law enforcement. Lodging a complaint is considered as a tedious process. This sentiment is due to a prior encounter with the police that did not result in a positive outcome. One respondent shared the following experience:

  "I have personally filed a complaint regarding a cyber harassment incident. They took around 2 months to call me to give a statement. Thereafter, the first officer I met told me that legal recourse may be futile for my case. All in all, the whole process took 5 hours, including for them to record my statement. At the end of it, I was not sure if I should even sign the Statement."

- Respondents also noted that the reluctance on the part of the police to pursue cases may also be due to a severe lack of knowledge about laws applicable to cybercrimes and cyber harassment.

- Some organizations accompanied victims to the Police Station for procedures such as filing a complaint, noting that the presence of a lawyer improves how the police receive and respond to the complainant, and a conscious effort is made to try and resolve the matter at the inquiry stage in order to avoid a prolonged process.

- With a lack of expeditious action from law enforcement, most women and girls resort to self-censoring or turning off their phones in order to avoid harassment. This indicates a serious gap in the current TFSGBV response pipeline that effectively leads to the silencing of women and girls.

- Respondents also noted that the reluctance to approach police where cyber offences were concerned was experienced by both men and women. Some also stated that more men might even be hesitant to report at all due to the patriarchal norms imposed on them.

Gendered Approach

“... fear they have is that people will engage in victim-blaming. The other fear is that they will be re-victimized or used by others if they reveal the incidents that have happened to them. There is also shame because of how society generally reacts to such unpleasant experiences. We have to inform society not to get caught in these traps and on how they can use social media carefully.”

When members were asked whether their organizations adopted a gendered approach when responding to TFSGBV many of them provided insights into their processes that indicated the affirmative. Several specific steps and considerations were informed by the knowledge that:

- It was mostly women and girls who were victims of TFSGBV,
- Cultural attitudes about sexual violence and victimhood often lead to an internalization of shame and stigma by victims, and
- A lack of awareness about the risks of cyber sexual violence, digital literacy, and specific laws meant that victims were at risk of falling through the cracks in the response apparatus.

As such, a gendered approach consisted of:

- Providing assistance in the form of legal advice and representation to women and girls when resorting to a formal legal process. This includes accompanying victims when visiting a Police Station, advocating for sensitive complaint processes and filing complaints on behalf of the victim in order to further minimize potentially traumatizing interactions with law enforcement.

- Awareness programs focused on encouraging women and girls to come forward with their experiences of TFSGBV. This includes information on possible avenues to respond to TFSGBV and the resources available. A gender-sensitive approach, informed by the complicated context, to encourage and empower women to lodge complaints instead of self-censoring was also noted.

- Actively advocating for gender sensitivity training for police and other State institutions working on TFSGBV. One respondent noted a positive incident where a woman police constable responded quickly and effectively to a complaint of TFSGBV, inferring that acknowledging police as a pivotal actor in this pipeline was as necessary.

- Seeking assistance and advice from other civil society organizations with better gender consciousness. This has proven to be helpful to provide victims with help while remaining sensitive to their plight.

5 TFSGBV Response Mechanisms

5.1 Background

Most complaints of TFSGBV are forwarded to the CCID as they are the primary authority in charge of enforcement of the law in relation to cybercrimes. In some instances, the Children and Women's Bureau of the Sri Lanka Police is able to handle cases themselves. Additionally, SLCERT, Ministry of Women, Child Affairs and Social Empowerment and National Child Protection Authority all redirect any cases they receive to the aforementioned two institutions.

The CCID is divided into several sub units, which includes:

- Social Media Unit
- Social Media Investigation Unit
- Intelligence and Surveillance Unit

Apart from its headquarters in Colombo, the CCID has three regional units in Ampara, Kandy and Matara.

5.2 Two-part approach

Schoenebeck, Haimson, and Nakamura (2020) [25] speak of two online governance tools that can be used to mitigate such online harassment and TFSGBV on social media platforms. These are:

1) Top-down approach: in this approach, the digital platform itself develops and sets out the policies and framework with regard to online harassment and the type of content that can be published;
2) Bottom-up approach: in this approach, the users themselves moderate the platform with regard to the parameters of conduct and content that can be published. They are vigilant of the content posted and report on any content which entails TFSGBV.

[25] Schoenebeck, S., Haimson, O. L., & Nakamura, L. (2021). Drawing from justice theories to support targets of online harassment. New Media & Society, 23(5), 1278–1300. https://doi.org/10.1177/1461444820913122

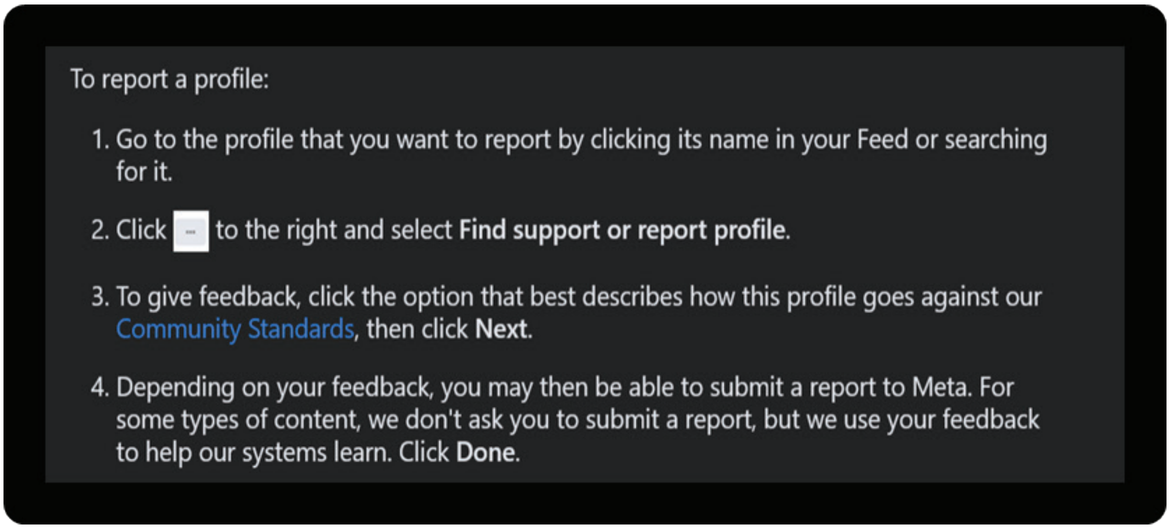
While many users inherently feel that platforms should govern and police content to feel safe, often it is not the case. Unlike on Reddit where subredditors can moderate the content that goes up on the page, Facebook and Instagram have their own teams of moderators to check whether or not the content adheres to the community guidelines. This could lead to certain harassment content going unchecked because it does not fit in their algorithm unless you especially report the content. Through platforms that rely on the bottom-up approach, strategies such as educating, sympathizing, shaming, and blocking users who create harassment content are enforced by the page's moderators, thus leading to a safe place for its other users.

