Research Study on

Technology-Facilitated Violence experienced by Women and Marginalized Groups in Sri Lanka

UNFPA

UN WOMEN

Acknowledgements

Lead Author
Fazeeha Azmi

Contributors
Management Frontiers (Pvt) Ltd.: Amena Akhtar Mohsin, Ravimal Bandara, Dhanya Ratnavale, Isha Miranda and Priyanjith Abeykoon

UN WOMEN: Prashani Dias and Prashanthi Jayasekara

UNFPA: Poorani Radhakrishnan and Piyumani Ranasinghe

Editorial support
Piyumani Ranasinghe and Daupadi Suduwelikanda

Layout and design
Malin Pradeep

Copyright © 2025 United Nations Population Fund and United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), all rights reserved.
Reproduction is authorized provided the source is acknowledged.

How to cite this publication: UNFPA and UN WOMEN, 2025. "Research Study on Technology-Facilitated Violence Experienced by Women, Girls, LGBTQIA+ persons, and Ethnic Minorities in Sri Lanka." Colombo: UNFPA and UN WOMEN.

August 2025

Disclaimer
This report is a publication commissioned by the United Nations Population Fund (UNFPA) and United Nations Entity for Gender Equality and the Empowerment of Women (UN Women) in Sri Lanka. The views expressed in this publication are those of the authors and do not necessarily represent the views of UNFPA, UN Women, the United Nations or any of its affiliated organizations.

Contents

LIST OF TABLES i
LIST OF FIGURES iii
ACRONYMS iv
GLOSSARY v
EXECUTIVE SUMMARY 1

SECTION 1
INTRODUCTION TO THE RESEARCH 7
1.1 Background of the study 8
1.2 Defining Technology-facilitated gender-based violence 10
1.3 Global context 11
1.4 Sri Lankan context 12

SECTION 2
ABOUT THE STUDY 17
2.1 Introduction 18
2.2 Objectives and scope of the study 18
2.3 Research questions 19
2.4 Conceptual framework 19
2.5 Methodology and approach 20
2.6 Study districts 21
2.7 Quantitative data collection and the demographic 21
2.8 Qualitative data collection 24
2.9 Data analysis 25
2.10 Ethical considerations 26
2.11 Study limitations 27

SECTION 3
DATA ANALYSIS AND KEY FINDINGS 29
3.1 Understanding the prevalence of TFGBV 30
3.2 Understanding hate content online 33
3.3 Understanding motives of perpetrating TFGBV 39
3.4 Offline impacts of TFGBV 42

SECTION 4
RECOMMENDATIONS AND WAY FORWARD 48

ANNEXURES 56
Annexure I: Existing legal framework 56
Annexure II: Development of online tracking system and data extraction 57
Annexure III: List of key informant interviews conducted 62
Annexure IV: List of focus group discussions conducted 63
Annexure V: Data visualization 64

REFERENCES 90

List of tables

Table 1 : Number of complaints received during the last 5 Years – Institution Wise 64
Table 2 : Social media platforms use by respondents 64
Table 3 : Disaggregation of data by gender - Social media platforms use by respondents 64
Table 4 : Disaggregation of data by ethnicity - Social media platforms use by respondents 65
Table 5 : Disaggregation of data by ethnicity - Time spend on social media 65
Table 6 : No. of hours spent on social media 65
Table 7 : Type of content make you or others feels unsafe or targeted 66
Table 8 : Disaggregation of data by ethnicity - Type of content make you or others feels unsafe or targeted 66
Table 9 : Disaggregation of data by gender - Type of content make you or others feels unsafe or targeted 67
Table 10 : Disaggregation of data by women's ethnicity - Type of content make you or others feels unsafe or targeted 67
Table 11 : Method used to target the survivors 68
Table 12 : Disaggregation of data by gender – Method used to target the survivors (103 Respondents) 68
Table 13 : Disaggregation of data by ethnicity - Method used to target the survivors (103 Respondents) 69
Table 14 : Social media platforms used to target the survivors 69
Table 15 : Disaggregation of data by ethnicity – Social media platforms used to target the survivors 70
Table 16 : Respondents' opinion on the risk of being subjected to content 70
Table 17 : Disaggregated data by ethnicity and gender - Do not know the risk of being subjected to violent content 70
Table 18 : Disaggregation of data based on district - Respondents' opinion on the risk of being subjected to content 70
Table 19 : Disaggregation of data based on age - Respondents' opinion on the risk of being subjected to content 71
Table 20 : Disaggregation of data based on ethnicity - Respondents' opinion on the risk of being subjected to content 71
Table 21 : Disaggregation of data based on gender - Respondents' opinion on the risk of being subjected to content 71
Table 22 : Opinion on the contribution of social media for individuals to commit violence 71
Table 23 : Types of gender-based violence, girls and sexual minorities 72
Table 24 : Disaggregation of data by gender - Types of gender-based violence, girls and sexual minorities 72
Table 25 : Online forum or social media groups engage in targeting people 72
Table 26 : Disaggregation of data by women from various ethnic groups Complaints - Online forum or social media groups engage in targeting people 72
Table 27 : Individuals and institutions creating and sharing hate contents 73
Table 28 : Disaggregation of data by women from various ethnic groups complaints - Individuals and institutions creating violent contents 73
Table 29 : Disaggregation of data by women from various ethnic groups complaints - Individuals and Institutions Sharing violent contents 74
Table 30 : Motive behind posting violent content in social media platforms 74
Table 31 : Disaggregation of data based on ethnicity - Motive behind posting violent content in social media platforms 75
Table 32 : Disaggregation of data by Women from various ethnic groups complaints - Motive behind posting hate content in social media platforms 75
Table 33 : Factors in initiating offensive content online and offline 76
Table 34 : Disaggregation of data by ethnicity - Factors in initiating offensive content online and offline 76
Table 35 : Disaggregation of data by women from various ethnic groups complaints - Factors in initiating content online 77
Table 36 : Hate content and gender targeted hate content for the from 2021 to 2024 77
Table 37 : Disaggregation of data by language - Hate content and gender targeted hate content – Sinhala Language 77
Table 38 : Disaggregation of data by language - Hate content and gender targeted hatecontent – Tamil Language 78
Table 39 : Disaggregation of data by language - Hate content and gender targeted hate content – English Language 78
Table 40 : Intersectional analysis of gender targeted hate content 78

Table 41 : Social media is a safe space for everyone 78
Table 42 : Disaggregation of data by gender - Social media is a safe space for everyone 79
Table 43 : Disaggregation of data by ethnicity – Social media contributes to violence 79
Table 44 : Most affected minority groups on hate content both online and offline 79
Table 45 : Respondents personally targeted on hate content 79
Table 46 : Disaggregation of data by ethnicity – Survivors' ethnicity 79
Table 47 : Disaggregation of data by ethnicity - Survivors' ethnicity 80
Table 48 : Disaggregation of data by gender - Survivors' ethnicity 80
Table 49 : Disaggregation of data by region – No. of survivors 80
Table 50 : Disaggregation of data by gender – Frequency of social media usage 80
Table 51 : Frequency of been targeted online 80
Table 52 : Disaggregation of data by frequency of usage - Survivors' social media usage frequency 81
Table 53 : Age of the respondent when exposed to violent content 81
Table 54 : Initial reaction to being targeted on violent content 81
Table 55 : Comfortable with someone from the LGBTQIA+ community - (Without LGBTQIA+ respondents) 81
Table 56 : Respondents targeted offline 82
Table 57 : Frequency of being targeted offline 82
Table 58 : Disaggregation of data by gender and ethnicity – Targeted offline 82
Table 59 : Disaggregation of data by gender – Frequency of offline targeting 82
Table 60 : Offline actions impacting the survivors daily life 82
Table 61 : Disaggregation of data by gender – Offline actions impacting the survivors daily life 83
Table 62 : Content result negatively in the day-to-day lives of the targeted communities and people 83
Table 63 : Economic loss due to online and offline targeting 83
Table 64 : Type of economic loss due to targeting 83
Table 65 : Mobile, Internet and Social Media Usage 2019 and 2021 84
Table 66 : Recent incidents targeted to specific communities 84
Table 67 : Disaggregation of data by ethnicity - Recent incidents targeted to specific communities 84
Table 68 : Disaggregation of data different women ethnicities - Specific incidents that have affected the specific communities 84
Table 69 : Frequency of violent content associated with particular incidents 84
Table 70 : Disaggregation of data by ethnicity - Frequency of violent content associated with particular incidents 85
Table 71 : Social Media contents targeting women, girls, and the LGBTQ community 85
Table 72 : Disaggregation of data different women ethnicities - Specific incidents that have affected the specific communities 85
Table 73 : Disaggregation of data by ethnicity: Religious minorities targeted during the Easter Bombing/COVID 19 85
Table 74 : Ways of religious minorities targeted during Easter Bombing/COVID 19 86
Table 75 : Violent content affecting the minority communities 86
Table 76 : Complains were not made to authorities 87
Table 77 : Types of support to sought by the survivors 87
Table 78 : Reasons for not seeking counselling services 87
Table 79 : Awareness about the reporting of incidents 88
Table 80 : Institutions to which complaints were reported 88
Table 81 : Steps taken by the authorities 88
Table 82 : Awareness of the existing laws to punish offenders of violent content 88
Table 83 : Opinion about the Online Safety Bill 88

List of figures

Figure 1: Socio-demographic profile of the respondents of the study 22
Figure 2: Types of online content that make respondents feel unsafe or targeted 30
Figure 3: Forms of abuse experienced by TFGBV survivors 31
Figure 4: Forms of TFGBV content on social media 31
Figure 5: Offline consequences of TFGBV on survivors 32
Figure 6: Factors initiating TFGBV content online and offline 33
Figure 7: Motives behind posting violent content on social media (as reported by respondents) 34
Figure 8: Key perpetrators of TFGBV (as reported by respondents) 38
Figure 9: Forms of online and offline hate against ethnic/religious minorities during crises (as reported by respondents) 40
Figure 10: XLM-R Model 58
Figure 11: BiLSTM Model 58
Figure 12: % of Hate content and gender targeted hate content on Facebook - Sinhala Language 89
Figure 13: % of Hate content and gender targeted hate content on Facebook - Tamil Language 89
Figure 14: % of Hate content and gender targeted hate content on Facebook - English language 89

Acronyms

AI	Artificial Intelligence
BASL	Bar Association of Sri Lanka
CBO	Community Based Organization
CCID	Computer Crime Investigation Division
CSO	Civil Society Organization
DS	Divisional Secretariat
FGD	Focus Group Discussion
FTL	Field Team Leader
GBV	Gender-Based Violence
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
INGO	International Non-Governmental Organizations
IP	Internet Protocol address
IWF	Internet Watch Foundation
KI	Key Informants
KII	Key Informant Interview
LGBTQIA+	Lesbian, Gay, Bisexual, Transgender, Intersex, Queer or Questioning and Asexual
NCII	Non-Consensual Intimate Image Sharing
NCPA	National Child Protection Authority
NCW	National Council of Women
NGO	Non-Governmental Organization
ODK	Open Data Kit
OTS	Online Tracking System
PVE	Preventing Violent Extremism
QA	Quality Assurance
QS	Questionnaire Survey
SLCERT	Sri Lanka Computer Emergency Readiness Team
SPSS	Statistical Package for the Social Sciences
TFGBV	Technology-facilitated Gender-Based Violence
ToR	Terms of Reference
TRC	Telecommunications Regulatory Commission
UN	United Nations
UNFPA	United Nations Population Fund
UNHRC	United Nations Human Rights Council
UNICEF	United Nations Children's Fund
UNSG	United Nations Secretary-General
UN Women	United Nations Entity for Gender Equality and the Empowerment of Women

Glossary

Artificial intelligence (AI): The concept of computer programming that can be used to instruct computers and other digital devices to make decisions. Machine learning attempts to bring reality as close as possible to the concept of artificial intelligence.

Capacity-building: Developing skills, knowledge and resources in individuals and organizations to effectively address technology-facilitated gender-based violence. This includes training on digital literacy, trauma-informed care and legal frameworks.

