CitW

Cyber Sexual and Gender-Based Violence in Sri Lanka

A Legal Gap Analysis

Naushalya Rajapaksha for Search for Common Ground.

December 2023

British High Commission Colombo

Search for Common Ground
Trust, Collaboration, Breakthroughs

Centre for Equality and Justice

#GENERATION தரப்பு தலைமுறை

Foreword

I am deeply honored to write a foreword for this vital report on Cyber Sexual and Gender-Based Violence (CSGBV) prepared by Ms. Naushalya Rajapakse, Attorney-at-Law, and published by Search for Common Ground Sri Lanka. As a practitioner and former President of the Bar Association of Sri Lanka (BASL), I understand the profound impact that the legal system can have on shaping our society and ensuring the rights and dignity of all individuals.

This report arrives at a pivotal moment when the legal framework concerning gender-based violence, and in fact the entire legal system stands under scrutiny. In an era marked by the remarkable influence of technology and digital communication, the issue of CSGBV has emerged as a complex and urgent challenge that transcends boundaries and necessitates a nuanced legal response.

The research carried out in this report is a testament to the dedication and expertise of its author, Naushalya Rajapakse, and the unwavering commitment of Search for Common Ground Sri Lanka. It delves into the heart of the matter by conducting a comprehensive legal gap analysis within the context of Sri Lanka. The primary goal of this study is to assess the adequacy of the current legal framework in addressing CSGBV, identifying areas where legal provisions fall short, potentially leaving victims and survivors vulnerable.

The report explores the various forms of CSGBV, providing a clear and nuanced understanding of the challenges posed by this digital phenomenon. From unauthorized and non-consensual acts using technology to the impersonation of identity, cyber sexual harassment, and the exploitation of women and children using technology, the report meticulously examines these multifaceted issues and maps them to relevant legal provisions in Sri Lanka.

Despite the presence of legal provisions such as the Penal Code Ordinance, Obscene Publications Ordinance, Children and Young Persons (Harmful Publications) Act, Convention on Preventing and Combating Trafficking in Women and Children for Prostitution, Computer Crimes Act, and the recently enacted Personal Data Protection Act, the report highlights persistent challenges, including ambiguities in interpretation and a lack of uniformity. Very often it is not the absence of laws, but rather the manner of their application that leaves a gap between what is expected of a law and its actual application.

To bridge these gaps effectively, the report offers a multifaceted approach, including the reformulation and amendment of laws, regular reviews of existing legal and policy frameworks, extensive public awareness campaigns, and continuous sensitization and training for legal professionals and authorities. By implementing these recommendations, Sri Lanka can strengthen its legal foundation, enhance support systems, and ensure that the rights of CSGBV victims and survivors are robustly protected under the law.

In an ever-evolving digital age, CSGBV has become a pervasive and alarming global issue. The statistics are disheartening, with a staggering number of women experiencing online violence or harassment. Sri Lanka, like many other nations, faces its own set of challenges in addressing these issues, as the data underscores.

This report serves as a critical tool for assessing the adequacy of existing legal provisions and policies in addressing the multifaceted nature of CSGBV. By identifying gaps and inconsistencies in our legal framework, we can chart a path toward legal reforms that better protect the rights and dignity of victims and survivors.

A comprehensive legal response is not only crucial in upholding principles of gender equality, human rights, and social justice, but it is also imperative in safeguarding individuals from the perils of CSGBV in the digital sphere.

I commend Ms. Rajapakse and the Search for Common Ground Sri Lanka for their invaluable work, and I urge all stakeholders to embrace the findings presented in this report. Together, we can create a safer and more just digital world for all.

Saliya Pieris P.C.

List of Acronyms

CSGBV	Cyber Sexual and Gender Based Violence
SCG	Search for Common Ground
SLCERT	Sri Lanka Computer Emergency Readiness Team
LGBTQ+	Lesbian, Gay, Bisexual, Transgender, Queer or Questioning, Intersex, Asexual, and more.
GIF	Graphics Interchange Formats
PCPD	Privacy Commissioner for Personal Data
ICT	Information and Communications Technology
UNSG	United Nations Secretary General
HRC	Human Rights Council

Executive Summary

This report undertakes a thorough examination of the legal landscape in Sri Lanka, specifically honing in on the critical issue of Cyber Sexual and Gender-Based Violence (CSGBV). The primary objective of this investigation is to evaluate the effectiveness of the current legal framework in addressing CSGBV and pinpoint areas where legal provisions may be inadequate, potentially leaving victims and survivors exposed to vulnerability.

Initiating the analysis, the report delves into various forms of CSGBV, identified through inclusive discussions involving multiple stakeholders and focus groups facilitated by Search for Common Ground. These discussions led to the identification of 14 distinct forms of CSGBV, encompassing manifestations such as the non-consensual distribution of explicit content, doxxing, impersonation, cyber stalking, and online child sexual exploitation.

To enhance clarity, these diverse forms of CSGBV were thoughtfully categorized into four subgroups: Unauthorized and Non-Consensual Acts Using Technology, Impersonation of Identity, Cyber Sexual Harassment, and Exploitation of Women and Children Using Technology.

Subsequent to this categorization, the report meticulously examines the legal framework in Sri Lanka, mapping each category of CSGBV to the relevant legal provisions. The existing legal framework in the country includes laws such as the Penal Code Ordinance, Obscene Publications Ordinance, Children and Young Persons (Harmful Publications) Act, Convention on Preventing and Combating Trafficking in Women and Children for Prostitution, Computer Crimes Act, and the recently enacted Personal Data Protection Act. Additionally, the analysis also takes a gander at the recently encompassed Online Safety Bill 2023.

Despite the existence of these legal provisions, the report underscores persistent challenges, including ambiguities in interpretation and a lack of uniformity. To effectively address these gaps, the report proposes a comprehensive approach, encompassing the reformulation and amendment of laws, regular reviews of existing legal and policy frameworks, extensive public awareness campaigns, and continuous sensitization and training for legal professionals and authorities.

Through the implementation of these recommendations, Sri Lanka has the opportunity to fortify its legal foundation, bolster support systems, and ultimately ensure robust protection of the rights of CSGBV victims and survivors under the law.

Introduction

In the dynamic landscape of our advancing digital era, the surge in Cyber Sexual and Gender-Based Violence (CSGBV) has emerged as a pervasive and concerning global challenge. The advent of the internet and digital communication platforms has presented both opportunities and challenges. While technology has propelled economic growth, education, and social connectivity, it has also given rise to new forms of gender-based violence that transcend geographical boundaries, making a nuanced legal response more crucial than ever.

This report conducts an in-depth examination of the legal terrain in Sri Lanka regarding CSGBV, recognizing the unique challenges posed by this digital phenomenon. It emphasizes the significance of such an analysis, rooted in the understanding that the law plays a pivotal role in shaping societal norms, protecting individuals' rights, and holding perpetrators accountable.

Global data underscores the urgency of addressing CSGBV. A report by the United Nations Broadband Commission reveals that a staggering 73% of women have experienced some form of online violence or harassment, indicating a troubling global trend. Additionally, the International Telecommunication Union (ITU) discloses that women in Asia and the Pacific region are 25% less likely than men to use the internet due to concerns related to online harassment, privacy violations, and digital threats.

In Sri Lanka, as in many nations, CSGBV has manifested itself through various forms, including non-consensual distribution of explicit content, doxxing, impersonation, cyber stalking, and online child sexual exploitation, among others. Local data (SL CERT, 2021) indicates that in 2019, 3566 incidents were reported. Incidents reported to Sri Lanka CERT surged to 16,376 in 2020 after the pandemic, marking an almost 460% increase in reported incidents compared to the previous year. These manifestations and incident rates have raised complex legal questions and challenges that require careful examination.

Navigating the complexities of the digital age necessitates safeguarding individuals from the perils of CSGBV. This report aims to contribute to the ongoing dialogue and actions required to ensure that Sri Lanka's legal framework remains robust and responsive, safeguarding the rights and dignity of all in the digital age. It serves as a critical tool for assessing the adequacy of existing legal provisions and policies in addressing the multifaceted nature of CSGBV. By identifying gaps and inconsistencies in the legal framework, we can chart a path toward legal reforms that better protect the rights and dignity of victims and survivors. Moreover, a comprehensive legal response is crucial for upholding principles of gender equality, human rights, and social justice in the digital sphere.

Methodology

The Analysis

The content of this desk review is based on information collected through a systematic review of the available documents relevant to the legal system in Sri Lanka in the light of the main form of Cyber Sexual and Gender Based Violence identified by the researcher. During the desk review the main forms of Cyber Sexual and Gender Based Violence are identified together with the applicable laws and the gaps in the legal system.

The applicable domestic legislation which has been analysed are as follows:

- **Penal Code Ordinance No. 11 of 1887 (as amended)**
- **Obscene Publications Ordinance No. 04 of 1927 (as amended)**
- **Children and Young Persons (Harmful Publications) Act No. 48 of 1956**
- **Convention on Preventing and Combating Trafficking in Women and Children for prostitution No. 30 of 2005**
- **Computer Crimes Act No. 24 of 2007**
- **Personal Data Protection Act No. 09 of 2022**

Further to the desk review of the gaps in the existing laws within the country, the researcher has also analysed some of the existing laws in the neighbouring South Asian Countries, to better understand the legislative measures they have taken to strengthen their preventive and response mechanisms towards various offences of CSGBV. Interpretive techniques were applied while conducting the secondary data analysis.