5.3 Let's take a look at the reporting tools Facebook, Instagram, and YouTube are currently using in order to make their platforms safe from TFSGBV

5.3.1 Facebook

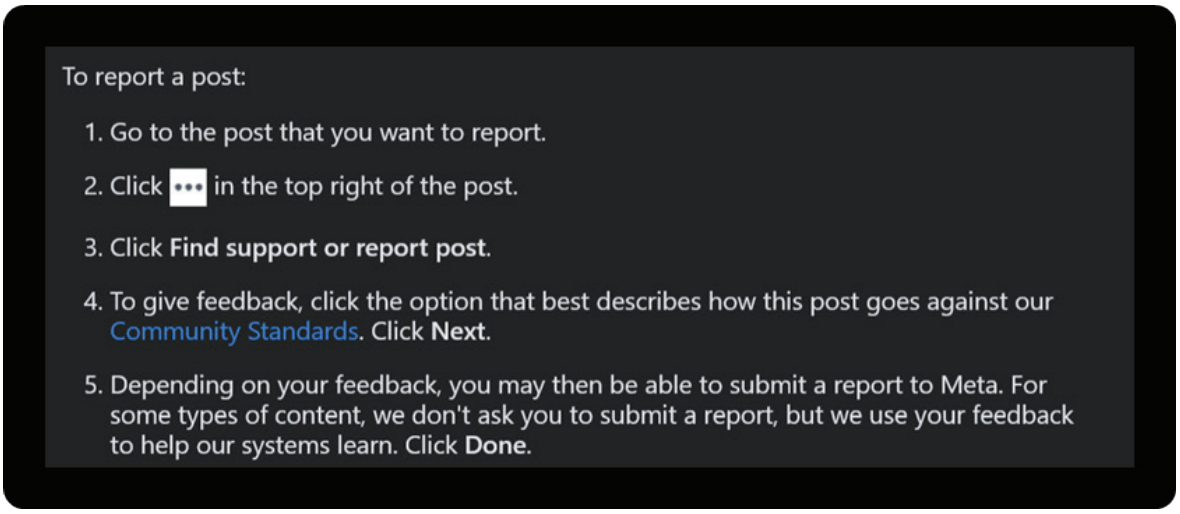
In the past years, the Facebook team has been cracking down on fake profiles to ensure the safety of their users. While their algorithms are created to block out harmful content or profiles, it is sometimes missed as bots do not fully grasp certain details. Due to this, users can manually report profiles, posts, comments, and other forms of content on Facebook.

How to report on Facebook?



To report a profile:

1. Go to the profile that you want to report by clicking its name in your Feed or searching for it.
2. Click ··· to the right and select **Find support or report profile**.
3. To give feedback, click the option that best describes how this profile goes against our Community Standards, then click **Next**.
4. Depending on your feedback, you may then be able to submit a report to Meta. For some types of content, we don't ask you to submit a report, but we use your feedback to help our systems learn. Click **Done**.



To report a post:

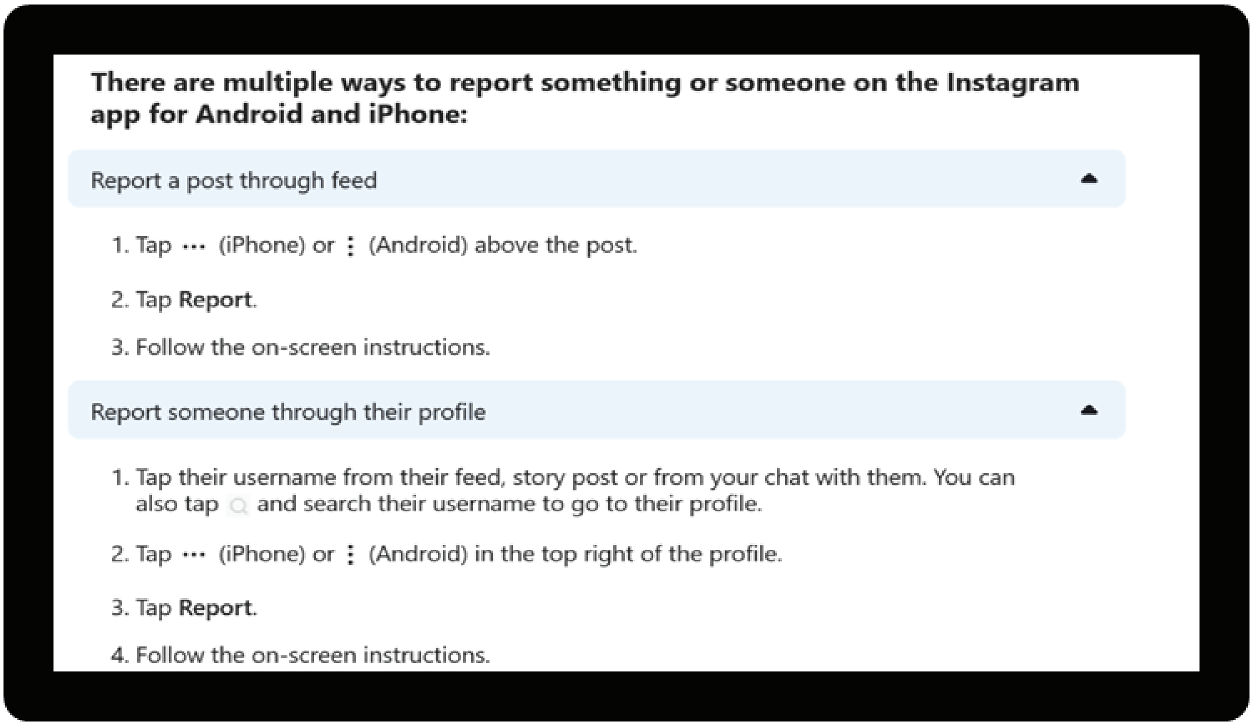
1. Go to the post that you want to report.
2. Click ••• in the top right of the post.
3. Click **Find support or report post**.
4. To give feedback, click the option that best describes how this post goes against our Community Standards. Click **Next**.
5. Depending on your feedback, you may then be able to submit a report to Meta. For some types of content, we don't ask you to submit a report, but we use your feedback to help our systems learn. Click **Done**.