Data point: A data point is a single piece of information or observation that represents a specific value or characteristic within a larger dataset such as an individual comment, post or a video title posted on social media platforms.

Deepfakes: Digital images, videos, and audio that are artificially altered or manipulated by AI and/or deep learning to make someone appear to do or say something that did not actually do or say. It is increasingly more difficult to distinguish artificially manufactured material from actual videos and images. Deepfakes are often used to create non-consensual sexual imagery that portray the target in a sexual manner.

Digital platform: Digital platforms are online businesses that facilitate commercial interactions and exchanges of information, goods or services to occur between producers and consumers as well as the community that interacts with said platform. Digital platforms can be social media platforms, knowledge platforms, media sharing platforms, or service-oriented platforms.

Doxxing: The malicious publication of personal, private or identifying information about an individual, such as publicly releasing someone's home and email addresses, phone numbers, employer and family member's contact information, etc. Often leads to further harassment.

Ethical considerations: The guidelines that dictate how data should be collected, managed and used, ensuring the privacy, confidentiality and dignity of technology-facilitated gender-based violence survivors.

Gendered disinformation: Strategy to silence women, girls and gender-diverse people and to dissuade them from participating in the public sphere. Involves the spread of information that relies on false or misleading gender narratives with the intent to cause harm. It incorporates three defining characteristics of online disinformation – falsity, malign intent and coordination.

Gendered hate speech: Any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in this case, based on their sex, gender, sexual orientation or gender identity. Specifically targets women, girls and LGBTQIA+ people and is based on patriarchy, misogyny, sexism, homophobia and transphobia.

Hacking: The use of technology to obtain illegal or unauthorized access to systems or resources for the purpose of attacking, harming or incriminating another person or organization by stealing their data, acquiring personal information, altering or modifying information, violating their privacy or infecting their devices with viruses.

Hate content: Any form of content that makes individuals or groups feel unsafe or targeted. This includes offensive, violent, harmful, misogynistic or abusive content, and any other online material used to harass or intimidate survivors.

Hate speech: Any kind of communication, verbal, written or behavioural, that is hostile or uses derogatory or discriminatory language against any person or group of people on the basis of who they are, or, in other words, on the basis of their religion, ethnic origin, nationality, race, skin colour, social origin, gender and other identity factors.

Image-based abuse: The use of imagery to coerce, threaten, harass, or abuse someone. Includes a range of behaviours such as the creation, distribution or threats to distribute intimate images without consent. When images are sexual in nature, we refer to this as "image-based sexual abuse."

Non-consensual intimate image (NCII) abuse: The non-consensual online dissemination of intimate images, obtained with or without consent, with the purpose of shaming, stigmatizing or harming the victim.

Online harassment: Online harassment on social platforms, the Internet, in chat rooms, instant messaging and mobile communications.

Online sexual harassment: Any form of online unwanted verbal or non-verbal conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular by creating an intimidating, hostile, degrading, humiliating or offensive environment.

Online child sexual exploitation and abuse: The sexualized exploitation and abuse of children facilitated by technology. This can include: grooming, live streaming, consuming child sexual abuse material, coercing and blackmailing children for sexual purposes.

Online platform: An online platform is a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet.

Online grooming: Children and young people are contacted through social media or other digital platforms, with the purpose of sexually assaulting them.

Sextortion: Use of ICT to blackmail a victim. In such cases, the perpetrator threatens to release intimate pictures of the victim in order to extort additional explicit photos, videos, sexual acts or sex from the victim.

Social media: Social media is a collective term for websites and applications that focus on Internet-based communication, community-based input, interaction, content-sharing and collaboration. Forums, microblogging, social networking, social bookmarking, social curation and wikis are among the different types of social media that allow quick electronic communication of content to users. Content includes personal information, documents, videos and photos. Users engage with social media via a computer, tablet or smartphone via web-based software or applications.

Technology-facilitated gender-based violence (TFGBV): An act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender.

Threats: A suggestion that something unpleasant or violent will happen, especially if a particular action or order is not followed.

Trolling: Involves someone posting or commenting online to deliberately provoke or upset others. An individual who perpetrates this behaviour is referred to as a 'troll.' A troll can also encourage others to join in the attack, leading to a pile-on where multiple people collectively target and harass the same person.

Victim-survivors: This is used to describe people who have direct experience of technology-facilitated gender-based violence. We use this term to acknowledge both the ongoing effects and harm caused by technology-facilitated gender-based violence and the resilience of people with lived experience of violence. We recognize that people may use different terms to describe their experiences.

EXECUTIVE SUMMARY

The rapid advancement of information technology has uncovered the widespread and growing threat of technology-facilitated gender-based violence (TFGBV), particularly against women, girls, LGBTQIA+ persons, and ethnic minorities. Global estimates show that 1 in 3 women experience physical or sexual violence in their lifetime, with TFGBV becoming an increasingly prevalent form. This violence not only causes long-term psychological, physical, and economic harm but also often escalates into offline abuse, threatening the safety and bodily integrity of those affected. Low levels of digital literacy, coupled with the rapid advancement in technology, have created new avenues for abuse. Yet, the responses from government and civil society actors remain inadequate, widening the gap in both prevention and survivor support. This study offers critical insight into the scale, context-specific nature, and evolving patterns of TFGBV shedding light on its forms, underlying motivations, and emergent trends.

This study, commissioned in 2024 by the United Nations Population Fund (UNFPA) and the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women) in Sri Lanka, explores the phenomenon of TFGBV, which disproportionately affects women, girls, LGBTQIA+ persons, and ethnic minorities. TFGBV as defined by UNFPA,[1] refers to "an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender." This study provides a comprehensive understanding of the nature, prevalence, impact, and prevention of TFGBV, with a particular emphasis on the spread of gendered hate content online. Its findings and recommendations aim to inform future research and policy interventions at the intersection of gender, hate content, and digital violence, while addressing the specific vulnerabilities of gender, sexual and ethnic minorities.

1 https://www.unfpa.org/sites/default/files/pub-pdf/UNFPA_Measuring%20TF%20GBV_%20A%20Discussion%20Paper_FINAL.pdf

Methodology

To contextualize the issue globally and locally, the study began with a comprehensive literature review and an assessment of Sri Lanka's legal and policy frameworks addressing Technology-facilitated gender-based violence. It also examined the role of non-governmental organizations in awareness-raising and advocacy. A mixed-methods approach was employed, combining both quantitative and qualitative data collection. Quantitative data were gathered through 361 questionnaire surveys targeting school leavers, university students, factory workers, LGBTQIA+ persons, differently abled persons, and survivors across five districts in Sri Lanka. Additionally, an online tracking system monitored TFGBV related content on five social media platforms for the period from 2021 to 2024. Qualitative insights were drawn from 43 key informant interviews and 11 focus group discussions with representatives from government agencies, civil society, community-based organizations, women politicians, professionals, ethnic and sexual minority groups. This integrated methodology enabled the study to capture the evolving nature, trends, motivations, and key actors involved in TFGBV offering a holistic understanding of its impact in the Sri Lankan context.

Key findings

1. The pervasiveness and evolving landscape of TFGBV

- Over 57 per cent of the 361 study participants reported feeling unsafe in online spaces, with 35 per cent unaware of online safety risks.
- Offensive visual content, including images, videos, cartoons, memes, objects, gestures, and symbols, contributed to 47.1 per cent of respondents feeling unsafe on social media platforms.
- Group-targeted offensive discourse (38.5 per cent) and threats to individuals (20.8 per cent) were also significant forms of online content making respondents feel unsafe or targeted.
- About 29 per cent of survey respondents, including purposively selected survivors (4 per cent of the sample), reported having survived TFGBV, with 12 per cent experiencing it daily or every other day.
- The most common abuses reported by survivors were obscene messages and videos (37 per cent), creation of fake profiles (37 per cent), and abusive calls (34 per cent).
- Social media platforms with higher usage rates, such as Facebook and WhatsApp were identified as key sites for online violence due to limited prevention and reporting measures.
- Common forms of TFGBV content on social media included revenge porn, blackmail, and cyber harassment.

- The study highlights the increasingly sophisticated nature of online abuse, often leveraging advanced technologies like AI to create deceptive content.
- A critical challenge is the inadequacy of AI content moderation tools in Sinhala and Tamil, allowing harmful content to persist on widely used platforms like Facebook and YouTube.
- A strong correlation exists between online hate content and its offline consequences; 92 per cent of respondents reported TFGBV occurring mostly online, but 54 per cent of survivors experienced offline harm.
- Offline consequences included physical violence, sexual harassment, stigma, reputational damage, mental health issues (including suicidal ideation), and loss of employment.
- As a result of TFGBV, 64 per cent of survivors withdrew from social media, 51 per cent faced relationship breakdowns, and 42 per cent faced community ostracism. Economic losses due to reputational harm and job loss were reported by 30 per cent.

2. Intersectional vulnerabilities and targeting of marginalized identities

- TFGBV is deeply rooted in gender inequality, patriarchy, and misogyny, and often exacerbates prevalent forms of offline violence. Online violence was primarily targeted against sexual orientation, gender identity, and cultural background of respondents.
- 90 per cent of study respondents believed social media increases the risk of gender-based violence, girls, and LGBTQIA+ individuals.
- LGBTQIA+ respondents reported high levels of safety concerns online.
- Disaggregated by ethnicity, 70 per cent of Muslim, 66 per cent of Sinhalese, and 60 per cent of Tamil respondents acknowledged social media's contribution to violence.
- Fewer than 5 per cent of Sinhala respondents felt safe online, compared to 19 per cent of Tamil and 15 per cent of Muslim respondents.
- Among women, 66 per cent of Sinhalese, 47 per cent of Muslim, and 40 per cent of Tamil women felt unsafe.
- 56 per cent of survivors were women, 27 per cent LGBTQIA+, and 17 per cent men, with most being under 30 years old.
- Humiliation of women and LGBTQIA+ persons (66 per cent), political gain (60 per cent), and ethnic/religious control (51 per cent) were identified as primary motivating factors for online hate.

- Hate content largely targeted women's appearance, attire, political views, caste, and religion, and subjected LGBTIQ+ persons to slurs, blackmail, and exclusion.
- Muslim (53 per cent) and Tamil (42 per cent) respondents reported higher exposure to identity-based hate than Sinhalese (31 per cent).
- LGBTQIA+ individuals (53 per cent) and women (47 per cent) were especially affected by offensive imagery and discourse online.

3. Nexus between national crises and TFGBV proliferation

- Periods of national crisis in Sri Lanka such as the COVID-19 pandemic, economic crisis, Aragalaya movement,[2] Easter Sunday Attacks have seen a significant proliferation of online hate content and TFGBV.
- Increased reliance on digital platforms during these crises exposed more individuals, especially youth, to TFGBV.
- Social media became a critical space for both political mobilization and the dissemination of misinformation and hate speech.
- Hate content increased, targeting religious and ethnic minorities, medical professionals, and government officials.
- Muslim communities faced intense online and offline attacks following the Easter Sunday bombings and during the COVID-19 pandemic, with hate content focusing on attire, burial practices, and alleged non-compliance with regulations.
- Politically motivated groups weaponized tragedies to deepen ethnic and religious divides through social media.
- The economic collapse has driven unemployed youth to exploit social media for income, sometimes through unethical or violent means, often funded by politicians and extremist groups to create hate content targeting minorities.
- Mainstream media outlets have amplified hate content on their social media channels, often without adequate regulation.
- Media institutions are deeply implicated in producing and amplifying hate speech and online violence, often reinforcing social hierarchies and marginalizing vulnerable communities. Private media outlets often publish sensationalized or fabricated stories, sometimes exposing survivors' identities without consent.

2 The non-violent Peoples' protest movement in Sri Lanka in 2022. https://www.cpalanka.org/wp-content/uploads/2023/12/A-Brief-Analysis-of-the-Aragalaya_Final-Report_FINAL_N3.pdf

- Social media platforms reward inflammatory content with higher visibility and monetization, making hate speech profitable.