The Structure

During this exercise, the researcher has taken into account the existing laws in Sri Lanka related to Cyber and Sexual Gender Based Violence (CSGBV) and has compared the same with the key identified forms of CSGBV identified by Search For Common Ground subsequent to numerous multi stakeholder and focus group discussions.

The said key identified forms of CSGBV subsequent to such discussions are as follows:

1. **Non-consensual creation, dissemination, distribution or digital sharing of photographs, videos or audio clips of a sexual or intimate nature.**
2. **Unauthorized access, use, control, manipulation, sharing or publication of private information and personal data.**
3. **Doxxing.**
4. **Impersonation and Identity Theft.**
5. **Surveillance and Monitoring.**
6. **Cyber Stalking.**
7. **Cyber Harassment.**
8. **Cyber Bullying.**
9. **Online Gendered Hate Speech.**
10. **Sextortion**
11. **Technology Facilitated Physical Violence.**
12. **Exploitation and or Trafficking of Women and girls through the use of Technology.**
13. **Attacks on Women's groups, organizations or communities.**
14. **Online Child Sexual Exploitation.**

Yet, upon a more detailed examination of the identified key forms, it becomes apparent that certain forms exhibit overlap, and that some of the key forms result as consequences of others. To enhance clarity and comprehension of these forms, as well as the applicable laws corresponding to each, the aforementioned forms are reorganized into the following four subcategories:

Re-grouped key forms of CSGBV:

1. Non-consensual creation, dissemination, distribution or digital sharing of photographs, videos or audio clips of a sexual or intimate nature, unauthorized access, sharing or publication of private information and personal data, use, control, manipulation/ Doxxing.
2. Impersonation and Identity Theft
3. Cyber Harassment: Cyber Stalking / Surveillance and Monitoring / Cyber Bullying / Online Gendered Hate Speech
4. Sextortion, Exploitation and or Trafficking of Women and girls through the use of Technology / Online Child Sexual Exploitation

Consequential offences of the above-mentioned key forms of CSGBV:

1. Technology Facilitated Physical Violence
2. Attacks on Women's Groups, organizations, or communities.

The mentioned two categories are deemed consequential offenses because these offenses may not occur in a virtual environment but could be equated to in-person attacks involving physical violence or violence stemming from other means. Consequently, these two domains have not been scrutinized in this research, as the focus of the study was primarily confined to the examination of 'Cyber' Sexual and Gender-Based Violence, excluding instances of Sexual and Gender-Based Violence occurring beyond the cyber realm.

Overview of CSGBV Categories, Definitions, and Laws

Category 01 Unauthorized and Non-Consensual acts using technology.

Unauthorized and/or Non-Consensual access, creation, dissemination of private information and personal data sexual or non-sexual in nature for various intents and purposes or attempt to do.

Key forms of CSGBV identified under this category:

- Non-consensual creation, dissemination, distribution or digital sharing of photographs, videos, or audio clips of a sexual or intimate nature.
- Unauthorized access, use, control, manipulation, sharing or publication of private information and personal data.
- Doxxing - involving unauthorized extraction and publication of personal information as a form of intimidation or with the intent to locate that person in "the real world" to harass them.

Applicable laws in Sri Lanka relevant to this category:

- Obscene Publications Ordinance No. 04 of 1927 (as amended)
- Sections 285 and 286 of the Penal Code Ordinance No. 11 of 1887 (as amended)
- Sections 3,4,5,7 and 10 of the Computer Crimes Act No. 24 of 2007
- Personal Data Protection Act No. 09 of 2022

Category 02 Impersonation of Identity

Impersonation of another person's identity on an online platform for various intents and purposes.

Key forms of CSGBV identified under this category:

- **Impersonation and Identity Theft** - A malicious activity that consists of impersonating another person online and using their personal data in order to threaten or intimidate them. This can be done by creating fake profiles or accounts on social networks or usurping email accounts or telephone numbers, which can be used to contact friends, family, colleagues, or acquaintances of the victim for the purpose of establishing communications and accessing information about them.

Applicable laws in Sri Lanka relevant to this category:

- Section 399 of the Penal Code Ordinance No. 02 of 1883 (as amended)

Category 03 Cyber Sexual Harassment

An act of causing or attempt to cause harassment or annoyance to an individual/or a group of individuals/ institution etc. by action or by words for various intents and purposes not limited to humiliation, intimidation or to infliction of fear of violence, exclusion, or isolation within their respective society.

Key forms of CSGBV identified under this category:

- **Surveillance and Monitoring** - Constant monitoring and surveillance of a person's online and offline activities or location constitutes a form of violence. This can be done with spyware installed on the victim's cell phone to covertly monitor them or steal their information. It is also carried out using geolocation devices located in cars or handbags, toys, surveillance cameras, virtual assistants, or connected smart devices.
- **Cyber Stalking** - Intentional and repeated activity carried out using computers, cell phones, and other electronic devices, which may or may not constitute harmless acts separately, but which, taken together, amount to a pattern of threatening behaviors that undermine a person's sense of security and cause fear, distress or alarm.
- **Cyber Harassment** - Cyber harassment involves the use of ICTs to intentionally humiliate, annoy, attack, threaten, alarm, offend or insult a person. Cyber harassment can take numerous forms and be associated with other types of online violence. For example, it can include sending unwanted and intimidating messages via email, text, or social networks; inappropriate or offensive insinuations on social networks or in chat rooms; online verbal violence and threats of physical violence or death.
- **Cyber Bullying** - Cyberbullying involves the use of technologies by children to humiliate, annoy, alarm, insult or attack other children or to spread false information or rumours about the victim, as well as to threaten, isolate, exclude, or marginalize them.
- **Online Gendered Hate Speech** - It is the use of language that denigrates, insults, threatens, or attacks a person by reason of their gender identity or other characteristics, such as sexual orientation or gender expression.

Applicable laws in Sri Lanka relevant to this category:

- Section 345 of the Penal Code Ordinance No. 02 of 1883 (as amended)

Category 04 Exploitation of Women and Children using technology.

An act of causing threats or attempt to cause threats to share images/videos of a person sexual/intimate in nature obtained with/without their consent as the means of coercion for both monetary and non-monetary gains.

Key forms of CSGBV identified under this category:

- **Sextortion** - Sextortion consists of threatening to disseminate intimate images or videos of a person in order to obtain more material about sexually explicit acts, engage in sexual intercourse, or extort money.
- **Exploitation and or Trafficking of Women and girls through the use of Technology** - Technologies are used to target and capture women and girls for sexual abuse or trafficking, force them to accept trafficking and sexual abuse situations, exercise power and control over them, and prevent them from freeing themselves from the abuse, including by threatening to disclose private information.
- **Online Child Sexual Exploitation** - Online child sexual exploitation includes a wide range of behaviours and situations. Most commonly this includes grooming, live streaming, consuming child sexual abuse material, and coercing and blackmailing children for sexual purposes. This could include: An adult engaging a child in a chat about sexual acts.

Applicable laws in Sri Lanka relevant to this category:

- Sections 483 and 487 of the Penal Code Ordinance No. 02 of 1883 (as amended)
- Section 2 (2) (a) of the Obscene Publications Ordinance as amended
- Sections 286A, 286B, 286C, 360A, 360B, 360E, Penal Code Ordinance No. 02 of 1883 (as amended)
- Obscene Publications Ordinance Act No. 4 of 1927 (as amended)
- Children and Young Persons (Harmful Publications) Act No. 48 of 1956
- Convention on Preventing and Combating Trafficking in Women and Children for prostitution No. 30 of 2005

Category 01 Unauthorized and Non-Consensual acts using technology.

Unauthorized and/or Non-Consensual access, creation, dissemination of private information and personal data sexual or non-sexual in nature for various intents and purposes or attempt to do.

Obscene Publications Ordinance No. 04 of 1927 (As Amended by Act No. 22 of 1983 and 12 of 2005)

About the Applicable Domestic Laws	Scope and Purview of the Laws	Identified Gaps/Issues in the Laws
What the Act is about: Surprisingly, the Act is devoid of a preamble, or a description of what the Act intends to cover. It simply states that this Ordinance relates to Obscene Publications. **What offences are covered in the Act:** Under Section 2 (2) of the Act, the following offences are covered: **a.** To make, produce or have in possession for the purpose of trade, distribution, public exhibition, or for another purpose, an obscene writing, drawings, prints, paintings, printed matter, pictures, posters, emblems, photographs, cinematograph films, video cassettes or any other obscene object.	The Act goes to the extent of covering Obscene matter or things kept in one's possession for purposes of business. However, then a question arises as to whether the Act covers incidents where an offender keeps such Obscene matter or things for personal viewing and if the offender had shared it with individuals or groups to cause humiliation or harassment to the victim devoid of a commercial purpose. An issue of this nature can be addressed by the words *"for purposes stated or otherwise",* meaning that the Legislature did intend to cover instances or offences that are not expressly mentioned in the Ordinance, as stated in Section 2 (2) (a) of the Ordinance, and by the words *"or in any manner whatsoever to put them into circulation"* as stated in Section 2(2) (b) of the Ordinance.	The Act does not define what an *Obscene matter or thing is.* The word *'obscene'* according to many dictionaries could also mean *'indecent',* which is a subjective evaluation placed on the hands of the Learned Judge to decide whether the photographs or videos at hand is obscene or not. Therefore, an offender who has pictures or videos of a victim obtained without consent, which does not fall into the realm of *'obscene'* may go unpunished under this Act. The best example is that of the pictures of schoolgirls in school uniforms shared on various social media platforms, as an objective person may not find anything *'obscene'* or *'indecent'* about a picture of schoolgirls in school uniforms.

b. To import, convey or export or cause to be imported, conveyed, exported any of the said obscene matters or things, or in any manner whatsoever to put them into circulation.

c. To carry on or take part in a business, be it public or private to deal, distribute or exhibit such obscene matters or things publicly or to make a business lending them.

d. To advertise or make others know by any means, and providing assistance to circulate or traffic, or to advertise or to make known how to or from whom such obscene matters or things can be procured either directly or indirectly.