The two images above explain how to report content or profiles according to the process provided in the Facebook Help Centre. Going further into the tool, Facebook offers a list of categories under which a user can submit a report.

Retain Evidence: In reference to the Facebook reporting systems set out above, it is advisable, as a best practice, to capture in the form of a photograph/screenshot, proof of the content or profile that is the source of harassment prior to submitting your report.

5.3.2 Instagram

Being another platform under the Meta company brand, Instagram uses the same reporting tool as Facebook. Even though the algorithm is designed to remove the offending content and fake profiles, bots tend to miss it. Hence users can manually block profiles and content. Instagram takes it up a notch by allowing its users to block profiles and any future profiles that a person may create or may have already created.



There are multiple ways to report something or someone on the Instagram app for Android and iPhone:

Report a post through feed

1. Tap ••• (iPhone) or ⋮ (Android) above the post.
2. Tap **Report**.
3. Follow the on-screen instructions.

Report someone through their profile

1. Tap their username from their feed, story post or from your chat with them. You can also tap 🔍 and search their username to go to their profile.
2. Tap ••• (iPhone) or ⋮ (Android) in the top right of the profile.
3. Tap **Report**.
4. Follow the on-screen instructions.

Instagram has a unique complaints mechanism. Under the Instagram Help Centre, instructions are provided on how to report the content or profile that causes violence. In case you don't have an Instagram account to report directly through the platform, Instagram offers a procedure under the Help Centre where you can submit proof of the content that is resulting in TFSGBV. As mentioned previously, you can also block a user who may create future profiles as well.

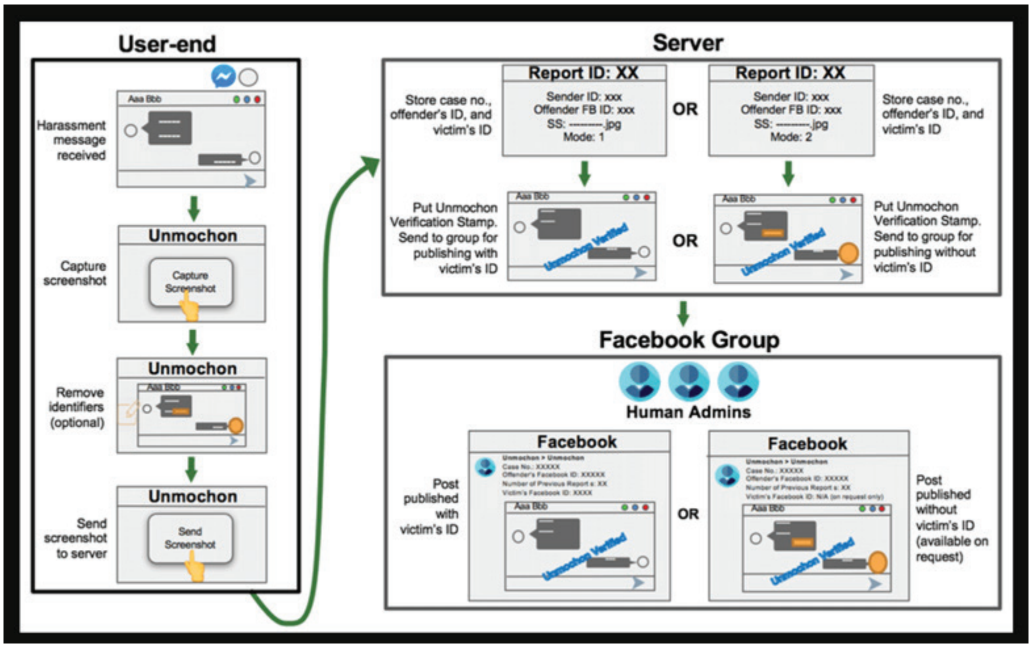
5.3.3 YouTube

YouTube is a video-based content platform owned by Google. Under its harassment and cyberbullying policy, YouTube does not tolerate "content that targets individuals with prolonged or malicious insults based on intrinsic attributes, including their protected group status (age, ethnicity, gender identity and expression, sexual orientation, etc.) or physical traits."