4. Systemic Deficiencies in Prevention and Response

- Sri Lanka's legal landscape is inadequately equipped to address the complexities of TFGBV, with definitional gaps and archaic laws.
- The Online Safety Act (OSA) No. 9 of 2024 has garnered criticism for potentially infringing on human rights, with 45 per cent of respondents believing it will curb freedom of expression.
- Institutional and operational limitations include a lack of specialized expertise in law enforcement regarding technical expertise, digital forensics, and gender sensitivity for handling TFGBV complaints.
- Judicial processes are slow, leading survivors to abandon cases due to prolonged trauma and fear of re-victimization. Low conviction rates further discourage reporting.
- Challenges in addressing complaints include Meta's reliance on Google Translate for Sinhala/Tamil, which often misses important context and nuances.
- Meta's and X's relaxation of rules related to hate speech and abuse, particularly concerning sexual orientation and gender identity, is a significant concern given these groups are key targets of hateful content with real-life consequences.
- The Cyber Crimes Investigations Division (CCID) operates in only five districts, leaving large parts of the country without direct access to specialized cybercrime units.
- Survivors reported authorities being ineffective in taking necessary actions; 39 per cent were afraid to go to the police, and 41 per cent feared personal information being shared.
- Lack of access to gender-sensitive legal aid, psychosocial services, and safe reporting channels, particularly for rural and marginalized communities, contributes to underreporting.
- Awareness and utilization of counselling services among survivors are extremely low (5.7 per cent).
- There is no central and secure data management system for complaints and incidents, leading to duplication and a severe lack of centralized data, hindering effective response and policymaking.

- Social media platforms lack accountability for failing to moderate hate content in Sinhala and Tamil, and their reporting mechanisms are often lengthy, technical, and complicated.
- Awareness of non-state actors (e.g., Hashtag Generation, Hithawathi) with "trusted partner" status for faster content removal is low among the general public.
- Gaps in digital literacy heighten vulnerabilities and contribute to the normalization of online abuse and the proliferation of TFGBV.

Key Recommendations

The study emphasizes an urgent shift towards a proactive prevention and response framework for TFGBV, advocating for a comprehensive, multi-sectoral approach that transcends traditional methods of addressing gender-based violence. Prevention efforts should be sustained and long-term, aiming to shift social norms, attitudes, and beliefs that legitimize inequality and violence. This involves interventions at various levels:

- **Individual Level:** Promote digital literacy, consent education, and resilience, especially among women, girls, and marginalized communities vulnerable to online harm.
- **Relationship Level:** Foster respectful online communication, challenge power dynamics, and support healthy digital boundaries, particularly within intimate relationships.
- **Community Level:** Transform schools, workplaces, and digital spaces into safe, inclusive environments with clear protocols for reporting and responding to TFGBV.
- **Societal Level:** Implement broader structural changes, including the enforcement of gender-equitable laws, greater accountability for digital platforms, and media reforms that counter misogynistic, racist, and homophobic narratives.

The study also calls for continued learning through sustained investment in monitoring and evaluating prevention and response efforts to inform future strategies. Applying the RESPECT Violence Prevention Framework, which focuses on Relationship skills strengthened, Empowerment of women, Services ensured, Poverty reduced, Environments made safe, Child and adolescent abuse prevented, and Transformed attitudes, beliefs, and norms, is recommended for a holistic and multi-level approach to TFGBV prevention.

01

INTRODUCTION

1.1. Background

The revolutionary advancements in technology and the rise of online communication platforms have significantly increased both the quantity and diversity of digital interactions, leading to a surge in users and a broadening of cyberspace. Over the past two decades, these platforms have served as vital spaces for communication and the free, seamless exchange of ideas and opinions. Digital spaces and information technology undoubtedly offer powerful tools for women's empowerment, providing increased access to education, employment, social connections, and essential services. However, while technology and digitalization present immense opportunities, they also create avenues for harm and misuse. The tone of online communication has increasingly become hostile and hateful, often leading to emotional harm, virtual violence, and even real-world consequences. Internet platforms have, at times, become breeding grounds for the promotion of discriminatory ideologies under the guise of protecting democracy, human rights, and peace. With the widespread use of social media, cyber gender-based violence, girls, LGBTQIA+ persons, and ethnic minorities has become as pervasive as physical violence in the real world. Furthermore, internet accessibility is often gendered, with men typically enjoying greater access than women. Whether online or offline, harmful communication undermines human dignity, restricts freedom, and negatively impacts the overall well-being of individuals and communities.

According to research, at least 38 per cent of women worldwide have experienced online violence.[3] This percentage began rising at a much faster pace during the COVID-19 pandemic, as women's lives increasingly shifted online for work, education, access to services, and social interaction. It has been recognized that various forms of violence are facilitated by technology and disproportionately perpetrated against girls, women, LGBTQIA+ persons, and ethnic minorities. These attacks often occur on an intersectional basis, influenced by race, ethnicity, age, sexual orientation, religion, gender identity, and expression, socioeconomic status, caste, and disability.[4] Certain groups of women are especially vulnerable due to their actions, identities, or use of technology. These include young girls, women politicians, activists, journalists, and feminists. TFGBV can be perpetrated by individuals, groups, or even anonymous users on social media platforms with whom the survivors may have no prior connection.

Those with intersecting marginalized identities, such as LGBTQIA+ individuals and members of religious and ethnic minorities are more likely to become targets of hate content. With the rapid evolution and widespread use of technology and digital spaces, online platforms are increasingly being exploited to harm individuals and communities. In recent years, technology has enabled new and more intense forms of gender-based violence, posing serious threats both online and in the real world. The growing prevalence of TFGBV experienced by women, girls, LGBTQIA+ persons, and ethnic minorities is deeply concerning,

3 https://rutgers.international/wp-content/uploads/2024/06/Decoding-TFGBV-Report-2024.pdf
4 https://www.unwomen.org/sites/default/files/2023-04/Technology-facilitated-violence-against-women-Taking-stock-of-evidence-and-data-collection-en.pdf

as online environments are becoming increasingly unsafe and hostile.[5]

TFGBV can take many forms and may be categorized based on the perpetrator's behaviour, the methods used to abuse the survivor, the nature of their relationship with the survivor, and the technology employed. Common forms include online harassment and abuse, non-consensual sharing of intimate images, cyberstalking, image-based sexual abuse, doxxing, technology-facilitated sexual abuse, targeted hacking, and hate speech. These acts of violence may occur as isolated incidents, repeatedly over time, or simultaneously alongside other forms of TFGBV.[6]

TFGBV is often directly linked to offline violence, and survivors frequently alter how they use digital technologies due to the associated risks. TFGBV exacerbates the gender digital divide and hinders large segments of groups of women and girls from fully enjoying the potential benefits of technology. Furthermore, it contributes to the discouragement and withdrawal of women from online public spaces and restricts their access to critical information and services.[7]

As the prevalence of TFGBV continues to rise rapidly in online spaces, evidence shows that women and girls are targeted primarily due to their sexual and gender identities.[8] They are likely to experience severe and long-lasting physical and psychological consequences because of hate content. Some countries, including Australia, the United Kingdom, the United States of America, Canada, and New Zealand, have introduced legal and policy measures to address the issues and mitigate impacts.[9]

To design effective responses and preventive strategies for TFGBV, it is crucial to understand its scale, context-specific dynamics, and to collect more evidence on interventions that are proven to work. Survivors of sexualized forms of TFGBV often face shame, blame, and reputational damage, negatively impacting many aspects of their social and professional lives, particularly for women who depend on online spaces for their careers.

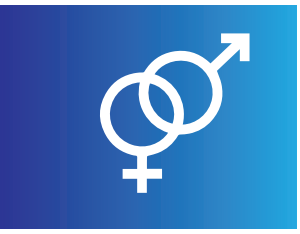
Addressing TFGBV is a global priority and can no longer be considered optional. For women to fully exercise their right to freedom of expression, it is essential that all individuals can participate online without fear of violence or harassment. Technology and digital platforms should serve as tools for advancing women's empowerment and accelerating progress toward gender equality.

Research studies have found that the implementation of effective response and prevention programs is often hindered by significant knowledge gaps and the absence of comparable, reliable data on the prevalence, forms, impacts, and drivers of TFGBV across different regions and social contexts. Prevention and response efforts require collective commitment of governments, technology companies, civil society organizations, gender-based violence service providers, researchers, and survivors of TFGBV.

5 https://eca.unwomen.org/sites/default/files/2024-01/research-tf-vaw_full-report_24-january2.pdf
6 https://eca.unwomen.org/sites/default/files/2024-01/research-tf-vaw_full-report_24-january2.pdf
7 https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women#:~:text=Violence%20and%20abuse%20online%20may%20limit%20women's,participation%20in%20political%2C%20social%20and%20cultural%20life.
8 https://www.unwomen.org/sites/default/files/2023-04/Technology-facilitated-violence-against-women-Taking-stock-of-evidence-and-data-collection-en.pdf
9 https://www.unfpa.org/sites/default/files/resource-pdf/Summary%20for%20Laws%20and%20Policies%20-%20Rights-based%20Regulation.pdf

1.2. Defining TFGBV

This study uses the term TFGBV and highlights the need for a globally accepted and standardized definition. A shared understanding is crucial to enable consistent measurement and to establish minimum standards for prevention and response efforts. After reviewing various definitions and concepts published in recent years by international organizations, academics, and civil society organizations, UNFPA has proposed a new operational definition of TFGBV, which is as follows:



An act of violence perpetrated by one or more individuals that is committed, assisted, aggravated, and amplified in part or fully using information or communication technologies or digital media, against a person based on their gender.[10]

The above definition is inclusive of violence that occurs in online spaces and of violence perpetrated through technological means, but which would not necessarily be thought of as "online violence".

TFGBV encompasses a wide range of harmful behaviours, including sextortion (blackmail involving threats to publish sexual information, photos, or videos); image-based abuse (sharing intimate photos without consent); doxxing (publishing private personal information); cyberbullying; online gender-based and sexual harassment; cyberstalking; online grooming for sexual assault; hacking; hate speech; online impersonation; and the use of technology to track and locate survivors in order to inflict further harm, among others.[11]

It is important to note that TFGBV extends beyond online violence. While it frequently occurs in digital spaces, it is facilitated through various forms of technology, including mobile phones, recording devices, drones, or GPS tracking tools, that may not necessarily be connected to the internet. There is often a spillover between online and offline spheres, where harassment initiated online can escalate into physical violence, and vice versa.

As this study primarily focused on gendered hate content in the context of TFGBV, the term "hate content" refers to any form of content that makes individuals or groups feel unsafe or targeted. This includes offensive, violent, harmful, misogynistic, or abusive content, and any other online material used to harass or intimidate survivors.

10 https://www.unfpa.org/sites/default/files/pub-pdf/UNFPA_Measuring%20TF%20GBV_%20A%20Discussion%20Paper_FINAL.pdf
11 https://www.unfpa.org/TFGBV

1.3. Global context

Recent research indicates that TFGBV has surged globally during the pandemic, with many nations struggling to address the violation of women's online lives due to the lack of strong legislative frameworks.[12] This issue particularly affects women and girls who face intersecting social disadvantages such as gender, race, class, caste, religion, and disability.[13] Among women, women of colour are more susceptible to online violence, while women belonging to ethnic or religious minorities, women with disabilities, and lesbian, bisexual, transgender, or intersex women face significant abuse on social media platforms.[14]

The Economist Intelligence Unit (EIU) reports that 38 per cent of women have experienced online violence personally, and 85 per cent of women who spend time online have witnessed digital violence against other women.[15] A study conducted by Plan International across 31 countries found that 58 per cent of young women and girls aged 15-25 years had experienced online harassment.[16] The COVID-19 pandemic exacerbated digital violence as women and girls increasingly moved online for work, education, and social activities. Data from India, Sri Lanka, and Malaysia showed a 168 per cent increase in the volume of misogynistic online posts during the COVID-19 lockdowns.[17] Misinformation and disinformation online are also major issues affecting girls' rights to participation, education, and freedom of expression.