What will be the sentence if found guilty:

Under Section 2 of the Ordinance, depending on the offence committed, a person who is found guilty will be sentenced with a fine between Rs. 2500 - 5000 or imprisonment for a term not exceeding 06 months, or with both such fine and imprisonment.

Further, according to Section 2(2)(c) of the Ordinance, anyone who assists such circulation can also be found guilty.

This is so, as anyone who 'make' or *'produce', 'or have in possession'* any such *'obscene matters or things,'* or even assist in such making or producing such obscene matters or things, which could potentially mean a consciously taken series of nude picture/s or video/s of oneself kept with oneself or shared with her/his/their partner/s could also be potentially punishable according to Section 2 and 3 of the provisions of the Ordinance.

Although the situation and the development of technology was much different to now when compared with the technological landscape in 1927 (in which year the Ordinance was originally enacted) or in 1983 (when the Ordinance was first amended), the legislature could have amended considering the current context these ambiguous provisions in 2005 when the Act was amended for the second time.

This interpretation could also affect the members of the LGBTQ+ community adversely as such *material* made or produced could also be tantamount to proving the offence of committing an *Unnatural Offence*, under Section 365 or 365A of the Penal Code which criminalizes same sex relationships between consenting adults.

Other information to keep in mind: The above offences are Triable* by the Learned Magistrate's Court.		Section 4 of the Act clearly states that: Nothing in this Ordinance shall affect or prevent a prosecution under the Penal Code or any other written law; but a person shall not be punished more than once for the same offence. This simply means that an offender who commits the same offence to the same person even after a conviction will not be punished, as he cannot be punished more than once for the same offence. Further, since discretion lies with the Learned Magistrate to either impose a fine or a sentence, an offender found guilty could go home after paying a fine of maximum Rs. 5000.

Penal Code of Sri Lanka Ordinance No. 02 of 1883 (As amended)

What the Act is about: The Penal Code in Sri Lanka enacts the criminal and penal laws in Sri Lanka. Under the Penal Code, several sections of the Penal Code such as Sections 285 to 286A and 287 are dedicated to offences related to Obscene Materials.		

What offences are covered in the Act:

Under **Section 285** of the Act, the following offence is covered ; where you sell, distribute, import, or print for sale or hire, or wilfully exhibit to public view, obscene book, pamphlet, paper, drawing, painting, photograph, representation, or figure or any attempt to do so, or if you even offer to do any of the above-mentioned acts shall be punished with an imprisonment for a term which may extend to 03 months, or with fine, or with both.

This Offence is also bailable*, not compoundable* and is triable in Learned Magistrate's Court, and the Police may arrest without a warrant.

Under **Section 286** of the Act, the following offence is covered.

If anyone has in his possession any such obscene book or other thing as is mentioned in the last section (Section 285) for the purpose of sale, distribution or other public exhibition, shall on conviction be liable to an imprisonment which may extend to 03 months, or with fine or with both.

Under Section 285, an incident in which an Obscene book, pamphlet, paper, drawing, painting, photograph, representation, or figure which is found to be distributed, imported can be an offence. This section is flexible to cover instances in which *'obscene'* photographs deliberately exhibited for public viewing, can be punishable.

In today's context, although public viewing can also be construed to include the number of viewers, shares, likes or comments a post may harness even on a social media platform, instances where certain images have been shown or shared for viewing by merely passing down the phone, or having the image appeared in printed form on a public place can also be construed under *'viewing'.* Therefore, not only on online platforms, offences committed on offline platforms can also be covered under these provisions.

Sections 285 and 286 are limited to having in possession any obscene book, pamphlet, paper, drawing, painting, photograph, representation, or figure for the purpose of sale, distribution, or other public exhibition.

However, the sections make no express reference to Graphics Interchange Formats (GIFs), videos, live videos, or live streams, which may deem to expire at the end of the intended period.

Further, the Sections 285 and 286 do not expressly cover an incident in which an obscene video of a person is kept in possession, for purposes of personal viewing and gratification, obtained from the victim with or without their consent, which may not necessarily be *'exhibited publicly'* Further, since discretion lies with the Magistrate to either impose a fine or a sentence, an offender found guilty could go home after paying a fine as decided by the Judge.

This Offence is also bailable*, not compoundable* and is triable in Learned Magistrate's Court, and the Police may arrest without a warrant.

Computer Crimes Act No. 24 of 2007

What the Act is about:

According to the Computer Crimes Act, the Act identifies the types of crimes that can be committed under the Act, how the investigation into such allegation should go about and other relevant matters.

What offences are covered in the Act:

Under the Computer Crimes Act, several offences under Part I from Sections 3 to 14 are identified as the sort of offences that can be committed under the Act.

Sections 3, 4 and 5 of the Act deals with the following offences respectively:

- Securing unauthorised access to a computer an offence.
- Doing any act to secure unauthorised access in order to commit an offence
- Causing a computer to perform a function without lawful authority an offence

The Computer Crimes Act is rather an interesting piece of legislation, as the Computer Crimes Act is said to be a direct result of the Budapest Convention.

This is considered to be a historic achievement, because Sri Lanka became the first country in South Asia (and only the second Asian country, after Japan) to become a state party to this Convention.

In light of that legislative progression, the Computer Crimes Act identifies various offences that can be covered under the Act. One such offence being dealing with unlawfully obtained information from a computer.

The Computer Crimes Act, although not amended since 2007 can still hold space for most of the crimes that are committed in today's context. As the Act is not limited in its nature to obscene or intimate images or videos, any unlawfully obtained photograph or video, whether it is obscene in nature or *otherwise.*

This Act is therefore useful especially in circumstances if an image of a person, although lawfully obtained is used for purposes unintended. For an example, if an image of a social media influencer, which is published for the public to view is reposted, shared, or disseminated in platforms and for purposes unintended, then Section 7 may come handy although the picture in issue may or may not fall under the categories of an obscene or an intimate picture.

Therefore, under **Section 3** of the Act, anyone who secures unauthorized access to a computer or any information held in a computer, knowing or simply having reason to believe that he has no lawful authority to secure such access shall on conviction be liable to a fine not exceeding 100,000/- or to imprisonment of either description for a term which may extend to 05 years, or both such fine and imprisonment.

Further, although the Computer Crimes Act does explicitly mention the word 'Computer', one may come to the quick conclusion that the Computer Crimes Act is limited in its application to the offences that can be done on a computer, from a computer or to a computer or through a computer.

However, such restrictive interpretation is dispelled by Section 38 of the Interpretation Section of the Act, which goes on extend meaning of the word computer to an *"electronic or similar device having information processing capabilities".* Therefore, offences that can be committed via the use of mobile phones with similar *'information processing capabilities"* can also be covered under the Act.

Secondly, if a question arises as to whether photographs, videos, or audio clips etc. of sexual in nature or otherwise, falls under the category of *'Information',* the answer is Yes, it does. This is so, under Section 38 of the Act, *Information* is construed to includes data, text, images, sound, codes, computer programmes, databases, or microfilm.

Further, for most of the provisions since discretion lies with the Learned High Court Judge to either impose a fine or a sentence, an offender found guilty could go home after paying a fine as decided by the Judge.

Under **Section 4** of the Act, doing any act to secure unauthorised access for himself or for any other person, to a computer or to any information held in a computer, with the intention of committing an offence under this Act shall on conviction be liable to a fine not exceeding Rs. 200,000, or an imprisonment for a term not exceeding 5 years, or both.

Under **Section 5** of the Act, causing a computer to perform any function knowing or having reason to believe that such function will result in either a -

a. Modification* or
b. Damage* or
c. Potential Damage* to any computer or computer system or computer programme, whether such consequences be temporary or permanent in nature.

Under **Section 4** of the Act, merely turning a computer on is sufficient to be found guilty under the Act. However, the access intended needs to be secured and unauthorized.

Under **Section 5** of the Act, instances in which an offender causes a computer to perform a function which will result in any modification, damage or potential damage to the computer, computer system or programme can be covered.

Under the explanation provisions, it also states that any unauthorised modification or damage or potential damage to any computer or computer system or computer programme, could also extend to situations in which information held in a computer is destroyed, deleted, corrupted, moved or even altered.

Therefore, under sections 3 and 4 of the Act, an offender who has unlawfully or does any act to gain the access to a computer or the information held in a computer, which could mean any images saved on a technologically advanced mobile phone, does any act to move, delete or even alter such information or image/s can be found guilty under Section 5 of the Computer Crimes Act.

Therefore, a pertinent question arises under Section 4 of the Act whether any *'information'* obtained from a platform which was not intended to be secured or unauthorized to the general public, such as an image posted on a public social media platform will be taken into consideration according to the explanation provided under Section 4 of the Act.