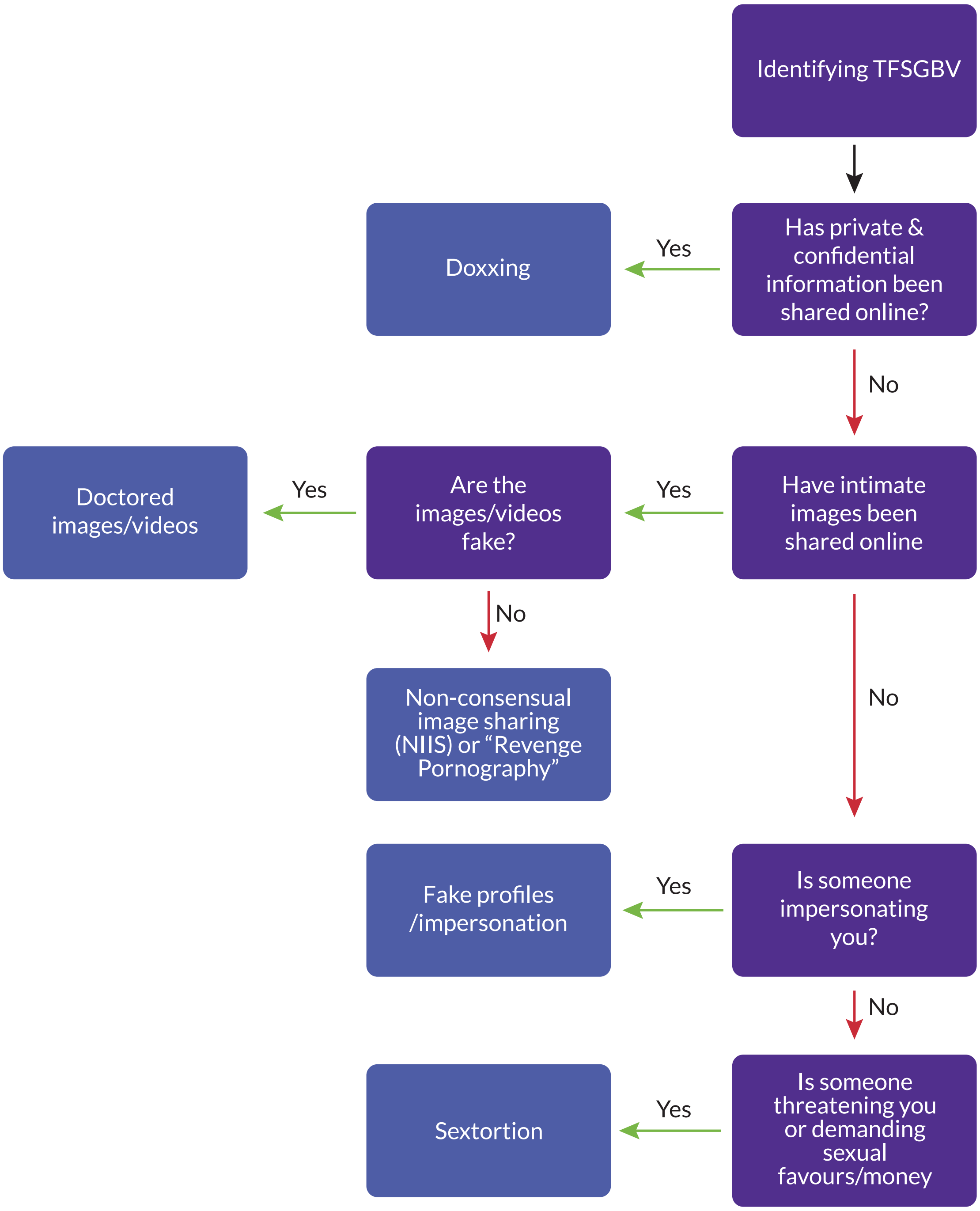
6 TFSGBV Protection Mechanisms

6.1 Unmochon (Bangladesh)

Women in the Global South often seek justice for their online harassment by unveiling the harassers and making screenshots of the harassing texts and visual content public. Thereafter, it is referred to the relevant authorities. Nevertheless, such evidence is often challenged for its authenticity. 'Unmochon' has been designed building on the 'shame-based model' of gender justice. It is a tool that captures authentic evidence and shares it with the victims' intended group.


User-end
Harassment message received
Aaa Bbb
Unmochon
Capture screenshot
Capture Screenshot
Unmochon
Remove identifiers (optional)
Unmochon
Send screenshot to server
Send Screenshot
Server
Report ID: XX
Sender ID: xxx
Offender FB ID: xxx
SS: --------.jpg
Mode: 1
OR
Report ID: XX
Sender ID: xxx
Offender FB ID: xxx
SS: --------.jpg
Mode: 2
Store case no., offender's ID, and victim's ID
Store case no., offender's ID, and victim's ID
Put Unmochon Verification Stamp. Send to group for publishing with victim's ID
OR
Put Unmochon Verification Stamp. Send to group for publishing without victim's ID
Unmochon Verified
Facebook Group
Human Admins
Facebook
Facebook
Post published with victim's ID
OR
Post published without victim's ID (available on request)

7 How to identify different types of TFSGBV


Identifying TFSGBV
Has private & confidential information been shared online?
Yes
Doxxing
No
Have intimate images been shared online
Yes
Are the images/videos fake?
Yes
Doctored images/videos
No
Non-consensual image sharing (NIIS) or "Revenge Pornography"
No
Is someone impersonating you?
Yes
Fake profiles /impersonation
No
Is someone threatening you or demanding sexual favours/money
Yes
Sextortion

This flowchart helps navigate through the different types of TFSGBV one might encounter. This simplified method helps the user eliminate certain types and helps them understand the nuances behind why there needs to be different classifications of TFSGBV.

7.1 Scenario-based identification of TFSGBV

7.1.1 Non-consensual intimate image (NCII) sharing

Scenario: A 15-year-old girl consensually sends intimate images of herself to a 16-year-old boy she is in a sexual relationship with. The relationship eventually disintegrates. 3 months later, she is notified that her intimate images are being shared on some local WhatsApp groups. When she confronts her former partner he says that someone must have hacked his device and obtained the images.

Key identifiers :

- Though the girl consensually sent the photos to the boy the same images being publicly circulated are non-consensual.
- While the hacking of his phone may or may not be true, this falls under the NCII sharing category.
- A common occurrence when a phone is given to repair, is that a person with malicious intent might run a recovery program such as Undelete to recover deleted photos and videos from the device.
- Another scenario occurs when a phone is compromised and all the content backed up on the cloud (iCloud, Google Drive) might come into the hands of a third party.
- The best way to avoid this happening is to refrain from backing up with iCloud or Google Drive storage and also to use software such as Undelete to delete intimate images or videos from a device permanently.

7.1.2 Doctored images

Scenario: A woman receives a Facebook message from a random Facebook account complimenting her photographs. The account asks if it is alright if they do some artistic edits to some of her photos, insisting that they are an art director. She consents, not thinking much of it. A few days later, another account messages her and threatens to release intimate images of her. This second account sends across digitally altered photos of herself, saying that they are going to publish these on a pornography site and send the link to her family and friends.