TFGBV often leads to offline violence, and vice versa. A survey conducted in Malawi found that 34 per cent of women were physically harmed because of online violence, while 54 per cent of women reported physical abuse.[18] A UN Women study on gender-based violence in the online space of Arab States revealed that nearly half (49 per cent) of female internet users felt unsafe from online harassment. This sense of unsafety was more pronounced among women activists and human rights defenders (70 per cent). In fact, 16 per cent of women in the Arab States reported having experienced online violence at least once in their lifetime. Furthermore, the number of women exposed to online violence increased during the pandemic, with 60 per cent of women respondents reporting having experienced online violence in the past year.[19]

The study also found that 70 per cent of women activists and human rights defenders had received unwanted images or symbols with sexual content, 62 per cent had received insulting or hateful messages, and 58 per cent had received abusive phone calls or inappropriate communications.

TFGBV is a grave concern for women in politics, often causing women to withdraw from political engagement. Research has highlighted the negative impact of unequal gender norms within political parties on women's political participation and voice. Women's experi-

12 https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/GDC-Submission_UNFPA.pdf
13 https://unric.org/en/how-technology-facilitated-gender-based-violence-impacts-women-and-girls/
14 https://www.orfonline.org/expert-speak/the-great-gender-glitch
15 https://onlineviolencewomen.eiu.com/
16 Plan International (2020). Free to Be Online? Girls' and young women's experiences of online harassment
17 https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/tech-facilitated-gender-based-violence
18 https://africaninternetrights.org/en/updates/tackling-gender-based-cyber-violence-against-women-and-girls-malawi-amidst-covid-19-pandemic
19 https://arabstates.unwomen.org/en/digital-library/publications/2021/11/violence-against-women-in-the-online-space

ences of political disempowerment are heavily influenced by social norms, with barriers to participation being compounded by factors such as religious identity, ethnicity, caste, class, age, sexuality, and disability.[20]

Many studies note that the prevalence of TFGBV cannot be accurately estimated due to various limitations such as underreporting, poor reporting mechanisms, and a lack of understanding of what constitutes technology-facilitated GBV. Findings also suggest that the prevalence of TFGBV varies depending on the form or behaviour of the abuse, as well as the characteristics of both the survivor and the perpetrator.[21]

1.4. Sri Lankan context

Trends in internet and social media use in Sri Lanka

During the past 6 years, internet usage has doubled from 6.7 million users in 2018 to 12.34 million users in 2024 in Sri Lanka. During the same period, the internet penetration increased from 32 per cent to 56.3 per cent. Similarly, there were 7.5 million active social media user identities in 2024, compared to 6.0 million in 2018, corresponding to 34.2 per cent and 29 per cent respectively, of the total population. The COVID-19 pandemic was one reason for the rise in social media platforms and internet usage in the nation.

The COVID-19 pandemic contributed to a rise in social media platforms and internet usage in the nation. The number of internet users in Sri Lanka increased by 4.1 per cent between 2019 and 2020. Following the COVID-19 pandemic, all public and private educational institutions including private tuition service providers commenced their education programmes using online learning platforms. This marked a significant change in the way people throughout the nation used the internet and social media platforms. The trend was also facilitated by the increased access to and use of smartphones, tablets and laptops and comparatively cheap internet facilities. Social media overtook the use of mainstream printed media and provided a low risk, easily accessible, user-friendly and high impact platform to spread hate content.

Rise of TFGBV and targeted group

Over the past five years, Sri Lanka has witnessed the destructive impacts of hate content both online and offline. Increasingly, individuals are using digital platforms to express and disseminate harmful and violent material. As a result, hate content is rapidly shifting into virtual spaces, and TFGBV has emerged as one of the most significant forms of violence in the digital realm. The spread of hate content has disproportionately affected women, girls, and individuals from sexual and ethnic minority groups. According to UN data on Sri Lanka, 51 per cent of harmful online content targets women, while 24 per cent is directed at minority communities.[23]

20 https://www.alignplatform.org/resources/too-young-too-old-too-emotional-how-gender-norms-hold-women-back-local-politics
21 https://journals.sagepub.com/doi/full/10.1177/15248380231154614#body-ref-bibr31-15248380231154614-2
22 https://datareportal.com/digital-in-sri-lanka
23 https://srilanka.un.org/en/265414-safeguarding-democracy-combatting-hate-speech-and-disinformation

The number of complaints received by both government and private sector institutions indicates a significant rise in TFGBV over the past five years. Reported incidents to the Sri Lanka Computer Emergency Readiness Team (SLCERT) increased from 2,969 in 2019 to 20,219 in 2023.[24] During the first nine months of 2024, SLCERT received 17,058 cyber-related complaints, of which 12,712 were related to TFGBV. These included cases such as the creation of fake accounts, hacking of social media profiles, dissemination of abusive content, sexual harassment, and the spread of false information. Of the total online violence complaints received by SLCERT, 7,356 or 58 per cent were reported by girls and women. However, it is widely understood that the actual number of cases is likely much higher, as many women choose not to report such incidents due to barriers including social stigma, fear of retaliation, and a lack of trust in law enforcement and the justice system. According to SLCERT data for 2024, the highest number of complaints originated from the Colombo District (31.3 per cent), followed by Galle (16.5 per cent), Kalutara (4.8 per cent), Kandy (4.6 per cent), and Kurunegala (4.6 per cent).

Research conducted by Hashtag Generation reveals that approximately 53.5 per cent of TFGBV was directed at women, particularly women politicians and activists. The LGBTQIA+ community also faced a significant proportion of TFGBV, accounting for 7 per cent of the reported incidents. Politicians were heavily targeted during the Aragalaya period, with 47 per cent of the incidents involving elements of gender-based harassment or hate content specifically directed at them. Additionally, TFGBV targeting activists and celebrities accounted for 21.3 per cent and 13.5 per cent of incidents, respectively.[25]

Sri Lanka has a growing LGBTQIA+ community that is increasingly becoming a target of hate content and other forms of TFGBV, both online and offline.[26] The violence directed at LGBTQIA+ individuals has deeply impacted their sense of identity and belonging, and they frequently face stigma and discrimination in their daily lives. Cultural and social prejudices have contributed to their continued exclusion and lack of acceptance within the mainstream Sri Lankan society.

Political ideologies are also a common target of hate speech in Sri Lanka. Nearly all Sri Lankan female politicians have been subjected to hate content on social media. The widespread dissemination of such content significantly impacts women's participation in active politics. Despite women's active involvement in the workforce and their contributions to economic development, their near absence from political leadership remained strikingly apparent until the most recent parliamentary elections. This underrepresentation is largely attributed to a combination of limited opportunities, personal reluctance, and a widespread fear of being subjected to verbal abuse and harassment fuelled by misogyny at a national level.[27]

24 https://cert.gov.lk/wp-content/uploads/2024/03/NCSS-Draft-V14.pdf
25 https://drive.google.com/file/d/1lQmfSOCsegCuympxRZk7pZCUbyPj6fz6/view
26 https://www.wfd.org/sites/default/files/2022-02/Summary-Book.pdf
27 https://beta.parliament.lk/en/learn/women-in-parliament/news/details/45

According to respondents, during the "Gota Go Home"[28] campaign, women were specifically targeted with misogynistic and sexist comments. However, such posts and remarks received limited attention, as public focus was largely directed toward politicians. Women's rights activists, female politicians, celebrities, and professionals who played active roles in the Aragalaya movement were subjected to various forms of hate content, often linked to their intersectional identities. The attacks primarily focused on their political affiliations, physical appearance, religion, profession, and educational background. Platforms such as Facebook and YouTube were widely used to disseminate misogynistic content, including heavily derogatory gendered slurs, doctored images, fake photos, and memes.

Based on recent research findings, the Hashtag Generation's team of social media analysts identified that 25 per cent of all hateful content on social media platforms in Sri Lanka in 2021 targeted women. Furthermore, discriminatory expressions rooted in misogyny represented the second-highest category recorded that year, accounting for 65 per cent of the content. The study also noted that during the Aragalaya period in 2022, 60.3 per cent of TFGBV incidents targeted women, particularly activists and female politicians involved in the protests. Additionally, nearly 30 per cent of TFGBV content consisted of gendered hate speech directed at women, the LGBTQIA+ community, and gender-diverse individuals. The study further emphasized that TFGBV is not solely a women's issue—it is an intersectional issue. Therefore, it is essential to consider the intersecting identities of both victims and perpetrators when addressing TFGBV.[29]

The rapid context assessment on young people countering hate content on social media, conducted by Search for Common Ground Sri Lanka, found that hate content creators often use memes, Facebook stories, and short videos that are particularly appealing to younger audiences. Racism and religious hatred emerged as key themes through which youth propagate hate content on social media platforms. The study further revealed that the Muslim community has been the primary target of much of this online hate content. However, other groups—including human rights activists, politicians, religious leaders promoting interfaith harmony, law enforcement personnel, international human rights organizations, women, the LGBTQIA+ community, and citizens who do not align with the hardline Sinhalese Buddhist agenda—have been subjected to online attacks.[30]

Legal framework and gaps

Sri Lanka has several laws and regulations enforced by various institutions to combat hate content. A detailed list of these laws, including relevant sections, is provided in Annexure I. However, recent research documents[31] have identified several criticisms of the existing legal framework:

- **Obscene Publications Ordinance No. 4 of 1972** does not clearly define what constitutes an "obscene" matter or thing. The term "obscene," often interpreted as "indecent," is subjective and left to the discretion of the presiding judge to deter-

28 A series of mass public protests against the government of Sri Lanka in the year 2022
29 https://drive.google.com/file/d/1lQmfSOCsegCuympxRZk7pZCUbyPj6fz6/view
30 https://documents.sfcg.org/wp-content/uploads/2020/05/SFCG-SRI_Lanka_Rapid_Conflict_Assessment_on_Hate_Speech_2019.pdf
31 https://www.sfcg.org/wp-content/uploads/2023/11/CitW_Gap_Analysis_2023_SFCG.pdf

mine whether a particular photograph or video qualifies as such. The Ordinance has not been amended since 2005, and its provisions do not adequately reflect technological advancements or current digital realities.

- **Sections 285 and 286 of the Penal Code Ordinance No. 2 of 1883** are limited to the possession of obscene books, pamphlets, papers, drawings, paintings, photographs, representations, or figures for the purpose of sale, distribution, or public exhibition. However, these sections do not address graphics, videos, or live streams, especially those that may disappear after a set time.

- **The Personal Data Protection Act No. 9 of 2022** applies to data processors and controllers but not to individuals. This creates a legal gap concerning offences such as doxxing. For instance, if an individual publicly shares the phone number of a young girl without her consent, the current law may not adequately address or penalize the act.

- **Online Safety Act No. 9 of 2024** aimed at strengthening the legal framework to combat violent content online, has faced criticism from legal professionals and civil society. Critics argue that several provisions could undermine human rights and fundamental freedoms, including freedom of information and expression.[32] Moreover, experts note that gaps in the law may only become apparent once it is fully implemented. While many legal provisions, policies, and institutions exist, they fail to comprehensively address the full spectrum of TFGBV or the diverse identities of victim-survivors, such as LGBTQIA+ persons.[33]

Overall, the current legal framework contains several ambiguities and lacks clear definitions or judicial interpretation specific to TFGBV. This opens the door for misapplication or selective enforcement of the law. According to legal experts, Sri Lanka's legal system is insufficiently equipped to address TFGBV comprehensively. Interpretation challenges arise from varying perceptions of what constitutes specific offences, and in many instances, crimes overlap, complicating the legal classification and prosecution of TFGBV cases.