However, under the *explanation* provision of Section 7 of the Act, which is also applicable sections 9 and 10, it is explicitly stated that it is immaterial that the offender had authority to access the computer or had authority to perform the function. Nevertheless, an explanation provision under Section 7, which is intended to be also used for Section 9 and 10 of the Act is applicable to explain an offence under Section 5 of the Act is also argumentative.

Under **Section 7** of the Act, any person who has obtained unlawful information or believes that the obtained information is unlawful from a Computer, buys, receives, retains, sells, or in any *manner* deals with, or offers to buy or sell, or downloads, uploads, copies, or acquires the substance or meaning of such information, shall on conviction be liable to a fine not less than Rs. 100,000/- and not exceeding Rs. 300,000/- or to imprisonment for a term not less than 06 months and not exceeding 03 years, or to both such fine and imprisonment.

Under **Section 7** of the Act, there are two issues to be addressed in terms of the applicability of the section:

The first question is whether, if a situation in which the offender had lawful access to such information and therefore whether obtaining such information for purposes it was not intended would still be covered? The answer is Yes, it can be. This is so, under the *explanation* provision of Section 7 of the Act, which is also applicable sections 9 and 10, it is immaterial that the offender had authority to access the computer or had authority to perform the function.

Secondly, a question arises whether the offender need to have the intention to cause loss or damage to a person or institution by committing such an offence? The answer, is NO. As per the explanation provided, the offender need not have intended to cause or have had the knowledge that he is likely to cause, loss or damage to any particular person or institution at the time of obtaining such information.

The Act is silent on what is meant by *'in any manner deals'* with. Such ambiguity however can be utilized for the benefit of a victim, as such could also mean sharing, posting, or even screen recording, or obtaining screen shots, air dropping etc. which modes are quite applicable in today's context given the certain advances in technology.

Under **Section 10** of the Act, any unauthorised disclosure of information enabling access to a service is an offence.

The Section clearly states that any person who was entrusted with information which enabled him access to any service provided by means of a computer discloses such information without having any authority to do so, shall on conviction be liable to a fine not less than Rs. 100,000 and not exceeding Rs. 300,000 or to an imprisonment for a term not less than 06 months and not exceeding 03 years or to both such fine and imprisonment.

Other information to keep in mind:

a. The sole jurisdiction to hear, try and determine cases under this Act is vested with the High Court.

b. Further, the Act also specifically states that not just an individual but even a body of persons, a corporation, a firm can also be found guilty for any of the listed offences.

c. Also, if an offence under this Act was committed outside the territory of Sri Lanka, it will be presumed / or consider to have been committed in Sri Lanka.

Under **section 10** of the Act, anyone who discloses information they are not authorized to disclose can be found guilty under the Act.

Under this section, anyone who was entrusted with information, which also means any data, text, images, sound, microfilm etc. violates such trust by disclosing such information entrusted on them, can be found guilty under the Act.

This Section can be utilized for an incident in which a victim places trust on a person who repairs mobile phones, or laptops and shares the password with consent for the sole purpose of getting a certain device fixed. In such an instance if such shop owner discloses such information enabling parties who were not authorized to access such service provided by such device can be found guilty under Section 10 of the Computer Crimes Act.

It is apparent from the above analysis that the offence of doxing, which is the act of publicly providing personally identifiable information about an individual or an organization can be covered under Section 10 of the Computer Crimes Act.

However, Section 10 of the Computer Crimes Act, invokes a limited situation in which a person has disclosed information which he/she was not authorized to do so, or in breach of any contract expressed or implied, and which disclosure has now resulted in enabling unauthorized access to a service provided by means of a computer.

d. If a person, who is arrested under this Act is not a citizen of Sri Lanka, then that person will be entitled to communicate without any delay to the nearest appropriate representative of the State, to be visited by such a representative, and to be informed of the fact that he has such rights.		This is so because the Act is predominantly concerned of individuals gaining access to a *'service provided by a computer',* although what is actually meant by a *'service provided by a computer'* is not identified or interpreted. Further, since the Act has placed explicit reference to the result of the offence being *'enabling access to a service provided by a computer',* it is unclear whether mere sharing of a person's information by an individual to cause harm, intimidation or harassment to such individual can be covered under the Act.
Personal Data Protection Act No. 09 of 2022		
What the Act is about: It became necessary for the Government of Sri Lanka to provide for a legal framework to provide for mechanisms for the protection of personal data of data subjects* ensuring consumer trust and to safeguard privacy whilst respecting domestic and applicable international legal instruments when processing personal data, which led to the development of this legislation in 2022.	Under **Section 56** of the Act, Personal data means, any information that can identify a data subject directly or indirectly, by reference to (a) an identifier such as a name, an identification number, financial data, location data or an online identifier (b) one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural, or social identity of that individual or natural person. Under **Section 2 (3)** of the Act, it very clearly mentions that the Act shall not apply to any personal data processed purely for personal, domestic or	When the Personal Data Protection Act is taken into account, it is very clear that the Act is not applicable to individuals but to a data processor or a controller. Therefore, a gap in law can be highlighted in terms of the offence of 'Doxxing', especially if for an instance, phone numbers of young girls are shared on a public platform by an individual without their due concurrence. However, in the event their details of email addresses together with the passwords are shared, then under Section 10 of the Computer Crimes Act, action can be taken as such

According to **Section 2** of the Act, it is important to remember that the Personal Data Protection Act applies to the processing of personal data under the following circumstances.

(a) where the processing of personal data takes place wholly or partly within Sri Lanka, or

(b) where the processing of personal data is carried out by a controller or processor who:

  (i) is domiciled or ordinarily resident in Sri Lanka

  (ii) is incorporated or established under any written law of Sri Lanka

  (iii) offers goods or services to data subjects in Sri Lanka including the offering of goods or services with specific targeting of data subjects* in Sri Lanka or

  (iv) specifically monitors the behaviour of data subjects in Sri Lanka including profiling with the intention of making decisions in relation to the behaviour of such data subjects in so far as such behaviour takes place in Sri Lanka.

household purposes by an individual and that the Act is not applicable for any data other than for personal data.

disclosure of information *'enables access to a service argumentatively provided by a computer',* but not under the Personal Data Protection Act, as and when the offender is an individual and is not a data processor or a controller.

Observations

Hence, it's crucial to highlight that, according to the Information and Cyber Security Strategy of Sri Lanka for 2019–2023, as published by the Sri Lanka Computer Emergency Readiness Team (SLCERT) Coordination Centre in collaboration with the Ministry of Digital Infrastructure and Information Technology, there were 54 instances of phone number misuse recorded in Sri Lanka between 2012 and 2017. However, as previously outlined, Sri Lanka lacks specific legislation addressing the misuse[1] of phone numbers, a category that could potentially encompass the offense of 'Doxxing'—the act of publicly disseminating personally identifiable information about an individual or organization, typically over the Internet.

In contrast, jurisdictions such as Hong Kong have taken legislative steps to address such issues. The Personal Data (Privacy) (Amendment) Ordinance 2021[2] amended the existing law to explicitly recognize offenses like 'Doxxing,'[3] acknowledging its significant rise in recent years. A Government Spokesperson representing the Hong Kong Special Administrative Region, in a press release, conveyed that:

> *"Since 2019, doxxers have attacked those of different political stances through the indiscriminate disclosure of their personal data, in effect weaponizing the personal data concerned. The Ordinance aims to combat malicious doxxing acts that have become more rampant in recent years, so as to protect the personal data privacy of the general public. We have to spare no efforts to combat such despicable doxxing acts that have a clear intent to harm, so as to eliminate conflicts in the society and establish the virtues of law-abidance and mutual respect..."* [4].

[1] Book - Strategy 2019-2023 (cert.gov.lk)
[2] s12021254032 (gld.gov.hk)
[3] The Personal Data (Privacy) Amendment Ordinance 2021 (pcpd.org.hk)
[4] Personal Data (Privacy) (Amendment) Ordinance 2021 comes into effect today (info.gov.hk)

Following the enactment of the new law, the Office of the Privacy Commissioner for Personal Data (PCPD) has issued a Gazette outlining the guidelines for investigating and prosecuting doxing-related offenses. This publication serves as a reference for the public, and the PCPD has undertaken the responsibility of educating and enlightening the public about the Act through mediums such as radio, television, posters, pamphlets, and more.[5]

In a recent legal case, Junior Police Officers' Association of the Hong Kong Police Force v Electoral Affairs Commission and others [2019][6], it was highlighted that over 2,000 police officers and their families, including young children in many instances, were victims of doxxing. This involved the extensive leaking of their personal information, leading to cyberbullying on the internet and various social and other media platforms. These doxxing practices resulted in widespread insecurity and infringements on their right to privacy.

Further, similar regulatory frameworks can be observed in other jurisdictions, including the Protection from Harassment Act 2014 in Singapore[7] as amended in 2019[8] recognized the publication of identity information, the Enhancing Online Safety Act 2015 in Australia[9] and the recently enacted Online Safety Act in 2021[10] recognized and the Harmful Digital Communications Act 2015 in New Zealand[11].