Key identifiers :

- The photos have been manipulated using software and in such a case, by using specific software one could identify if they were doctored.

- There are web-based photo forensic applications that could be used to identify manipulated images.
- A victim can take platform-specific action in this case and file a report regarding the doctored image.

7.1.3 Doxxing

Scenario: S and V separate after a 5-year romantic relationship, after which S begins a relationship with someone of the same sex. V, who is angered by S's unwillingness to rekindle their romance, opens a fake social media account. V adds several hundreds of people, including his former partner's family, employers, and friends. Through this account, V reveals that S is bisexual, and posts details such as an address, telephone numbers, and images of S with their same-sex partner that is only visible on S's small, private social media account. Following this S and the new partner are harassed by family and friends, and strangers who are now making inappropriate sexual advances due to their sexuality.

Key identifiers :

- The release of any personally identifiable information without consent such as the address, phone number, or National Identity Card number.

7.1.4 Sextortion

Scenario: A young woman begins a romantic relationship with a person she met online, who claims to be a young man. The online relationship develops, and one day while on a video call the man asks her to remove some of her clothing. Although she refuses at first, she eventually relents. The next day the man sends her screenshots of her topless on a video call and threatens to send the photos to her parents if she ever breaks up with him. It is also revealed that the man is in fact middle-aged and married. He demands more sexual favours from her in exchange for not releasing her images.

Key identifiers:

- Threatening to distribute private and sensitive material if one does not provide images of a sexual nature, sexual favours, or money.

7.1.5 Fake profiles & impersonation

Scenario: A woman is alerted by her friends to two fake profiles of her. They are made using her photos, and one is under her name with some personal details. She gets multiple people to report them, and the accounts are eventually taken down by the platform. A week later, another profile appears. Before she can report it, the account blocks her. The next day, another new profile is created, this time spreading defamatory comments about her character and reputation. Over the next few months over 20 such accounts are created. Despite reporting and removal, new profiles emerge, always blocking her.

Key identifiers:

- Someone other than the authentic person in the photos is creating profiles on Social Media platforms with a malicious intent.

8 The Sri Lankan Legal System's Response to TFSGBV

8.1 Laws pertaining to TFSGBV

In Sri Lanka there are no laws specifically applicable to TFSGBV offences. The lack of specific laws relating to TFSGBV means that law enforcement authorities must rely on general penal offences to address TFSGBV. These general penal offences do not consider the modes through which TFSGBV is carried out and the impacts of gender and intersectionality on TFSGBV, which defines TFSGBV. As a result of which most law enforcement authorities and other institutions in the criminal justice system are not fully aware of the gendered elements of TFSGBV and the impacts of intersectionality. Consequently, these institutions fail to appreciate the immensely traumatic, sensitive and high risk (including risk to the victim's safety) nature of the offence in relation to the victim-survivors, which is reflected in their responses to victim-survivors. Overall, these issues pose obstacles for victim-survivors when attempting to access legal remedies and protection from perpetrators of TFSGBV.

In the absence of specific laws addressing TFSGBV, the criminal justice system has adopted some laws from the general body of criminal laws to tackle acts of TFSGBV. The laws so applied are, broadly, as follows:

1) Section 285 of the Penal Code – Section 286A : Publication and distribution of obscene materials
2) Section 345 of the Penal Code : Sexual Harassment
3) Section 372 of the Penal Code : Extortion
4) Section 399 of the Penal Code : Cheating by impersonation
5) Section 483 of the Penal Code : Criminal Intimidation
6) Obscene Publications Ordinance No: 4 of 1927 (as Amended)
7) Online Safety Act No.9 0f 2024

Section 285 of the Penal Code (as Amended)

This particular section deals with a wide variety of actions which are carried out in order to release obscene publications to the public. It prohibits the sale, distribution, importation, printing for the purpose of selling or hire any obscene book, pamphlet, paper, drawing, painting, photograph, representation or figure. The section also prohibits knowingly allowing the public to view such obscene publications by displaying it and attempting to sell them. The penal sanction for this offence is imprisonment of either description for a term which may extend to three months, or a fine, or both fine and imprisonment.

This section can therefore be applied to instances of Image Based Sexual Abuse (IBSA). However, a key ingredient that needs to be present in order to apply Section 285 is that the photo or document which is being made available to the public is of an obscene nature. As such, this section would not, for example, apply to a situation where the face or clothed full image of the victim is used in a meme (unless, the content of the meme in words is obscene).

Section 286 & Section 286A of the Penal Code (as Amended)

The context in which the offence is related to Section 285: Section 286 prohibits a person from having in possession an “obscene publication” (as identified in Section 285) for the purpose of selling it or distributing it or making it available to the public. The key ingredient here, apart from the publication being obscene, is that the offender should have it in his possession with the intention to sell, distribute or make it available to the public.

Section 286A deals with obscene publications of children. It prohibits taking photos, attempting to take photos and distribution of obscene material related to children.

Section 345 of the Penal Code

Section 345 of the Penal Code prohibits and criminalizes sexual harassment as follows:

1) Sexually harassing a person by using criminal force or assaulting
2) Causing sexual annoyance or harassment by the use of words or deeds

The description to the offence categorically states that an act causing sexual harassment or annoyance can be any act that does not amount to rape, as identified in Section 333 of the Penal Code. This section is very versatile and can be adopted to address a range of TFSGBV. For example, threatening the victim-survivor over social media and communication platforms, and memes that are intended to vilify the victim-survivor and destroy their reputation are amongst some offences that can benefit from Section 345. In July 2024, a draft amendment Bill was gazetted to further strengthen Section 345 by explicitly including harassment "by means of any communication" (e.g., electronic or internet-based harassment such as sexually explicit messages, images, audio/video) and clarifies what is meant by "use of words or actions" which could cause sexual annoyance or harassment.[24]

Section 372 of the Penal Code

This section deals with "extortion." It criminalizes the act of obtaining valuable items or documents that can be converted into valuable security under threat of harm to the victim-survivor or another person. This section has limited scope in its application. However, as discussed earlier, persons do not only commit sextortion, they also use compromising images or videos for financial gain, in which case this section can be used.