Government institutional mechanism for response/reporting

Government institutions such as the National Child Protection Authority (NCPA) and the Sri Lanka Computer Emergency Readiness Team (SLCERT) have established online complaint facilities for victims, supported by a 12-hour hotline service available in all three national languages. Recognising the urgency of combating child abuse in cyberspace, the NCPA, in collaboration with the Internet Watch Foundation (IWF), a global leader in internet child safety enforcement, launched an online reporting platform. This initiative is financially supported by Save the Children and ChildFund. Through this system, online complaints related to child sexual abuse are processed by the IWF, which works closely with the NCPA to identify, track, and remove abusive videos and images from the internet. Once detected,

32 https://www.icj.org/sri-lanka-proposed-online-safety-bill-would-be-an-assault-on-freedom-of-expression-opinion-and-information/
33 https://ohrh.law.ox.ac.uk/gendered-dimensions-a-critical-look-at-the-online-safety-act-of-sri-lanka/

the offending content is promptly removed, and legal proceedings are initiated against the perpetrators.[34]

In addition, SLCERT conducts online training sessions to educate individuals and organizations on the risks associated with online violence and the responsible use of social media. Training materials are regularly updated, and refresher courses are provided to ensure users remain informed about emerging cyber threats and best practices. SLCERT also offers clear guidelines for reporting suspected security incidents or vulnerabilities.[35] These capacity-building programmes play a crucial role in addressing the human factor in cybersecurity and fostering a safer digital environment.

Addressing gaps to prevent and eliminate TFGBV

To effectively address the above challenges, it is imperative to formulate comprehensive laws, policies, and action plans that consider the identified gaps. Regular monitoring and annual reviews of these laws and policies, having in active collaboration with non-state organizations in Sri Lanka are essential. Survivors seeking legal assistance often encounter issues such as lack of understanding of the legal system and procedures, as well as prolonged delays in investigations. Addressing these barriers is crucial to fostering a supportive environment that encourages survivors to come forward.

A recent research study conducted in Sri Lanka[36] recommended several initiatives to prevent and eliminate TFGBV. These include:

- Introducing online and social media safety into the school curriculum, supported by up-to-date tools and increased technology-based education for children;
- Enhancing rights-based education and awareness to reduce GBV and violence against minorities;
- Improving the effectiveness of SLCERT and other government institutions in receiving and investigating complaints;
- Strengthening the police division responsible for handling issues related to social media violence;
- Promoting social media literacy among individuals and youth to encourage positive online engagement, counter hate speech, and report online anti-social behaviour;
- Developing support programmes in collaboration with stakeholders to assist victims of social media violence in overcoming trauma;
- Providing platforms for victims to voice their concerns directly to social media companies and government authorities.

34 https://www.adaderana.lk/news/98277/new-online-reporting-system-launched-for-child-sexual-abuse-complaints
35 https://www.cert.gov.lk/resources
36 https://www.britishcouncil.lk/sites/default/files/youth_social_media_and_violence_research_report_compressed.pdf

02

THE STUDY

2.1. Introduction

This exploratory study was commissioned in 2024 by the United Nations Population Fund and UN Women Sri Lanka. It focuses on the occurrence and various forms of TFGBV experienced by women, girls, LGBTQIA+ individuals, and ethnic minorities, exploring the motivations behind its proliferation and emerging trends.

The findings and recommendations presented in this report are intended to serve as a launching pad for broader future inquiries into TFGBV and its impacts both online and offline. This report offers valuable insights and provides a foundation for enhancing strategies, programmes, and policies aimed at prevention and response.

2.2. Objectives and scope of the study

The overall objective of this study is to understand the prevalence and forms of TFGBV faced by women, girls, LGBTQIA+ individuals, and ethnic minorities in Sri Lanka, including the motivations behind its proliferation and the emerging trends and undertones it takes. The findings are expected to offer valuable insights to inform and enhance future strategies, programmes, and policies addressing this issue.

To analyse the dynamics of hate content related to TFGBV in Sri Lanka over the past four years, several key areas were identified for exploration:

- Gauging the prevalence of hate content, identifying the primary targets and recipients, understanding who is more likely to be affected, the extent to which they have been directly targeted, and their level of awareness regarding such content.
- Examining the types of content, identifying the main creators and instigators, and exploring their stated motivations for targeting specific gender, sexual, and ethnic minority groups.
- Investigating the offline impacts of TFGBV, including the various forms it takes, the severity of these offline actions, changes in occurrence over time, and any connections to significant national events.
- Reviewing existing interventions addressing TFGBV against women, girls, LGBTQIA+ individuals, and ethnic minorities to identify gaps and provide recommendations for more effective responses.

These objectives guided the comprehensive analysis of TFGBV in Sri Lanka and served as the basis for developing targeted strategies for the prevention of and response to TFGBV.

2.3. Research questions

The study was designed to explore the following key questions:

- What are the various forms of TFGBV observed in Sri Lanka, and have these forms evolved over time?
- Who are the primary targets, recipients, and audiences of this hate content, and which groups are more likely to experience it?
- To what extent have these groups been directly exposed to TFGBV, and how aware are they of such content being shared?
- What types of content gain the most traction, and why? Through which platforms is this content shared, and who engages with it?
- Who are the main creators and instigators of this hate content, and what are their stated motivations?
- Why are specific gender groups and minorities particularly targeted by this content?
- Does online violent content lead to offline consequences or actions? If so, in what forms do these manifests?
- Has the dissemination of hate content changed over time, and are these changes linked to specific key events in the country?
- What interventions have been implemented or are currently underway to address TFGBV in Sri Lanka?
- What are the existing gaps in programming, and what actionable recommendations can be made to strengthen TFGBV prevention and response efforts in Sri Lanka?

2.4. Conceptual framework

Using UNFPA's definition of TFGBV, this study focused on analysing disaggregated data based on gender, sexuality, and ethnic identity. The primary emphasis was on online hate content experienced by women, girls, and gender and sexual minorities. Accordingly, the study considered any form of communication; verbal, written, or behavioural that is hostile or uses derogatory or discriminatory language against women, girls, LGBTQIA+ persons, and ethnic minorities based on religion, ethnic origin, nationality, race, skin colour, social origin, gender, or other identity factors.

Technology has significantly altered both the context and severity of targeting, enabling the rapid dissemination of violent content through social media platforms and other digital spaces. This study focused on TFGBV, wherein technology and digital platforms have facilitated new avenues for the perpetration of gender-based violence. The forms of TFGBV explored include the circulation of obscene text messages and videos, doctored images and videos, unauthorized disclosure of personal information, cyber blackmail, creation of fake profiles, data breaches, threats, harassment, and various forms of verbal abuse.

Additionally, the study investigated the offline impacts and severity of TFGBV. TFGBV is an escalating phenomenon with potential to cause serious physical, sexual, psychological, social, political, or economic harm, as well as violations of rights and freedoms. Online violence can lead to offline physical violence and, conversely, offline violence can continue in digital spaces. Online abuse often exacerbates offline gender-based violence such as stalking, sexual harassment, and intimate partner violence. In some cases, perpetrators use content shared online, such as intimate images and videos, to blackmail survivors for money or sexual favours, which may escalate into direct physical violence.

The study also examined how different gender identities, sexual orientations, and ethnic or religious identities influence the risk and experience of TFGBV. Such an intersectional analysis was vital for understanding the nexus between violent extremism and TFGBV, particularly given the increased vulnerability of religious and political minorities in the wake of recent socio-political events. Although the study faced data limitations that prevented a fully comprehensive intersectional analysis, every effort was made to interpret disaggregated data through an intersectional lens where possible.

2.5. Methodology and approach

The methodology for this study was developed in close consultation with UNFPA and UN Women to gain a comprehensive understanding of the nature of TFGBV experienced by women, girls, LGBTQIA+ persons, and ethnic minorities in Sri Lanka. The study aimed to generate evidence-based recommendations to inform the design of strategies for the prevention of and response to TFGBV.

A mixed-methods approach was adopted to effectively address the study's objectives and research questions. This approach combined both quantitative and qualitative data collection techniques to ensure a holistic analysis. The following tools were used for data collection:

- Questionnaire Survey (QS): Designed to capture quantitative data on the prevalence, trends, and demographic characteristics associated with TFGBV.
- Key Informant Interviews (KIIs): Conducted with experts and stakeholders to gather in-depth insights into the nature, causes, and consequences of TFGBV, as

well as gaps in current responses.

- Focus Group Discussions (FGDs): Facilitated among affected groups to explore lived experiences and understand the socio-cultural dynamics influencing TFGBV.
- Extraction of Data from an Online Tracking System (OTS): A dedicated tool developed to monitor and extract data on online hate content and incidents of TFGBV. The design and methodology of the OTS are detailed in Annexure II of this report.

The quantitative component, led by the questionnaire survey, enabled the measurement of trends and patterns, while the qualitative methods enriched the findings with context, experiences, and nuanced perspectives. Together, these approaches contributed to a comprehensive understanding of TFGBV and laid the groundwork for actionable recommendations.

2.6. Study districts

The study was conducted across five districts in Sri Lanka: Colombo, Kandy, Ampara, Jaffna, and Galle. The selection of these districts was based on a combination of strategic factors, including demographic and ethnic diversity, histories of conflict and war, levels of social media usage, the volume of TFGBV-related complaints reported, and documented offline impacts of TFGBV. This selection ensured a comprehensive representation of diverse socio-political and cultural contexts across the country, enhancing the relevance and applicability of the study's findings.

2.7. Quantitative data collection and the demographics

Questionnaire Survey

For the quantitative data collection, a total of 361 individuals were interviewed. This sample size reflects an increase from the originally proposed 300 respondents to ensure better representation across gender, ethnicity, and religion, supporting robust disaggregated data analysis. The sample was determined using a 95 per cent confidence level, allowing for a high degree of generalizability of the study's findings.

A stratified random sampling method was used to select respondents from the above-mentioned five districts. The allocation of the sample across districts was proportionate to the size of the female population in each area. Respondents represented a diverse cross-section of ethnic, religious, age, educational, and professional backgrounds, including school leavers, university students, factory workers, LGBTQIA+ persons, and religious and ethnic minorities.

The questionnaire consisted of 58 core questions applicable to all participants and an additional 20 questions specifically designed for TFGBV survivors. It was administered in Sinhala and Tamil, based on respondents' language preference. While the general sample was selected through stratified random sampling, a purposive sampling method was adopted to recruit TFGBV survivors for interviewing to capture their specific experiences for the study.

Figure 1 below presents the socio-demographic profile of the study participants.

Figure 1: Socio-demographic profile of the respondents of the study

Ethnicity	Sinhala	Tamil	Muslim
No. of Respondents	190	90	81
Percentage (%)	53%	25%	22%

Gender Identity	Woman	Man	LGBTQIA+
No. of Respondents	221	85	55
Percentage (%)	61%	24%	15%

Survey District	Colombo	Kandy	Jaffna	Ampara	Galle
No. of Respondents	129	77	53	52	50
Percentage (%)	36%	21%	15%	14%	14%

Age	18 - 24	25 - 29	30 - 35	36 - 45	46 - 59
No. of Respondents	153	93	54	40	21
Percentage (%)	42%	26%	15%	11%	6%

Religion	Buddhism	Islam	Hinduism	Christianity	Catholicism
No. of Respondents	133	82	60	48	38
Percentage (%)	37%	23%	17%	13%	11%

Respondents Category	University Students	Factory Workers	School Leavers	LGBTQIA+ Persons	Persons with Disabilities	TFGBV Survivors
No. of Respondents	87	94	78	55	24	15
Percentage (%)	24%	26%	24%	15%	7%	4%

Level of Education	Grade 1 - 10	GCE O/L	GCE A/L	Diploma	Under graduate	Graduate
No. of Respondents	16	80	116	31	88	30
Percentage (%)	4%	22%	32%	9%	24%	8%

The sample had 68 per cent respondents aged 18 to 29 years. The next highest group (32 per cent) aged 30 to 60 years. The study intentionally focused on individuals aged 16 to 30 years considering the literature review finding that over 70 per cent of recent online violence complaints reported to government and private institutions originated from this age cohort.

The questionnaire was administered to 103 survivors of TFGBV. Of these, 15 survivors (4 per cent of the total sample) were selected through purposive sampling, while the remaining individuals disclosed their experiences of TFGBV during the survey.