[5] ibid
[6] Junior Police Officers' Association Of The Hong Kong Police Force v Electoral Affairs Commission And Others - Case Law - VLEX 847860552
[7] Protection from Harassment Act 2014 - Singapore Statutes Online (agc.gov.sg)
[8] Protection from Harassment (Amendment) Act 2019 - Singapore Statutes Online (agc.gov.sg)
[9] AUS105255 2017.pdf (ilo.org)
[10] Online Safety Act 2021 (legislation.gov.au)
[11] Harmful Digital Communications Act 2015 No 63 (as at 09 March 2022), Public Act Contents – New Zealand Legislation

In Australia, under the recently enacted Online Safety Act 2021, a person must not post certain categories of materials which cover cyber-bullying material targeting an Australian child or an adult. So long as the materials are classified as cyber-bullying and targeted at an Australian child or adult, the Commissioner would have the power to issue a request to remove the material concerned within 24 hours subject to receiving notice.

Further, under Section 108 of the Code of Criminal Procedure in India [12] , it provides security for good behaviour from persons disseminating seditious matters, including obscene matters as follows —

> *(1) When 2 [an Executive Magistrate] receives information that there is within his local jurisdiction any person who, within or without such jurisdiction, —*
>
> *(i) either orally or in writing or in any other manner, intentionally disseminates or attempts to disseminate or abets the dissemination of,*
>
> *(a) any matter the publication of which is punishable under section 124A [13] or section 153A [14] or section 153B [15] or section 295A [16] of the Indian Penal Code (45 of 1860), or*
>
> *(b) any matter concerning a Judge acting or purporting to act in the discharge of his official duties which amounts to criminal intimidation or defamation under the Indian Penal Code (45 of 1860),*
>
> *(ii) makes, produces, publishes, or keeps for sale, imports, exports, conveys, sells, lets to hire, distributes, publicly exhibits or in any other manner puts into circulation any obscene matter such as is referred to in section 292 of the Indian Penal Code (45 of 1860)*

[12] THE CODE OF CRIMINAL PROCEDURE, 1973 (legislative.gov.in)

[13] Sedition.

[14] Promoting enmity between different groups on ground of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony

[15] Imputations, assertions prejudicial to national integration

[16] Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs

Category 02 Impersonation of Identity

Impersonation of another person's identity on an online platform for various intents and purposes.

Penal Code of Sri Lanka as amended		
About the Applicable Domestic Laws	**Scope and Purview of the Laws**	**Identified Gaps/Issues in the Laws**
What the Section is about: Under Section 399 of the Penal Code, sets out the offence of Personation. Personation means to assume the duty of another person with the intent to deceive. Therefore, according to the section, a person said to "cheat by personation " : **a)** if he cheats by pretending to be some other person, or **b)** by knowingly substituting one person for another, or **c)** representing that he or any other person is a person other than he, or such other person really is.	The Section can be applicable for instances in which a person is pretending to be someone else in the physical world as well as in the virtual world, especially in the case of a fake social media account. Therefore, if anyone pretends to be a person they are not especially on platforms like social media, then this section can be very useful.	The Section does not expressly provide for instances of 'Identity theft' as recognized in other jurisdictions. Further Section 399 is also claimed to be used to discriminate members of the LGBTQ+ community, especially the transgender community whose gender has not yet been re-recognized by the Gender Recognition processes and procedures listed under the Ministry of health, Sri Lanka.

What will be the sentence if found guilty: Under Section 400 of the Penal Code, a person who is found to be guilty of Cheating therefore shall be punished for a term which may extend to one year or with fine or with both. **Other information to keep in mind:** Triable in Magistrate's Court, the charge of cheating is not bailable and is also not compoundable.		

Observations

Although identity theft is not specifically recognized in Sri Lanka, out of the 3,675 social media related incidents reported, 2,018 of them have been incidents of fake social media accounts according to the Information and Cyber Security Strategy of Sri Lanka, 2019 – 2023 published by the Sri Lanka Computer Emergency Readiness Team (SLCERT) [17].

Nevertheless, the Information Technology Act 2000 in India [18] which deals with the legislation in India governing Cyber Crimes, Punishment for Identity Theft is set out under Section 66 C, and states that:

> *whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.*

Further, Section 66 D on Punishment for cheating by personation by using computer resource, states that:

> *whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.*

[17] ibid 1

[18] A2000-21_0.pdf (legislative.gov.in)

Category 03 Cyber Sexual Harassment

An act of causing or attempt to cause harassment or annoyance to an individual/or a group of individuals/ institution etc. by action or by words for various intents and purposes not limited to humiliation, intimidation or to infliction of fear of violence, exclusion, or isolation within their respective society.

The Penal Code of Sri Lanka as amended		
About the Applicable Domestic Laws	**Scope and Purview of the Laws**	**Identified Gaps/Issues in the Laws**
What the Section is about: Under **Section 345** of the Penal Code as amended by Act No. 22 of 1995 and Act No. 16 of 2006, states that whoever: **a)** by assault or **b)** use of criminal force sexually harasses another person, or **c)** by the use of words or **d)** actions, causes sexual annoyance or harassment to such other person.	In the context of online harassment too this provision can be used as there is no explicit reference to this section being limited to being applied only in matters connected to harassment in the physical world. In Sri Lanka, therefore due to the lack of criminal laws to counter online gendered hate speech, this section can be utilized. However, in terms of hate speech that *incite* violence amongst religious groups we have plenty of laws provided by the Penal Code, International Covenant on Civil and Political Rights [19], Prevention of Terrorism Act [20], Police Ordinance [21],	It is clear that the section does not clearly define what Sexual Harassment or Sexual Annoyance means, but how that can be caused either physically or verbally. Further, under the *explanation* provisions, the Section goes on to identify *unwelcome sexual advances by words or actions used by a person in authority, to a working place or any other place* shall constitute the offence of sexual harassment.

[19] https://www.lawnet.gov.lk/wp-content/uploads/2016/12/INTERNTIONAL-COVENANT-ON-CIVIL-AND-POLITICAL-RIGHTS-ICCPR-ACT-NO-56-OF-2007.pdf

[20] PREVENTION OF TERRORISM – LawNet

[21] police_ordinance.pdf

What will be the sentence if found guilty:

Shall on conviction be punished with imprisonment for a term which may extend to 05 years or with fine or with both and may also be ordered to pay compensation of an amount determined by court to the person in respect of whom the offence was committed for the injuries caused to such person.

Other information to keep in mind:

1) Under Section 345 of the Code, assault may include that does not tantamount to the offence of Rape under Section 363 of the Code, and injuries can also mean psychological and mental trauma.

2) This offence is triable in Magistrate's Court, bailable and is not compoundable.

and even by the Constitution [22] of Sri Lanka.

Further, as a civil remedy, a victim can also file action under the laws on Defamation.

Therefore, a reasonable question may arise as to whether any comment/ post or message on an online platform by a colleague at work which amounts to an 'unwelcome sexual advance' can also be considered as an *"unwelcome sexual advance"* especially if the colleague who made the comment was *not* someone who is in authority.

Further, another question may arise as to whether any online platform, such as social media, Messenger, WhatsApp etc. can necessarily be construaed under 'any other place' in which such sexual harassment may occur.

[22] https://www.parliament.lk/files/pdf/constitution.pdf

Observations

The aforementioned category is reclassified into distinct forms representing potential occurrences of cyber harassment. Despite the explicit reference in Section 6 (1) (c) of the Computer Crimes Act, stating that individuals causing danger or imminent danger to public order are punishable, it remains challenging to determine whether this provision adequately addresses issues related to online gendered hate speech. This complexity arises from the fact that hate speech, occurring within the realm of Cyber Harassment induced by bullying, stalking, or monitoring, typically targets individuals or specific communities, rather than broad religious groups. Such targets may include young girls or a group of young girls spanning different age categories, ethnicities, or religions.

Although Cyber Harassment or Bullying lacks specific recognition in Sri Lankan laws, the Information and Cyber Security Strategy of Sri Lanka for 2019–2023, published by the Sri Lanka Computer Emergency Readiness Team (SLCERT) [23] , reveals that out of the 3,675 reported social media-related incidents, 57 were instances of social media bullying.

Nevertheless, we have observed how certain State Commissions have taken the initiative to ensure that there be no harassment or bullying especially in times of an election against any candidate, independent group, or a political party. One such initiative was when the Election Commission of Sri Lanka by Extraordinary Gazette Notification No. 2178/24 dated 03rd June 2020 [24], where certain Media Guidelines were issued in terms of Article 104B(5)(A) of the Constitution Sri Lanka by the Elections Commission. The purpose of which was to *inter-alia* ensure that all telecasting, broadcasting and print media shall be neutral and impartial in their reporting matters related to an election, and not to discriminate any individual, independent group or political party. However, such guideline lacked the capacity to fully monitor compliance, and experience shows that guidelines are not always followed by either state or private media due to the lack of sanctions attached to it.

[23] Ibid 1

[24] PG 4996 (E) Election.pmd (documents.gov.lk)

In the Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective 2018 [25], it was recognized that online and ICT-facilitated acts of gender-based violence against women and girls include threats of such acts that result, or are likely to result, in psychological, physical, sexual or economic harm or suffering to women and such risk of harm arises from both online content (sexist, misogynistic, degrading and stereotyped portrayals of women, online pornography) and behaviours (bullying, stalking, harassment, intimidation facilitated and perpetrated via social media, tracking applications, and profiling technology) [26].