Section 399 of the Penal Code

This section criminalizes "cheating by impersonation", where a person is cheated by another person who knowingly pretends to be someone else, or knowingly substitutes one person with another, or represents himself as someone else. This section can be used for offences such as doxing or fake profiles depending on the context and facts.

Section 483 of the Penal Code

Section 483 deals with criminal intimidation. It criminalizes any activity where a person is threatened and frightened with harm to him/herself or to a relative or friend, so as to coerce the victim-survivor into yielding to the wishes of the perpetrator.

[24] Groundviews.org, 'Criminalizing Sexual Harassment: Are We Doing Enough?' (2024)<https://groundviews.org/2024/08/20/criminalizing-sexual-harassment-are-we-doing-enough/ >accessed 01 September 2025.

Obscene Publications Ordinance No. 4 of 1927

Section 2(2) describes the offences set out in the act. Broadly, it criminalizes keeping obscene publications for the purpose of sale or distribution, as discussed in the Ordinance itself.

Online Safety Act No.9 of 2024

One of the objectives of this Act (Section 3(c)) is “to introduce measures to detect, prevent and safeguard against the misuses of online accounts and bots to commit offences under this Act”.

Though the provisions of the Act do not expressly include TFSGBV, some provisions that can be interpreted as acts of TFSGBV include Section 17 (online cheating), Section 18 (online cheating by personation), and Section 20 (communicating statements to cause harassment).

8.2 Institutions conducting investigations into TFSGBV and GOHS and the tools available for inter- jurisdictional investigations

The key institution in the criminal justice system that handles complaints of TFSGBV and GOHS is the Sri Lanka Police, as that is the institution with law enforcement and investigating powers.

8.2.1 What is the CCID?

The main unit handling cyber related crimes of the Sri Lanka police is the Computer Crimes Investigation Division (CCID), established under the Criminal Investigation Department (CID). However, this unit is employed to investigate complicated cyber related violence especially where the perpetrator/s is/are unknown or hidden. The CCID manages the whitelisted email address (which was initially managed by the SLCERT), which gives them direct contact with Facebook. Cases which need blocking or removal of content should now be referred to the CCID, often along with relevant web-links. To facilitate investigations under the signature of the Deputy Inspector General (DIG) of the CID, the following requests and orders can be made without court orders:

a) Requests to mobile service providers for information related to the identification of specified individuals.

b) Requests to the Department for Registration of Persons for passport & national identification card information of specified individuals.

c) Requests to issue orders to the Department of Immigration and Emigration prohibiting the overseas travel of specified individuals.

8.2.2 Can local Police Stations entertain complaints of CSGBV and GOHS?

Yes. All local Police Stations must entertain complaints of TFSGBV or GOHS as they are now capacitated and equipped to handle TFSGBV and GOHS, especially where the phone number, IP Address or the perpetrator is known. The complaint with regard to these offences should be recorded as a normal complaint by the police, and the normal course of action which is followed in an investigation will be taken. However during the course of the investigation, in the event that the local Police Station reaches a point beyond which they are not able to proceed, for example due to advanced technology used by the perpetrator, they may refer the investigation to the CCID.

8.2.3 Does the Children and Women's Desk in the Police Station have a role to play?

Yes. TFSGBVand GOHS when directed at women and girls can be entertained by the Children and Women's Desk as these constitute violations against women. It is noted that any Children and Women's Desk is now able to handle complaints of TFSGBV and GOHS where the perpetrator has been identified. These units are now capacitated and equipped to obtain court orders in relation to investigations of TFSGBV and GOHS. The Police Children and Women's Bureau, headquartered in Colombo, has the capacity and capabilities for handling advanced and complicated TFSGBV and GOHS offences as they have now developed their own specialized cyber-crime unit. The Bureau is also able to obtain court orders and direct it to Facebook, Instagram and other similar social media sites requesting to disclose information to assist the investigations of the Bureau. The Children and Women's Bureau too has a whitelisted email with Facebook through which they communicate complaints and take further action regarding sites and profiles carrying out TFSGBV and GOHS.

8.2.4 How do we obtain international cooperation for investigations?

In terms of conducting investigations, it must be noted that META platforms in the USA are not forthcoming with information due to their strict privacy and data protection laws. Moreover, these social media platform operating companies are not bound by law to release information about individuals unless the content is categorized as terrorism or child pornography. Therefore, the process these institutions work through is the Mutual Legal Assistance (MLA) scheme. However, this is laborious and time consuming, since it requires the coordination of four key State institutions, which are the Ministry of Justice, Ministry of Foreign Affairs, CCID and the Attorney General's Department. With regard to GOHS there is an additional obstacle. As most social media platforms are organizations based on profits they do not wish to interfere with the user's privacy and freedoms, therefore, clear information is required to show that certain content may generate criminal offences.

Nevertheless, since 2006, consequent to the Budapest Convention on Cyber Crime being ratified by Sri Lanka, there is a mechanism through which information may be obtained regarding TFSGBV and GOHS offenders and offending channels. Through the enforcement mechanism set out in this Convention, the law enforcement authorities of the countries which are signatories to this convention have established a 24/7 active focal point via which they exchange and obtain information to assist the law enforcement investigations. In Sri Lanka too there is such a 24/7 contact point managed by the CCID through which the CCID can request for information when international jurisdictions are involved and vice versa.

The CCID, through this platform, can also request to freeze bank accounts of suspected perpetrators, to facilitate investigations as well as to receive information about specified bank accounts including transactions made from the bank account.

However, reports obtained through this channel will have no evidentiary value in court proceedings and may only be used for investigational purposes. An MLA will be required for information that can be produced in court proceedings.

8.2.5 Are there other State institutions that can investigate and take action with regard to TFSGBV and GOHS?

Yes. The NCPA also has a role in addressing TFSGBV and GOHS incidents related to children. The NCPA can entertain complaints either in person or through the 1929 Helpline. The NCPA also has their own police investigation unit. In addition, the Chairman of the NCPA has the authority to request from the relevant telecommunications organizations, identification details to obtain phone numbers/IP addresses as well as the locations of TFSGBV and GOHS offenders for purposes of investigations. This process is quicker and efficient in comparison to the process local Police Stations must follow to obtain court orders to access such information. The NCPA set up the Internet Watch Foundation (IWF) Sri Lanka Reporting Portal in 2024 which encourages individuals to report instances of online child sexual abuse through an anonymous and straightforward process. The portal emphasizes the importance of reporting, stating that such actions can help rescue victims from further harm. Users can report quickly, and while anonymity is maintained, providing an email allows for follow-up on the report's outcome.