Development of online hate content tracking system and Data extraction

To better understand the proliferation of hate content online, the platforms used, and the evolving trends, the study developed a custom online tracking system. This system was designed to collect and analyse data from various social media platforms in three languages, enabling the identification of different forms of gender-targeted hate content and their trajectories across digital spaces.

The software efficiently extracts data from platforms such as Google, Facebook, YouTube (including YouTube Shorts), and X.com (formerly known as Twitter), with a particular focus on classifying and analysing gendered hate content. At its core, the system integrates an AI-powered classification model, combining the Cross-Lingual Language Model (XLM-R) built on RoBERTa architecture with a Bi-directional Long Short-Term Memory (BiLSTM) classifier. This hybrid model is pre-trained for cross-lingual understanding and optimized for performance across diverse datasets.

For data storage, a lightweight, portable SQLite database was used to ensure efficiency and mobility. The system also includes graph-based data visualization tools that allow for intuitive filtering and exploration. These visuals can be exported in PNG format for use in external reports and presentations. Using this system, the study extracted and manually annotated 33,161 data points from the five platforms mentioned. The model demonstrated strong performance, with:

93 per cent accuracy in detecting general hate content,
87 per cent accuracy in detecting gendered hate content,
89 per cent recall rate for general hate content, and
83 per cent recall rate for gendered hate content.

While the system successfully extracted content from public Facebook pages, YouTube, YouTube Shorts, Google, and X.com, it faced challenges with other platforms:

- Instagram and TikTok use CAPTCHA systems to verify users, which cannot be bypassed by robotic scrapers.
- WhatsApp and IMO feature end-to-end encryption, making content extraction without violating legal protocols impossible.
- Telegram requires admin access to view public group content, which cannot be granted programmatically.

The system also analysed the extracted content for intersectional targeting. It found that many hate posts/comments overlap multiple identity intersections, such as gender, ethnicity, religion, and profession. However, some gendered content lacked specific indicators linking it to other identity markers, making it difficult to classify under a distinct intersectional category. Moreover, many text-based data points did not contain enough contextual details to clearly identify whether those gendered hate content are relating to intersections such as race, age, disability, ethnicity, nationality, religion, profession, or sexist.

A detailed analysis of the tracking system's development and functionality is available in Section 3 of this report.

2.8. Qualitative data collection

Qualitative data played a crucial role in providing deeper insights into the intersections between gender and hate content in both online and offline spaces. Given the limited literature on the intersections of different forms of TFGBV in Sri Lanka, qualitative findings were essential in ensuring the study's comprehensiveness.

Key Informant Interview

The study aimed to collect in-depth information on the prevalence, forms of TFGBV, offline consequences, emerging trends, and current interventions through Key Informant Interviews (KIIs) with key stakeholders. The sample for the KIIs was drawn from a pre-identified list of relevant stakeholders, ensuring representativeness of diversity.

A total of 43 KIIs were conducted using a semi-structured interview guide, allowing for consistency while maintaining flexibility to explore relevant emerging themes. Interviewees included:

- Government officials
- Survivors of TFGBV
- Women politicians
- Civil society representatives and NGO staff
- Women's rights activists
- Journalists and media professionals
- Identified perpetrators
- Social media activists
- Members of the LGBTQIA+ community
- Other relevant professionals

Of the total interviews conducted, 16 KIIs were with government officials, providing valuable insights into institutional responses and challenges. All interviews were conducted in person by members of the research team and employing the preferred language of the interviewee (Sinhala or Tamil), ensuring both comfort and accuracy.

A detailed list of KIIs conducted is provided in Annexure III of this report.

Focus Group Discussion

A total of 11 FGDs were conducted across the selected five districts, involving 137 participants in all. The selection of FGD participants was based on identified risk factors relating to ethnic, religious, and other identity-based vulnerabilities. The discussions aimed to capture diverse lived experiences of TFGBV and understand the contextual nuances that may not be evident in survey data.

FGDs were conducted with a wide range of groups, including:

Members of the LGBTQIA+ community

Factory workers

University students

Women's societies

Officials of non-governmental organizations (NGOs)

To ensure linguistic inclusivity and participant comfort, seven FGDs were conducted in Sinhala and four in Tamil, aided by structured FGD guidelines prepared by the consultants.

The FGDs explored a broad set of themes, including:

- The different forms of TFGBV experienced by participants
- The main target groups and individuals most at risk
- The extent of exposure to TFGBV
- The types of content that gain the most attention online
- The platforms used for dissemination
- The creators and instigators of such content
- The motivations behind these attacks
- The offline consequences of online violence

These discussions provided crucial qualitative insights that enriched the study's understanding of TFGBV in Sri Lanka. The list of FGDs conducted is given in Annexure IV of this report.

2.9. Data analysis

The quantitative data collected through the questionnaire survey were analysed using the SPSS statistical software. This analysis generated frequency tables, cross-tabulations, and descriptive statistics for each survey question, offering a comprehensive understanding of the prevalence, trends, and demographic characteristics related to TFGBV.

All qualitative data collected through Key Informant Interviews (KIIs) and Focus Group Discussions (FGDs) were transcribed, translated into English, and analysed using thematic content analysis. The research team employed the QDA Miner software to code the data according to study objectives, categorising insights into thematic areas. The software then generated detailed summary reports for each theme, contributing to a nuanced understanding of the research questions.

The annotated data extracted through the online hate content tracking system were analysed to identify trends in gender-based hate content across time and platforms. This analysis focused on understanding how online hate evolves, which platforms are most used for dissemination, and how different categories of hate intersect with gender-based targeting.

Although a mixed-method approach was used to meet the study's objectives, qualitative methods played a critical role in validating and enriching the quantitative findings. Research on sexual and gender-based violence (SGBV) has consistently demonstrated the value of qualitative data in uncovering root causes, contextual dynamics, and pathways for intervention.

In this study, KIIs and FGDs captured in-depth perspectives from risk groups, ethnic and sexual minorities, survivors, service providers, policymakers, and other stakeholders. KIIs with survivors were conducted using survivor-centred research principles to sensitively explore the various forms of TFGBV and the ways in which intersecting identities such as gender, sexuality, ethnicity, and religion, shape the nature and impact of the violence experienced.

KIIs also provided context-specific insights into TFGBV and its connection to broader manifestations of SGBV in Sri Lanka. FGDs with service providers helped to understand the forms of TFGBV from a systems perspective and shed light on prevention and response efforts. FGDs conducted with ethnic and sexual minority groups offered crucial insight into the unique vulnerabilities faced due to cultural, linguistic, religious, and caste-based factors.

2.10. Ethical considerations

The study strictly adhered to ethical guidelines to ensure the safety, dignity, and confidentiality of all participants. Ethical approval for the research was obtained from the Ethics Review Committee for Social Sciences and Humanities, Faculty of Arts, University of Peradeniya. In addition, the study complied with UN Women's guidelines on "Safe Consultations with Survivors of Women and Girls", particularly when engaging with survivors of TFGBV.[37]

Prior to participation, all individuals were provided with an information sheet translated into their preferred language. This document explained the study's objectives, potential risks, confidentiality protocols, and voluntary nature of participation. Informed written consent

37 https://www.unwomen.org/sites/default/files/2022-12/Safe-consultations-with-survivors-of-violence-against-women-and-girls-en.pdf

was obtained from all participants before data collection began.

With respect to KIIs and FGDs, facilitators were trained to avoid prompting the participants to share personal experiences unless they did so voluntarily and without coercion. Special care was taken to ensure the emotional well-being and safety of participants, especially those from vulnerable groups.

All data collected during the study are treated as strictly confidential. No data have been, or will be, reused, shared, or accessed without proper authorization. Notes and recordings from KIIs and FGDs were stored securely and separately from identifying information. These recordings were used solely for the purposes of this research and were permanently destroyed upon the completion of the study to maintain participant confidentiality and data protection standards.

2.11. Study limitations

The study was conducted amidst several challenges and limitations. While these did not significantly impact the overall findings, it is important to acknowledge the constraints that may have influenced certain aspects of the research process and analysis:

1. **Exclusion of individuals under 18 years of age**
   Although it was observed during KIIs and FGDs that school-aged children are frequent users of social media and are both victims and perpetrators of TFGBV, the study did not include individuals under 18 due to ethical considerations. As a result, the specific dynamics of TFGBV among children and adolescents remain underexplored in this study.
2. **Limited representation of cultural nuances**
   The study covered districts with diverse ethnic and religious backgrounds, each with unique cultural interpretations of hate content. However, due to the sensitive nature of the topic and the ethical necessity of safeguarding participants, the study was unable to fully capture or analyse the varied cultural nuances in how hate content is perceived and experienced across different communities.
3. **Limitations in automatic data scraping**
   Data scraping was hindered on several platforms, namely Instagram, TikTok, and X.com, due to the implementation of CAPTCHA and anti-scraping measures. This necessitated manual data collection, limiting the volume and scalability of extracted data from these platforms.

4. Challenges in extracting whatsapp data

The end-to-end encryption and privacy safeguards in WhatsApp restrict access to message content, making automated or manual extraction of relevant data infeasible. Additionally, bypassing these protections would have breached ethical and legal standards. Consequently, WhatsApp data were excluded from the hate content analysis.

5. Insufficient data from X

During manual inspection, the research team found minimal gendered hate content on X relevant to the Sri Lankan context. This is consistent with usage statistics, which show only 2.2 per cent of social media users in Sri Lanka use X[38] with just 0.56 per cent being female users (as of 2024). A decline of 53 per cent in the platform's popularity between October 2023 and January 2024 [39] further impacted content availability. Moreover, the discontinuation of free access to X's API in 2023 posed additional barriers to data extraction.

6. Lack of date metadata in some platforms

Certain platforms, such as YouTube and Google search, do not consistently provide content timestamps. This made it difficult to accurately track temporal trends and patterns in hate content dissemination over time.

7. Legal and ethical constraints on private content

The study strictly adhered to ethical research standards and legal frameworks by limiting data collection to public sources. As a result, private content including posts from personal accounts was not accessed, limiting the scope of the analysis.

8. Current limitations in the machine learning model

Due to the insufficient volume of annotated positive data for several hate content categories, the classification model was limited to identifying whether content constitutes hate speech and whether it targets gender specifically. As the tracking system continues to collect data over time, and once a sufficient volume of positive examples is available, the model can be retrained to identify additional hate content categories with greater granularity.