It must also be noted here that in 2015, the Human Rights Council (HRC), in its resolution 29/14 [27], recognized that domestic violence could include acts such as cyberbullying and cyberstalking — thereby reinforced that online gender-based violence is a continuing violence against women — and that the Member States had a primary responsibility for preventing and promoting the human rights of women and girls facing violence, including those facing domestic violence.

In this backdrop, as a response to the rampant and alarming trends of growing xenophobia, racism and intolerance, violent misogyny [28], antisemitism and anti-Muslim hatred around the world, United Nations Secretary-General (UNSG) António Guterres launched the United Nations Strategy and Plan of Action [29] on Hate Speech on the 18th of June 2019., in which it was highlighted that tackling hate speech is the responsibility of all governments, societies, the private sector, starting with individual women and men. All are responsible, all must act. However, yet Sri Lanka has no clear or specific laws on gendered online hate speech or to tackle any forms of online harassment.

[25] G1818458.pdf (un.org)

[26] Ibid 20

[27] Para 4 of G1516182.pdf (un.org)

[28] Misogyny is hatred of, contempt for, or prejudice against women. It is a form of sexism that is used to keep women at a lower social status than men, thus maintaining the social roles of patriarchy.

[29] UN Strategy and Plan of Action on Hate Speech 18 June SYNOPSIS.pdf

In Singapore, Protection from Harassment Act 2014 in Singapore [30] as amended in 2019 [31], recognizes protects persons against harassment and unlawful stalking [32] and false statements of fact, and to provide for the establishment of the Protection from Harassment Court. Specifically, under Section 7 (3) of the Act, it also states ways or examples in which unlawful stalking may be committed as follows:

(a) following the victim or a related person;

(b) making any communication, or attempting to make any communication, by any means —

i) to the victim or a related person;

(ii) relating or purporting to relate to the victim or a related person; or

(iii) purporting to originate from the victim or a related person;

(c) entering or loitering in any place (whether public or private) outside or near the victim's or a related person's place of residence or place of business or any other place frequented by the victim or the related person;

(d) interfering with property in the possession of the victim or a related person (whether or not the accused has an interest in the property);

(e) giving or sending material to the victim or a related person, or leaving it where it will be found by, given to or brought to the attention of, the victim or a related person;

(f) keeping the victim or a related person under surveillance.

[30] Protection from Harassment Act 2014 - Singapore Statutes Online (agc.gov.sg)

[31] Protection from Harassment (Amendment) Act 2019 - Singapore Statutes Online (agc.gov.sg)

[32] Section 7 of the Act

Further under Section 7 (5) of the Act, it provides the factors that the court must take into account when considering whether a course of conduct is likely to cause harassment, alarm or distress to a victim, as follows:

(a) the number of occasions on which the acts or omissions associated with stalking were carried out;

(b) the frequency and the duration of the acts or omissions associated with stalking that were carried out;

(c) the manner in which the acts or omissions associated with stalking were carried out;

(d) the circumstances in which the acts or omissions associated with stalking were carried out;

(e) the particular combination of acts or omissions associated with stalking comprised in the course of conduct;

(f) the likely effects of the course of conduct on the victim's safety, health, reputation, economic position, or the victim's freedom to do any act which he or she is legally entitled to do or not to do any act which he or she is not legally bound to do; and

(g) the circumstances of the victim including his or her physical or mental health and personality

Furthermore, under the Prevention of Domestic Violence Act [33] in Sri Lanka, Section 23 of the Act explicitly recognizes 'domestic violence' to mean, any emotional abuse, committed or caused by a relevant person within the environment of the home or outside and arising out of the personal relationship between the aggrieved person and the relevant person; Further "emotional abuse" is defined to mean a pattern of cruel, inhuman, degrading or humiliating conduct of a serious. Therefore, even under the Prevention of Domestic Violence Act Sri Lanka, such offences analysed before can be taken into consideration, especially if such offences have resulted in causing an emotional abuse.

[33] https://www.refworld.org/pdfid/4c03ba2f2.pdf

Category 04 Exploitation of Women and Children using technology.

An act of causing threats or attempt to cause threats to share images/videos of a person sexual/intimate in nature obtained with/without their consent as the means of coercion for both monetary and non-monetary gains.

1. Sextortion: The act of threatening to share nude or explicit images.

The Penal Code of Sri Lanka as amended		
About the Applicable Domestic Laws	**Scope and Purview of the Laws**	**Identified Gaps/Issues in the Laws**
Under **Section 483** of the Penal Code, the offence of Criminal Intimidation is provided as follows: Whoever threatens another with any injury to his person, reputation, or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.	Although the Penal Code of Sri Lanka has no express provision on Sextortion, the offence of Criminal Intimation is deemed to suitable to tackle an issue of this nature. This is since the offence of Criminal Intimidation also covers an incident in which a person is threatened with injury to his/her reputation, as in a case of sextortion.	Sections 372 and 373 of the Penal Code of Sri Lanka covers the law on extortion, through which, if the offender intentionally puts any person in fear of an injury to that person or to any other and dishonestly induce that person to deliver any property or valuable security or anything signed or sealed is known as extortion. However, the offence of 'sextortion' is quite different to that of 'extortion'. In that the offender who has with or without consent has in his/her possession nude/explicit/obscene pictures, videos etc. of the victim, and could now be threating the victim to release them unless and otherwise his/her demands are met.

According to **Section 486** of the Penal Code, the sentence afforded to such an offence given is twofold:

1) In the first instance, anyone who commits the- offence of criminal intimidation shall be punished with imprisonment which may extend to 02 years, or with fine, or with both.

2) Secondly, if the threat be, amongst other things, to impute unchastely to a woman, shall be punished with imprisonment which may extend to 07 years, or with fine, or with both.

Under the Penal Code, injury is also defined to include psychological and mental harm.

Therefore, although the offender has not yet acted on what he/she has threatened to do a mere threat to cause:

a. injury to the victim, or

b. injury to victim's reputation or property, or

c. injury to a person or

reputation of anyone that the victim has an interest in will be sufficient to form liability under this offence provided that:

a) the victim can prove that such threat to cause injury made the victim alarmed or

b) that such threat caused the victim to do any illegal act or

c) that such threat caused the victim not to do an act which the victim was legally entitled to do in order to avoid such threat being executed.

Section 2 (2) (a) of the Obscene Publications Ordinance explicitly prohibits an incident in which obscene writings, drawings, prints, paintings, printed matter, pictures, posters, emblems, photographs, cinematograph films, video cassettes or any other obscene objects are distributed or for other purposes which may not even be recognized by the Act.

On the other hand, 'Imputing Unchastity to women' [34] according to the Oxford dictionary means a woman who had committed adultery or engages in adulterous relationships or multiple sexual relationships. Therefore, imputing unchastity to a woman is undoubtedly derogatory and is defamatory in nature. Thus, if the threat is such that it causes threat to impute unchastity to a woman, such an offence receives a higher sentence according to Section 486 of the Penal Code.

However, it too makes no reference to an offence of sextortion, where a victim is threatened to release certain obscene images in the possession of the offender unless his/her demands are met.

Nonetheless, under the Act, it is also an offence to *"make or produce, or have in possession for purposes stated or otherwise, obscene... Photographs".*

Therefore, although the Ordinance is silent on the offence of sextortion per se, perhaps the same Ordinance can be utilized to charge the offender for either making, producing or for even having in possession such obscene materials for the purpose of threatening the victim, which purpose although not explicitly mentioned is also invariably accommodated as a purpose stated or otherwise.

[34] Imputation of unchastity - Oxford Reference

2. Exploitation, and/or trafficking of women and girls through the use of technology and Online Child Exploitation

Technologies are used to target and capture women and girls for sexual exploitation, force them to accept trafficking and sexual abuse situations, exercise power and control over them, and prevent them from freeing themselves from the abuse, including by threatening to disclose private information [35].

Convention on Preventing and Combating Trafficking in Women and Children for Prostitution Act No. 30 of 2005		
About the Applicable Domestic Laws	**Scope and Purview of the Laws**	**Identified Gaps/Issues in the Laws**
What the Act is about: Government of Sri Lanka became a signatory to the Convention on Preventing and Combating Trafficking in Women and Children for Prostitution in 2002, Kathmandu, Nepal. As a result of which, this Act came into realization, as it was obligatory for the signatory to make legal provision to give effect to the provisions of the Convention signed.	According to the definition given on what Sexual Exploitation of a child means, a question arises as to whether coercing and blackmailing children for sexual purposes using technology, would be covered under the Act. The Act explicitly speaks of 'Trafficking' as opposed to 'Exploitation' and has gone to the extent of defining what 'Trafficking' is.	Therefore, this Act is applicable to a situation in which a woman or a child is being sold, bought, or moved for the purpose of 'Prostitution' it can be considered as Trafficking within the strict meaning of the Act. Thus, a question arises as to whether coercing and blackmailing women or children for sexual purposes online, can be covered under the Act, unless such 'sexual purposes' would mean 'prostitution' in the deciding case.

[35] Under this section, special focus will be shed on Online Child Sexual Exploitation of Children, as every other form of Online Sexual and Gender Based Violence can be considered as various forms through Online Sexual Exploitation of Women can be committed.

What offences are covered in the Act:

Under Section 02 (1) and (2) of the Act, any person who commits, aids and abet to commit, attempts to commit, or conspires to commit,

a. keeps, maintains, or manages,

b. knowingly finances or takes part in financing or,

c. knowingly letting or renting, a building or other place or any part for the purpose of trafficking of women and children for prostitution or any matter connected.