8.3 Guidelines on receiving victims of TFSGBV as first responders & the role of the Police

It is crucial that the institutions and stakeholders of the criminal justice system are sensitive to the various issues victim-survivors are compelled to face. This is especially so where they are the first responders, such as the police. The victim-survivors are not only faced with a criminal offence having been committed on them but a series of interconnected issues such as mental health, physical safety and concerns regarding re-socialization. The Assistance to and Protection of Victims of Crime and Witnesses Act No. 4 of 2015 in Part II (Section 4) provides a checklist for the police to adhere to when faced with a victim of crime and/or witnesses. The same list is equally applicable where police deal with victim-survivors of TFSGBV.

8.3.1 Equal Treatment & Respect for the Dignity of the Person

Section 3(a) of the Assistance to and Protection of Victims of Crime and Witnesses Act No. 4 of 2015 specifically states that it is the right of a victim "to be treated with equality, fairness and with respect to the dignity and privacy of such victim." The victim-survivors must, at all times, be treated with respect and dignity. In the circumstances they should be treated in such a manner that they feel safe, accepted and comfortable, and that they repose their trust in the legal system. To that end, appreciating the sensitive nature of a complaint it is advisable to take down the complaint within a private space, away from the police officers of the station. If the complainant is a woman, it is essential to direct her to the Children and Women's Desk in the Police Station and for a woman police officer to take down her statement.

All Police Stations have the powers to take down a complaint of TFSGBV Every Police Station has jurisdictional power to entertain a complaint of TFSGBV and to investigate the same. Therefore, it is important that complainants are not turned away unreasonably. Furthermore, under Article 12 of the Constitution, all persons have an equal right to equal protection of the law, which requires that their complaint is entertained and investigated. However, where the police require further technical assistance, the matter may be referred to the CID or such specialized agency. It takes a lot of courage for a victim of a TFSGBV crime, especially of image based sexual assault/ NCII sharing, to approach the Police Station and relate their story. Therefore, it is crucial that when a victim-survivor arrives at the Police Station they are not turned away. Turning the victim-survivor away would result in them having to return again or go to a different Police Station to tell the story, which can be traumatic as well as a financial challenge.

8.3.2 Ensure the best interests of Child victims

Section 3(b) of the Assistance to and Protection of Victims of Crime and Witnesses Act No. 4 of 2015 stipulates that: "where the victim is a child, to be treated in a manner which ensures the best interest of the child." In this regard it is important to ensure that on the one hand, the child is provided with a setting in which he/she will feel safe and comfortable to talk about the incident, and on the other hand, the first responder (most often the police) must immediately take steps to ensure the protection of the child. Therefore, it is best to inform the probation officer and the child protection officer at the Divisional/District Secretariat.

In addition, where the child is a female under 18 years, a woman police officer in plain clothing must take down the complaint and where the child is a boy under 18 years, a male officer in plain clothing must take down the complaint. Providing a quiet, comfortable and private space would encourage the victims to relate their story and enable the recording of a detailed statement.

8.3.3 Be unbiased: Do not judge the victim and their actions that led them to be subject to TFSGBV

This is an essential principle that all criminal justice stakeholders should adopt in relation to TFSGBV crimes. Given the context of TFSGBV offences, it is very easy to judge the victim-survivor for their "behaviour" and interactions with the perpetrator, who is most often an ex-partner and where such incidents have initially arisen out of instances of intimacy by mutual consent. The victim-survivors themselves struggle to come forward to the Police Station for reasons ranging from shame and embarrassment, to depression and fear of the perpetrator. If the police convey an attitude of explicit bias or disbelief towards the victim-survivor, it will be apparent to the victim-survivor, who will then withdraw from seeking justice due to shame and a lack of confidence in the system. It is therefore important not to make any comments on their actions, but instead to listen to their story and conduct the investigations impartially.

8.3.4 Be empathetic

This simple guideline is crucial. Most victim-survivors are fraught with anxiety, experience a sense of loss and are depressed at times. Some are also steeped in fear and shame. Struggling with so many emotions and mental agony, the victim-survivors require either counselling or psychiatric help. It is crucial that the police are intuitive and perceptive of these needs and are able to identify a victim-survivor who poses a risk (potential risk of self–harm and harm to others). The first responders must be able to identify whether the victim would need counselling or psychiatric assistance and if deemed to be necessary, they must refer the victim either to the counselling officer at the District/Divisional Secretariat, or to the Counselling Unit or psychiatry ward at the nearest government hospital.

In addition, the Assistance to and Protection of Victims of Crime and Witnesses Act No. 4 of 2015 at Section 3(e) provides that, a victim of crime has a right to "be medically treated for any mental or physical injury, harm, impairment or disability suffered as a victim of crime."

It is also important to refrain from rushing the victim-survivor when he or she is giving the statement or from interrupting the person to ask questions. Clarifications can be made after the statement has been given. Furthermore, it is important to allow the victim to provide the statement in the language of their choice (Sinhala or Tamil).

8.3.5 Be impartial and prompt with investigation: provisions of the Code of Criminal Procedure apply

The sensitivity of the offence requires prompt investigation. Evidence must be carefully collected and numbered where necessary. More importantly with regard to TFSGBV, screenshots of fake profiles, messages sent via social media platforms and telecommunication platforms, relevant photos, memes etc. should be taken, as the chances are that the perpetrator would erase the evidence, especially once he is informed of the complaint. Part V of the Code of Criminal Procedure Act relating to the investigation of offences also applies to the investigation of TFSGBV as well as the provisions in the Evidence Ordinance. The Assistance to and Protection of Victims of Crime and Witnesses Act No. 4 of 2015 at Section 3(g) provides that a victim of crime shall have a right to "present either orally or in writing a complaint pertaining to the commission of an offence and to have such statement recorded by any officer, in any Police Station or other unit or division of the police department, and to have such complaint impartially and comprehensively investigated by the relevant investigating authority."