38 https://gs.statcounter.com/social-media-stats/all/sri-lanka
39 https://datareportal.com/reports/digital-2024-sri-lanka

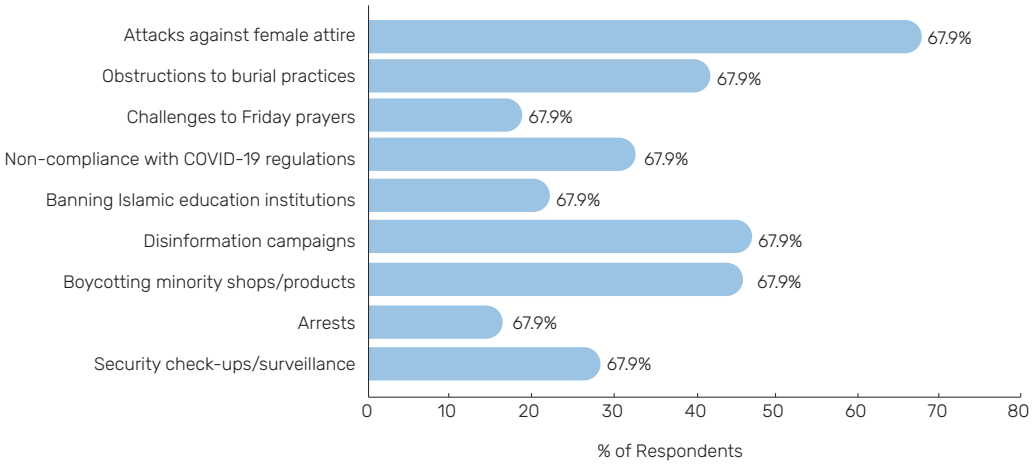
03

DATA ANALYSIS & KEY FINDINGS

3.1 The pervasiveness and evolving landscape of TFGBV

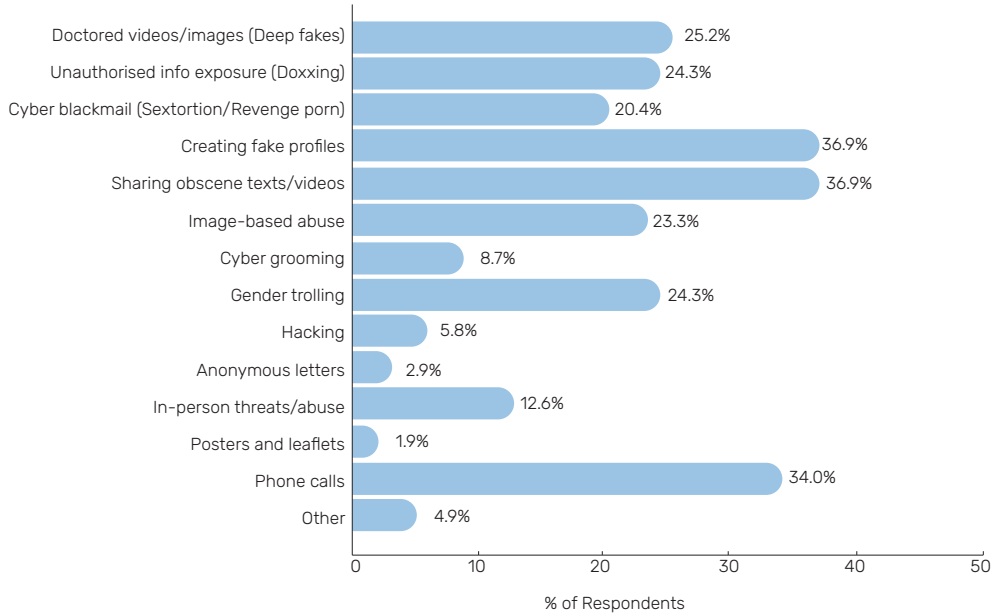
Technology-facilitated violence is a growing human rights violation that adds to the staggering rates of gender-based violence in Sri Lanka – although with limited national statistics of its prevalence. This study sets out to understand the prevalence, nature, and characteristics of TFGBV in a smaller, yet representative sample based on the women's district-wise population. With over 57 per cent of 361 study participants reporting unsafety in online spaces and 35 per cent of respondents stating to be unaware of online safety risks, this study identifies the prevalence of diverse forms of technology-facilitated violence. As such, 47 per cent of respondents stated that offensive visual content, including images, videos, cartoons, memes, objects, gestures, and symbols, contributed to a sense of feeling unsafe on social media platforms.

Figure 2: Types of online content that make respondents feel unsafe or targeted



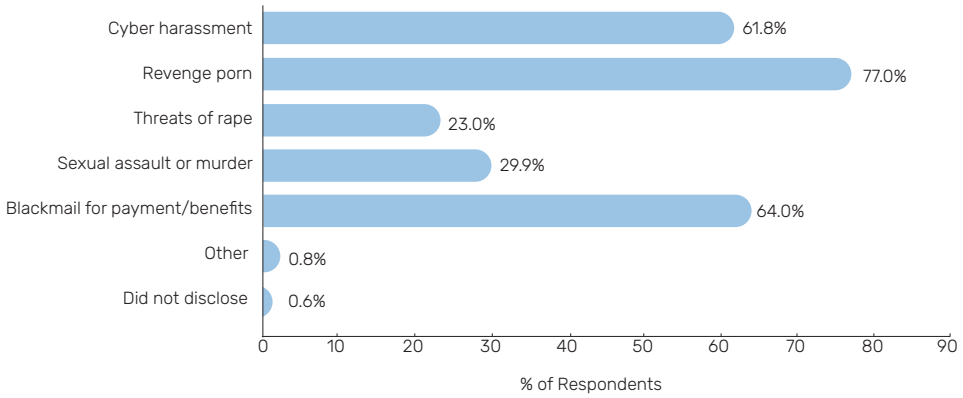
About 29 per cent of survey respondents, including the known survivors purposively selected for the sample (a share of 4 per cent), revealed that they had been survivors of TFGBV, of which 12per cent experiencing TFGBV daily or every other day. Most common abuses reported by survivors were obscene messages and videos (37per cent), creation of fake profiles (37per cent), abusive calls (34 per cent), and doctored media (25 per cent), cyber blackmail (20 per cent), and unauthorized exposure of personal information (24 per cent).

Figure 3: Forms of abuse experienced by TFGBV survivors



66 per cent of study respondents said that social media platforms with higher usage rates (as 84 per cent of survivors reported extensive daily usage of these platforms), limited violence prevention and reporting measures are sites where online violence is most experienced or witnessed. 77 per cent of survivors reported experiencing violence on Facebook and 52 per cent on WhatsApp - correlating to frequent usage of these platforms by the participants. These findings are consistent with insights from the online hate content tracking system, which identified YouTube and Facebook as platforms with the highest concentration of gendered hate content, including posts, comments, and reactions. Survey respondents identified cyber harassment (62 per cent), revenge porn (77 per cent), blackmail (64 per cent), and threats of rape/murder (23-30 per cent) constituting majority TFGBV content on social media.

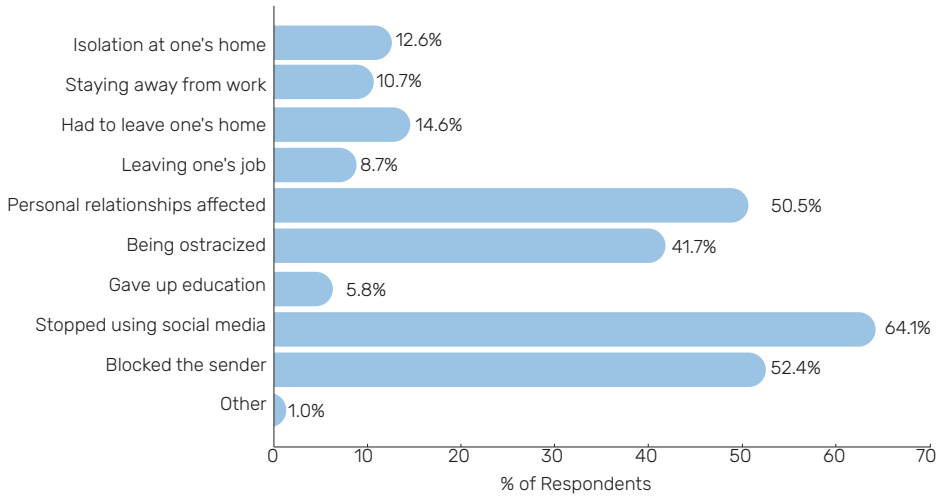
Figure 4: Forms of TFGBV content on social media



The study significantly reveals the increasingly sophisticated nature of online abuse, often leveraging advanced technologies such as AI to create deceptive and damaging content. A critical challenge identified is the inadequacy of AI content moderation tools in local languages, particularly Sinhala and Tamil, allowing harmful content to persist on widely used platforms like Facebook and YouTube. This technical gap underscores the imperative for collaboration with 'big tech' companies to develop and implement more effective, linguistically sensitive content filtering mechanisms.

Furthermore, the study confirms a strong correlation between online hate content and its offline consequences. While 92 per cent of respondents reported that TFGBV occurred mostly online, there were also offline consequences in private spheres and public spaces. 54 per cent of survivors of the study reported to have experienced offline harm – they reported experiencing offline targeting, ranging from physical violence and sexual harassment, and stigma in public spaces to reputational damage, affects to mental health including suicidal ideation, and loss of employment or professional disengagement. 64 per cent survivors withdrew from social media, 51 per cent faced relationship breakdowns, and 42 per cent faced community ostracism. 30 per cent reported economic losses due to reputational harm and job loss. Survivors of TFGBV reported copying strategies such as confrontation, reporting, digital withdrawal, relocation, identity changes, and avoidance. This necessitates a nuanced approach that addresses both digital and physical safety, recognizing that online abuse is not merely a virtual phenomenon but has tangible and severe real-world consequences for victim-survivors.

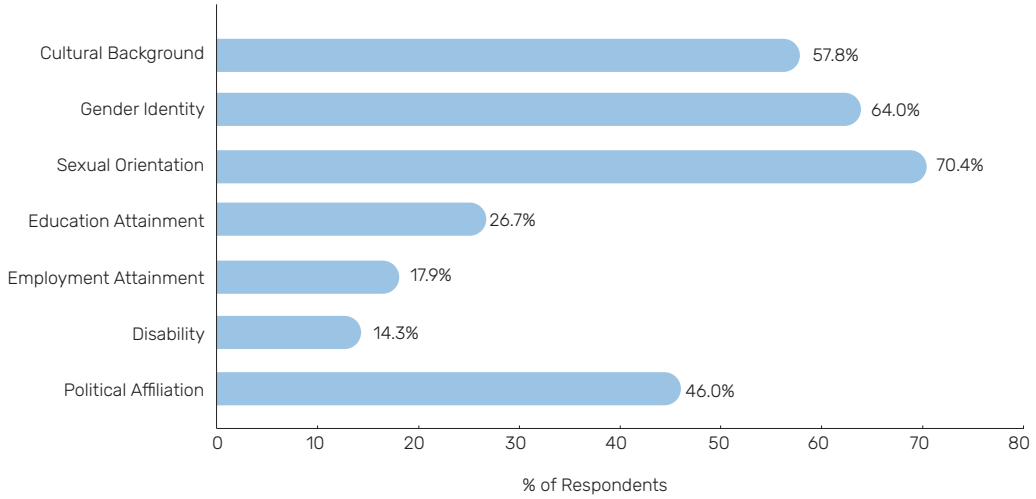
Figure 5: Offline consequences of TFGBV on survivors



3.2 Intersectional vulnerabilities and the targeting of marginalized identities

The study confirms how technology-facilitated violence is rooted in gender-inequality, patriarchy and misogyny, leading to physical, sexual, psychological, economic, or social harm in online spaces and often exacerbates prevalent forms of offline violence such as intimate partner violence and non-partner sexual harassment. A pronounced finding of the study is the intersectional nature of technology-facilitated violence in Sri Lanka, with most of the online violence was targeted against sexual orientation (70 per cent), gender identity (64 per cent), and cultural background (58 per cent) of the respondents. The findings reveal deep-rooted male dominance fueling entitlement to control and humiliate women, discriminate against minority ethnic and religious groups, and justify hate against women, LGBTIQ+ persons and minorities.

Figure 6: Factors initiating TFGBV content online and offline



90 per cent of study respondents believed social media increases the risk of gender-based violence , girls, and LGBTQIA+ individuals, with high levels of safety concerns in online spaces were reported by LGBTQIA+ respondents. When disaggregated by ethnicity, 70 per cent of Muslim respondents, 66 per cent of Sinhalese respondents, and 60 per cent of Tamil respondents acknowledged that social media contributes to violence.