What will be the sentence if found guilty?

A person found guilty will be punished with imprisonment for a period not less than 03 years and not exceeding 15 years and be liable to a fine.

Other information to keep in mind:

a. The above offences are triable under the High Court* of Sri Lanka.

b. A child means a person who has not attained the age of 18 years.

c. Trafficking means the moving, selling or buying of women and children for prostitution within and outside a country for monetary or other considerations with or without the consent of the person being subjected to trafficking

Children and Young Persons Harmful Publications Act No. 48 of 1956.

What the Section is about:

This Act prevents the dissemination of certain pictorial publications harmful to children and young persons.

What offences are covered in the Act:

Under Section 3 of the Act,

a. anyone who prints, publishes, sells, or allows such publication to be hired,

or

c. has in his possession any such publication for the purpose of selling it or for such publication to be hired will be considered as offences.

What will be the sentence if found guilty:

Will be liable to a fine not exceeding Rs. 1000/-, or imprisonment not exceeding 06 months or to both such fines and imprisonment.

According to the definition given on what Sexual Exploitation of a child mean, under the Children and Young Persons Harmful Publications Act, it is only an offence to print, publish, sell, or allow such publication to be hired or to have such publication in possession with the intention of selling or having that material hired.

It must also be noted that the sanction of the Attorney General must be received to prosecute under this Act.

The Act is silent on whether having such child sexual abuse material in possession for the personal consumption is an offence.

Further, the definitions of who a 'young person' is problematic as there are laws such as the Employment of Women, Young Persons and Children Act No. 29 of 1973 (as amended), where a child is defined as a person who is under the age of 16 and a young person is defined as a person who has attained the age of 16 but is under the age of 18.

Further, under the Convention on Preventing and Combating Trafficking in Women and Children for Prostitution Act No. 30 of 2005 a child means a person who has not attained the age of 18 years.

Nevertheless, under the Children and Young Persons Harmful Publications Act No. 48 of 1956, a child is a person under the age of 14 years and a young person is a person who has attained the age of 14 years but is below 16 years.

Other information to keep in mind: **a.** The above offences are Triable* by the Learned Magistrate's Court **b.** According to the Act, a child is a person under the age of 14 years. **c.** According to the Act, a young person is a person who has attained the age of 14 years but is below 16 years. **d.** To prosecute under this Act, sanction of the Attorney General should be received.		A child is defined as a person below the age of 18 according to our Penal Code, striking a similarity with the age defined for a child under the Child Rights Convention.

Penal Code of Sri Lanka as amended

What the Act is about: The Penal Code in Sri Lanka enacts the criminal and penal laws in Sri Lanka. Under the Penal Code, several sections of the Penal Code such as Sections 286A, 286B, 286C, 360B, 360C and 360E are dedicated to recognizing the wrongdoings committed against Children.	Sections 286A, 286B, 286C and 360B of the Penal Code (as amended) has very strong legal provisions to counter offences against child exploitation. A child is defined as a person below the age of 18 according to our Penal Code, although as we may have observed the age of the child may have varied in other special laws.	

What offences are covered in the Act and its sentence:

1) Section 286A of the Act makes legislative provision to criminalize obscene publication exhibition &c relating to children. Child means a person under 18 years of age.

On conviction will be imprisoned for a term not less than 02 years and not exceeding 10 years and may be with a fine.

If you are a developer of such material, then on conviction you are liable to an imprisonment for a term not less than 02 years and not exceeding 10 years and may also be punished with a fine.

2) Section 286B recognizes the legal duty of each person, who either provides a service by means of a computer or someone with such knowledge of a computer being utilized to commit such crimes, to inform and help prevent sexual abuse of a child.

On conviction will be liable to an imprisonment for a term not exceeding 02 years or to a fine or to both such imprisonment and fine.

Section 286B specifically provides provision to counter offences against child exploitation by means of a computer facility. Section 286B was incorporated into the Penal Code in 2006 and it is interesting to note that it holds dual provision to convict the person who uses such facility to exploit children, and even the person who has mere knowledge of such facility being in existence and is being used to realize such crimes for inaction if such crimes are not duly reported.

Under Section 286B, what amounts to a computer facility is not defined in our law. Nonetheless, when the definition of what tantamount to a 'computer facility' is searched online, it is clear that even a smart phone in today's context can be included under the same category given its embedded advanced technology in place to replicate the work of a computer. However, it is argumentative.

3) Section 286C recognizes the legal duty of any person who, having the charge, care, control, or possession of any premises, to inform the relevant authorities, if such premises are being used for the commission of such offences. On conviction will be liable to an imprisonment for a term not exceeding 02 years or to a fine or to both such imprisonment and fine. This Offences from Sections 286A, 286B and 286C are also bailable*, not compoundable* and is triable in Learned Magistrate's Court, and the Police may arrest the offender without a warrant.	Unlike the other sections discussed, under Section 286C, a legal duty is imposed on the any person to inform the relevant authorities about any such commission of offence. However, being able to prove that someone had knowledge of such commission of the crime will be a very difficult task to prove by the prosecution.	This section imposes accountability to a third party to keep the authorities informed of such commission of an offence. However, many due to the lack of legal knowledge have a natural tendency to believe that it is not up to them to keep the relevant authorities informed due to various social and political adversities they may have to encounter if such complaint to the authorities turns out to be nugatory.
4) Section 360B provides the ways in which a child can be sexually exploited. Will be liable on conviction to an imprisonment for a term not less than 05 years and not exceeding 20 years and may also be punished with a fine. Section 360B is also bailable*, not compoundable* and is triable in Learned Magistrate's Court, and the police officer shall not arrest without a warrant.	According to Section 360B therefore, following are the ways in which a child can be sexually exploited. Whoever – **(a)** knowingly allows a child to remain in premises for the purpose of such child to be sexually abused or to participate in any form of sexual activity or in any obscene or indecent exhibition or show.	Section 360B on the other hand covers a wide variety of ways in which a child can be exploited, including threats and through monetary considerations. Nevertheless, a pertinent question may arise as to whether a child who does any of these acts willingly will also be punished for causing exploitation on him or herself. However, provided that a child is under the age of 18 (as per the Penal Code of Sri Lanka),

	(b) acts as a procurer[36] of a child for the purposes of sexual intercourse or for any form of sexual abuse. **(c)** induces any person to be a client of a child for sexual intercourse or for any form of sexual abuse, by means of print or other media, oral advertisements, or other similar means **(d)** takes advantage, of his influence over, or his relationship to, a child, to procure such child for sexual intercourse or any form of sexual abuse **(e)** threatens, or uses violence towards, a child to procure such child for sexual intercourse or any form of sexual abuse **(f)** gives monetary consideration, goods or other benefits to a child or his parents with intent to procure such child for sexual intercourse or any form of sexual abuse.	any act willingly done for or by him/herself will be irrelevant as a person below the age of 18 is considered as a person who cannot give consent or show willingness to such act being committed. Therefore, any act done to such person below the age of 18, will be considered as a criminal offence, despite the consent being obtained or not. Further, the generalized language used in describing what tantamount to Sexual Exploitation of Children can also act beneficial in prosecuting matters relating to Online Sexual Exploitation of children too.

[36] Someone who obtains or acquires.

Observations

There is a lack of consistent legal definition for Online Child Sexual Exploitation in both national and international frameworks. Consequently, the protective measures have been inconsistent in adapting to the evolving needs of the system to prevent and safeguard children from various forms of progressive harm. Despite this, numerous multilateral instruments rightly vary the definition of child sexual exploitation to align with diverse cultural, social, and political expectations.

However, the Luxembourg Guidelines, adopted by the Interagency Working Group in Luxembourg in 2016 [37], present a set of terminology guidelines for protecting children from sexual exploitation and abuse. Developed through the collaborative efforts of 18 partners, these guidelines aim to standardize terms and definitions related to child protection. In essence, Online Child Sexual Exploitation can generally be described as a scenario where a child (under eighteen years of age) engages in sexual activity in exchange for something, be it a benefit, promise, or gain.

With the escalating use of mobile phones by children and young individuals in Sri Lanka, gaining dominance in the country's cyber landscape, it becomes crucial to establish effective legislation to counteract and respond to any progressive abuse, harm, or potential exploitation of children. This is essential in line with the international obligations undertaken by the country.