The victim-survivors should also be informed of the provisions in the Assistance to and Protection of Victims of Crime and Witnesses Act No. 4 of 2015 through which a victim-survivor under threat can seek protection.

9 Conclusion

Even though key organizations, including law enforcement authorities, are increasingly taking a more active approach towards TFSGBV complaints, it is nevertheless a growing challenge to tackle the rising number of complaints with limited resource allocations

This factor combined with the reluctance of victims to seek legal redress due to reasons such as victim shaming, as well perceptions prevailing around issues of sexual crimes in a patriarchal society, has contributed to make TFSGBV a systemic problem. Furthermore, most cybercrimes occur on different online platforms that operate in different territorial jurisdictions and this poses a major obstacle to taking platform-specific action, which would be the most effective response.

The lacuna created by the lack of Sri Lankan laws specifically criminalizing TFSGBV causes perpetrators of TFSGBV to go unpunished. This situation also lends to delaying the criminal justice process thereby delaying justice. In addition, the inability of some law enforcement officers and a lack of training in some others, have resulted in the law enforcement officials failing to use the existing penal laws to bring perpetrators of TFSGBV before courts.

Key ingredients towards successfully addressing and arresting TFSGBV, with the available resources and tools, may be achieved through building an understanding by the user on how to safely use digital platforms and an appreciation of the existing penal laws by the law enforcement authorities in relation to TFSGBV crimes.

However, that is a requirement for the short term. We must not lose sight of the necessity for long lasting and current legal reforms to directly address TFSGBV, the empowerment of enforcement officials, the sensitization of enforcement officials through trainings, and, if possible, further resource allocation coupled with awareness programs and discussions about TFSGBV targeting users from a young age in order to stem the spread of TFSGBV in Sri Lanka.

10 List of References

'Gender Based Interpersonal Cyber Crime' (UNODC, February 2020) <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/gender-based-interpersonal-cybercrime.html> accessed 05 March 2023.

Chamara S, 'Unsafe outside, unsafe online' (The Morning, 13 March 2022) <https://www.themorning.lk/unsafe-outside-unsafe-online > accessed 05 March 2023.

Council of Europe, Explanatory Report to the Council of Europe Convention on Preventing and Combatting Violence Against Women and Domestic Violence (Council of Europe Treaty Series No: 210); UNGA, 'Discrimination and violence against individuals based on their sexual orientation and gender identity: Report of the Office of the United Nations High Commissioner for Human Rights' UN Doc A/HRC/29/23 (04 May 2015).

De Mel N, Peiris P and Gomez S, 'Broadening gender: Why masculinities matter?: Attitudes, practices and gender-based violence in four districts in Sri Lanka' (Care International Sri Lanka, 2013).

Fonseka B, 'The Growing Dangers of Online Sexual Exploitation of Children' (Groundviews, 20 November 2021) <https://groundviews.org/2021/11/20/the-growing-dangers-of-online-sexual-abuse-of-children/> accessed 05 March 2023.

Gender Based Interpersonal Cyber Crime' (UNODC, February 2020) <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/gender-based-interpersonal-cybercrime.html > accessed 05 March 2023.

Gunasekera D, 'Online gender-based violence: The new normal of sexual harassment' (The Morning, 28 February 2021) <https://www.themorning.lk/online-gender-based-violence-the-new-normal-of-sexual-harassment/ > accessed 05 March 2023

Hapuarachchi P, 'Special Police Unit to crack-down on Child Pornography' (Newsfirst, 29 July 2021) <https://www.newsfirst.lk/2021/07/29/special-police-unit-to-crack-down-on-child-pornography/> accessed 05 March 2023.

Kemp S, 'Digital 2022: Sri Lanka' (Datareportal, 15 February 2022) <https://datareportal.com/reports/digital-2022-sri-lanka > accessed 05 March 2023.

Krug EG et al. (eds), World report on violence and health (World Health Organization, 2002).

Population Matters, 'Sexual Harassment on Public Buses and Trains in Sri Lanka' (UNFPA Policy Brief, March 2017)< https://srilanka.unfpa.org/sites/default/files/pub-pdf/ FINAL%20POLICY%20BRIEF%20-%20ENGLISH_0.pdf > accessed 05 March 2023.

Save the Children et al., Online Violence Against Children in Sri Lanka(March 2022) <https://srilanka.savethechildren.net/sites/srilanka. savethechildren.net/files/Online%20Violence%20Against%20Children%20in%20Sri%20Lanka.pdf> accessed 05 March 2023

Schoenebeck, S et al. (2021). Drawing from justice theories to support targets of online harassment. New Media & Society, 23(5), 1278–1300. https://doi.org/10.1177/1461444820913122

Sri Lanka Medical Association (SLMA), Review of Research Evidence on Gender-Based Violence in Sri Lanka (2011); University Grants Commission (UGC), Center for Gender Equity and Equality & UNICEF, Prevalence of Ragging and Sexual and Gender-Based Violence in Sri Lankan State Universities (2022).

UN Committee on the Elimination of Discrimination Against Women (CEDAW), CEDAW General Recommendation No. 19: Violence against women, 1992 <https://www.refworld.org/docid/52d920c54.html > accessed 27 January 2023.

UN Human Rights Office of the High Commissioner, Born Free and Equal: Sexual Orientation, Gender Identity and Sex Characteristics in International Human Rights Law (2nd edn, United Nations 2019)

Ward J and Lafrenière J, Guidelines for Integrating Gender-Based Violence Interventions in Humanitarian Action: Reducing Risk, Promoting Resilience and Aiding Recovery. (: Inter-Agency Standing Committee 2015)

Centre for Equality and Justice

37/2, Elibank Road, Colombo 05, Sri Lanka.

Tel/Fax: +94 11 2055404

www.cejsrilanka.org

srilanka.cej@gmail.com

/CEJ.SL | /cej_srilanka | /CEJ_SriLanka | /@CEJSriLanka

ISBN 978-624-5847-26-6

9 786245847266