The following table outlines key international instruments related to online child sexual exploitation and Sri Lanka's current status concerning each [38]:

[37] https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf

[38] https://www.veriteresearch.org/wp-content/uploads/2020/11/VeriteResearch-Study-on-Legal-Framework-on-Online-Child-Sexual-Exploitation-in-Sri-Lanka.pdf

Convention on the Rights of the Child (CRC)	Ratified: 12 July 1991
ILO Worst Forms of Child Labour Convention, 1999 (No. 182)	Ratified: 1 March 2001
Budapest Convention – Convention on Cybercrime (Council of Europe)	Acceded: 29 May 2005
Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (CRC-OPSC)	Ratified: 22 Sept 2006
Palermo Protocol - Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children	Ratified: 15 June 2015
Rio Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents – World Congress 2008:	Sri Lanka is a member state.
WeProtect Global Alliance.	Sri Lanka is a member state.
South Asian Initiative to End Violence Against Children (SAIEVAC)	Sri Lanka is a member
Luxembourg Guidelines 2016	N/A
Lanzarote Convention – Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Council of Europe)	Sri Lanka is not a state party

Further, despite the above international commitments, the Government of Sri Lanka is robustly bound by Chapter VI of Constitution of Sri Lanka which has listed the Directive Principles of State Policy and Fundamental Duties, Article 27 (13) [39] very clearly states as follows:

[39] https://www.parliament.lk/files/pdf/constitution.pdf

> *"The State shall promote with special care the interests of children and youth, so as to ensure their full development, physical, mental, moral, religious and social, and to protect them from exploitation and discrimination"*

Furthermore, under Chapter III of the Constitution under which, the constitution has recognized the fundamental right to Equality under Article 12. Article 12 (4) [40] of the Constitution states as follows:

> *"Nothing in this Article shall prevent special provision being made, by law, subordinate legislation or executive action for the advancement of women, children or disabled person"*

Therefore, it is abundantly clear that ensuring such effective preventive and response state mechanisms exist for the safety, protection and welfare of both children and women of the State is a duty and a responsibility of the State as directed by the very own constitution of the Country. Failure to comply would result in palpable adverse results to the greater public.

[40] Ibid.

A Word about the Online Safety Bill 2023

On September 18, 2023, the Ministry of Public Security officially published a Bill entitled 'Online Safety[41],' aiming to establish the Online Safety Commission. The proposed legislation includes provisions to prohibit the online communication of certain factual statements in Sri Lanka. It also addresses the prevention of the use of online accounts, particularly inauthentic ones, for prohibited purposes. The Bill further outlines measures to identify and declare online locations used for prohibited activities in Sri Lanka. Additionally, it seeks to curb the financing and other forms of support for the dissemination of false statements of fact. These provisions are interconnected with various aspects of online safety, reflecting an effort to shape the legislative landscape in Sri Lanka. It is worth noting that the timing and content of this gazette bear resemblance and coincidence with the Online Safety Bill introduced in the United Kingdom Parliament in 2022, suggesting a parallel effort to address similar concerns in the digital realm.

Despite the outlined objectives in Clause 03 of the Bill, including the protection of individuals from harm caused by false or threatening statements, ensuring safeguards against contempt of court or statements prejudicial to the judiciary's authority, implementing measures to prevent the misuse of online accounts and bots for offenses under the Act, and curbing the financing and support of online locations disseminating false statements in Sri Lanka, it has led to 45 petitions[42] being filed in the Supreme Court. Concerned parties have expressed apprehension about potential violations of the fundamental rights guaranteed by the Constitution of Sri Lanka.

Some of the petitions have pointed out the curious aspect of the Minister responsible for Public Security introducing the Bill, rather than the Ministry of Mass Media and Digital Technology. Consequently, the same Minister will be responsible for appointing experts to aid investigations, and these experts, who are private individuals, will be granted significant powers by the Commission. These individuals can accompany police officers during search procedures and, with the authority granted by a police officer above the rank of a sub-inspector, can compel individuals to surrender documents or devices, provide traffic data, or undergo oral examination. The concentration of such extensive powers in the hands of unaccountable private individuals raises concerns about potential avenues for abuse. The bill does not provide for judicial review of the Commission's decisions or procedures. Instead, Clause 49 seeks to protect the Commission, its staff, or any expert appointed under Clause 37 from being brought to court for any act or omission done in good faith.

[41] http://documents.gov.lk/files/bill/2023/9/284-2023_E.pdf

[42] https://www.dailymirror.lk/breaking_news/45-petitions-before-SC-against-Online-Safety-Bill-Speaker/108-269454

Concerns have been expressed about the impartiality of the Online Safety Commission, given that its five members will be appointed by the President based on qualifications. One of these members will serve as the Chairman and possess the casting vote in cases where the Commission's decisions result in a tie. This mode of appointment contrasts with other nominally independent commissions in Sri Lanka, where appointments necessitate the consent of the Constitutional Council through nomination or ratification. Consequently, this bill grants the President unrestricted discretion in both appointment and removal processes, deviating from established practices in other independent commissions.

Furthermore, within the Powers and Functions of the Commission, it is granted the authority, among other things, to maintain an online portal aimed at informing the public about the falsity of statements, conduct investigations and offer services as directed by any court, issue codes of practice for service providers and internet intermediaries offering communication services to end-users in Sri Lanka, and hold and manage movable and immovable property, with the ability to sell, lease, mortgage, exchange, or dispose of such property. Consequently, the Commission is endowed with a broad spectrum of powers, some of which encroach upon judicial functions. It assumes the role of the sole arbiter of matters of fact, empowered to issue notices or directives against any individual, internet service provider (ISP), or internet intermediary accused of disseminating prohibited or false statements. Notably, the bill lacks specificity regarding the decision-making process employed by the Commission.

Additionally, the Commission is authorized to block websites and instruct ISPs to restrict access to specific online locations. Such powers raise concerns about potential government overreach, censorship, and possible violations of the right to information safeguarded by Article 14A of the Constitution and international law.

The Bill draws a distinction between Prohibited Statements and False Statements. A Prohibited Statement is defined as one specified in Clauses 12 to 23 of the Bill, encompassing offenses falling under these sections. Among these 14 instances, only a select few, such as Cheating, Cheating by Personation, Doxxing, Online Harassment, Online Child Abuse, and Making or Altering Bots to Commit, can be considered as introducing new offenses necessary for our legal system. The remaining offenses involve statements that pose a threat to national security, public order, or promote feelings of ill-will and hostility among different classes of people. On the other hand, False Statements are characterized as statements known or believed by the maker to be incorrect or untrue, made with the intent to deceive or mislead. However, this definition excludes cautions, opinions, or imputations made in good faith, raising concerns about potential infringements on the fundamental rights of thought and expression.

Moreover, concerning measures against the communication of specific factual statements in Sri Lanka, concerns have been raised about the potential violation of the fundamental right to a fair trial. Complaints to the commission can be lodged by any person, either orally, in writing, or in electronic form, related to the commission of such an offense. Notably, the complainant is only obligated to serve a copy of the complaint to the person if it is feasible to do so.

Furthermore, when the Commission believes that sufficient material indicates the communication of a prohibited statement, it is empowered to conduct investigations through its officers. If the Commission is convinced that a prohibited statement has been communicated, it may issue a notice to the responsible party, considering the gravity of the matter and the potential harm caused by the statement. Importantly, the recipient of such a notice is required to comply immediately, but not later than twenty-four hours from the issuance. Failure to adhere to the notice within this timeframe prompts the Commission to issue a notice to the internet access service provider or internet intermediary facilitating the communication of the prohibited statement. This notice may instruct either the disabling of access by end users in Sri Lanka to the prohibited statement or the removal of the statement from the online location.

In the event that an individual affected by the communication of a prohibited statement seeks recourse, they have the option to apply to the Magistrate's Court through a petition and affidavit to obtain an order preventing the circulation of such information.

The bill lacks provisions for judicial review of the decisions or procedures of the Commission. Instead, Clause 49 aims to shield the Commission, its staff, or any expert appointed under Clause 37 from legal action for any act or omission undertaken in good faith. Consequently, for Sri Lanka's Online Safety Bill to truly be a transformative piece of legislation, adjustments are evidently needed to align it with the local context, as well as the political and legal landscape. However, Deputy Speaker Ajith Rajapaksa has disclosed that the Supreme Court recently noted certain sections of the Online Safety Bill as inconsistent with the Constitution, emphasizing the necessity for its approval by a special majority. Nonetheless, the bill could potentially be passed by a simple majority if the recommended amendments by the Supreme Court are incorporated.

Conclusion

Upon careful consideration of the analysis presented above, it is evident that the legal framework in Sri Lanka does contain provisions to address Online Sexual and Gender-Based Violence. However, navigating these provisions is not a straightforward task, as the interpretation of certain offenses can be subject to various perspectives. Complicating matters, offenses may exhibit duplicity, with one offense incorporating elements of another. The lack of uniformity in existing laws, exemplified by differing definitions of a child's age across legislations, further underscores the complexity.

To address these challenges effectively, it is imperative to formulate comprehensive laws, policies, and action plans that take into account the highlighted gaps. Regular monitoring and annual reviews of these laws and policies, with active collaboration from non-state organizations in Sri Lanka, are essential. This approach will not only enhance citizens' understanding of their rights but also clarify the state's role in safeguarding these rights, as mandated by the law.

The mainstream media plays a pivotal role in disseminating information on these laws and policies, ensuring that discussions reach ordinary citizens in a trilingual manner. This inclusive approach contributes to a broader understanding of legal frameworks and their implications. Additionally, legal actors, including defense attorneys, state prosecutors, judges, and other authorities such as the police, the cybercrimes division of the criminal investigation department, and SLCERT, must undergo continuous sensitization. This involves staying abreast of existing laws, understanding international developments, and, crucially, honing the best ways to respond to victims and survivors seeking assistance.

Sensitization efforts should extend to redress mechanisms, recognizing their paramount importance. Victims and survivors seeking legal redress often face inherent biases, entrenched perceptions, prolonged investigation delays, and a lack of knowledge about systems and procedures. Addressing these challenges is essential to create an environment that not only welcomes but also applauds and supports victims and survivors who come forward, fostering a culture of encouragement rather than discouragement.

Cyber Sexual and Gender-Based Violence in Sri Lanka
A Legal Gap Analysis

Search for Common Ground.
December 2023