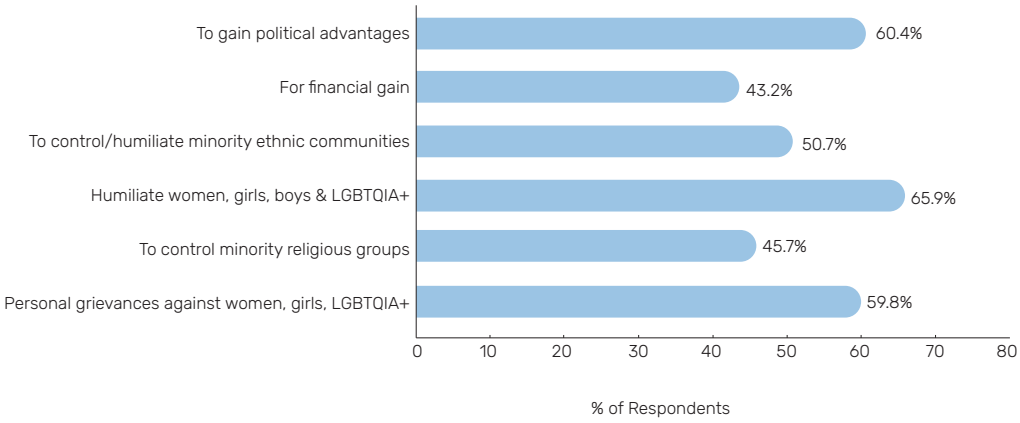
56 per cent of women and 62 per cent of LGBTQIA+ respondents reported feeling unsafe online. Ethnic disparities show that fewer than 5 per cent of Sinhala respondents feel safe, compared to 19 per cent of Tamil and 15 per cent of Muslim respondents. In terms of gender, 66 per cent of Sinhalese, 47 per cent of Muslim, and 40 per cent of Tamil women feel unsafe. Among participants who reported as survivors of online violence, 56 per cent of survivors were women, 27 per cent LGBTQIA+, and 17 per cent men. Most were under 30 years old. 50 per cent of frequent victims of TFGBV were identified to be LGBTIQ+ persons

and 9 per cent had experienced TFGBV before age 18.

An analysis of hate content in social media revealed that 39 per cent of hate content was gender related. 42 per cent of survey respondents also said that online hate content is primarily motivated against gender and 41 per cent noted sexual orientation. Amongst the motivating factors of online hate identified by the respondents were humiliation of women and LGBTQIA+ persons (66 per cent), political gain (60 per cent), ethnic/religious control (51 per cent), and personal grievances and caste-based superiority. Majority hate content was identified to be against women's appearance, attire, political views, caste, and religion; subjected LGBTIQ+ persons to slurs, blackmail, and exclusion; targeted young girls with revenge porn and exploitation, especially in school settings; as well as launched blame against marginalized groups such as migrant workers as responsible for COVID-19 spread thus subjecting to stigmatization and harassment.

39 per cent of respondents felt unsafety due to online hate content targeting identity markers. Muslim (53 per cent) and Tamil (42 per cent) respondents reported higher exposure to identity-based hate than Sinhalese (31 per cent). LGBTQIA+ individuals (53 per cent) and women (47 per cent) were especially affected by offensive imagery and discourse online. This means vulnerable groups, including women, girls, LGBTQIA+ persons, and ethnic minorities, are disproportionately experiencing violence in online spaces based on intersecting identities such as gender, sexuality, ethnicity, religion, physical appearance, and professional roles.

Figure 7: Motives behind posting violent content on social media (as reported by respondents)



Intersectional nature of TFGBV

The focus group and interview findings reveal that online harassment, discrimination, and tech-facilitated violence are deeply intertwined with the lived realities of marginalization, affecting a broad spectrum of communities—including LGBTQIA+ individuals, women, ethnic and religious minorities, youth, and workers. While the nature of abuse varies, it is often shaped by intersecting factors such as gender, class, caste, language, religion, and sexual orientation.

LGBTQIA+ individuals experience some of the most extreme forms of online abuse, including the non-consensual outing of gender identities, blackmail through dating apps, and targeted smear campaigns involving doctored photos, slurs, and threats of violence such as stoning or rape. These attacks come not only from strangers but also from former partners and are often amplified by religious or political groups seeking social media virality or financial gain. Transgender women are particularly stigmatized due to prevailing patriarchal norms, and Tamil and Muslim LGBTQIA+ people are doubly targeted through ethnically coded hate speech.

Women across regions and age groups endure normalized misogyny online. Common forms of abuse include hate speech using slurs like «baduwa» or «gediya,» sextortion, revenge porn, and fake job scams—particularly affecting single or economically vulnerable women. Women in public life, such as political leaders, activists and academics, are subjected to sexualized character attacks. Muslim women face additional layers of harassment linked to religious identity, particularly around attire like the hijab or burqa. Rural and estate-sector women, especially those from marginalized castes, are ridiculed for their speech, appearance, or perceived social status and are often blamed by family or police when targeted. Women with disabilities are mocked and vilified for defying gender and social norms, such as participating in public roles.

Ethnic and religious minorities, especially Muslims and Tamils, are frequent targets of online hate. Following the Easter Sunday attacks and the COVID-19 pandemic, Muslims were scapegoated as extremists or virus carriers, leading to digital harassment and offline discrimination—including verbal abuse in public transport and denial of basic services. Tamil and estate communities endure caste-based slurs like “parayan” or “sakkilian,” often circulated through memes, matrimonial ads, and social media posts. Muslim LGBTQIA+ individuals face marginalization from both within their religious communities and the wider public. These layered identities often restrict access to justice, education, and institutional support.

Youth and children—particularly post-COVID—are increasingly vulnerable due to widespread access to digital devices without corresponding safety education. Many fall victim to grooming, sextortion, and cyberbullying, with girls from economically disadvantaged or single-parent households being especially at risk. LGBTQIA+ youth or those who visibly defy gender norms face both online and offline harassment, often leading to trauma, educational withdrawal, or social isolation.

Factory and estate-sector workers, especially women, face a combination of digital exploitation and systemic neglect. Many report harassment through fake profiles and job scams, and some have had personal data stolen during phone repairs, which is then used for blackmail. Their reluctance to report abuse is heightened by class-based prejudice in

police stations, a lack of Tamil-language services, and fears of workplace retaliation. Estate women, in particular, experience caste, regional, and language-based exclusion, often viewed as uneducated or easily manipulated. LGBTQIA+ individuals in factory settings face the constant threat of exposure and abuse from coworkers or supervisors.

In sum, the digital landscape in Sri Lanka mirrors and amplifies offline inequalities. For marginalized groups, online spaces are not merely unsafe—they are structured by the same hierarchies of power that govern physical spaces. The intersection of caste, class, gender, ethnicity, religion, and sexuality profoundly shapes who is targeted, how they are harmed, and whether they can seek support or justice. Addressing these issues requires intersectional, rights-based approaches that prioritize safety, access, and dignity for all.

A digital divide between urban and rural sectors is visibly contributing to the level of exposure to online violence. For example, the highest number of respondents reported to be survivors (42 per cent) were from Colombo (urban), where respondents reported a higher frequency of internet usage (with 54 per cent of respondents reportedly using social media over 7 hours daily). Whereas in Ampara (rural), there were 7 per cent of respondents reported as survivors of TFGBV, and over 47 per cent of respondents noted to be using social media less than 1 hour a day. These disparities suggest that access to internet infrastructure and digital literacy may influence the frequency of usage and consequently, the risk of exposure to online violence. However, the digital divide and lower internet literacy may also contribute to a lack of awareness of TFGBV risks and reporting mechanisms, which may heighten exposure to online violence although with limited reporting of cases of violence.

Lack of awareness of online safety risks was more pronounced amongst women respondents, especially of ethnic minority groups - with 32 per cent of Muslim women, 21 per cent of Tamil women, and 15 per cent of Sinhalese women reporting unawareness of the risks associated with social media use. Moreover, Muslim and Tamil community respondents especially highlighted barriers to reporting online violence due to challenges in language, stigma, lack of awareness, and intimidation and discouragement for reporting. As such, these findings highlight how pre-existing digital divide, societal prejudices and discriminatory norms around intersectional identities are amplified within digital spaces, resulting in violence and widening inequalities.

TFGBV against the backdrop of the digital divide

Focus group and interview discussions revealed that Sri Lanka's digital divide is a multi-dimensional issue rooted not only in internet access but in deep and persistent inequalities across digital literacy, device ownership, safety knowledge, language accessibility, and institutional trust. This divide disproportionately affects women, LGBTQIA+ individuals, rural and upcountry communities, ethnic and religious minorities, workers, youth, and persons with disabilities—intensifying their exposure to online harm while limiting their ability to respond or seek support.

Participants across communities consistently highlighted a widespread lack of awareness around safe digital practices. Many users do not know how to activate two-step verification, adjust privacy settings, or report abuse on platforms. As a result, personal information is often shared publicly or carelessly, leaving individuals—especially women and youth—vulnerable to scams, phishing attacks, and impersonation. LGBTQIA+ individuals, in particular, reported frequent incidents of account hacking and identity theft, often due to unknowingly sharing one-time passwords or lacking basic digital safeguards.

Language emerged as a critical barrier, especially for Tamil-speaking and rural populations. Most online safety information, help services, and public forms are only available in Sinhala or English. Many government officials do not offer translation or support in Tamil, resulting in further marginalization of already underserved communities. This leaves large sections of the population without access to even the most basic tools for digital protection.

The digital divide is also shaped by unequal access to devices and digital education. Many factory workers, estate youth, and upcountry Tamils lack personal phones and rely on shared or borrowed devices, increasing their risk of data breaches and identity misuse. Limited digital exposure and economic desperation make these groups prime targets for online fraud, fake job offers, and phishing schemes.

Trust in institutional support remains low. Women and LGBTQIA+ individuals in particular avoid reporting online abuse to the police due to prior experiences of harassment, misgendering, or being blamed. Some victims reported that law enforcement officials disclosed their complaints to the perpetrators. Social media platforms such as Facebook and TikTok are also seen as unresponsive, and many victims are unaware of how to navigate platform complaint systems.

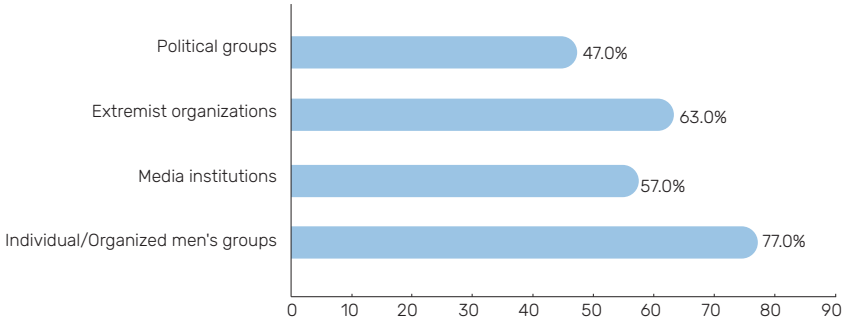
Because of these intersecting barriers, marginalized groups are more likely to experience severe consequences from online abuse, including blackmail, revenge porn, identity theft, public exposure, and community ostracism. The psychological toll is significant—some victims have been forced to change their appearance, relocate, or, in extreme cases, attempt suicide. With little knowledge of their rights or avenues for redress, many victims silently exit the digital space by deleting accounts or throwing away SIM cards. However, this withdrawal does not eliminate the harm, which often persists or escalates offline.

A culture of silence and shame further suppresses reporting, especially for women who are Muslim, LGBTQIA+, or from rural areas. Victim-blaming and fear of social consequences lead many to hide their experiences rather than seek help. As one organization observed, "Only 20–30 per cent of our community members report online abuse—and even fewer go to the authorities."

Ultimately, the digital divide in Sri Lanka reflects and reinforces broader structural inequalities. Without targeted, inclusive digital literacy programmes, culturally and linguistically accessible safety resources, and trusted institutional support, the most vulnerable will remain at greatest risk—online and offline.

There is an organized dimension of online hate that underscores the need for proactive measures to counter malicious campaigns and hold perpetrators accountable. Political groups (47 per cent), extremist organizations (63 per cent), media institutions (57 per cent), and individual as well as organized men's groups (77 per cent) were identified in the study as amongst key perpetrators. Focus group discussions and interviews reveal that hate speech in Sri Lanka is not only widespread but also strategically manipulated for political purposes. Politicians and politically motivated groups deliberately exploit social media platforms to spread divisive narratives, particularly targeting ethnic, religious, and sexual minorities. Hate content is often disguised within "entertainment" pages, which are later weaponized to incite communal tensions, distract from governance failures, and rally extremist support under the guise of nationalism and cultural protection. Politicians reportedly fund youth groups to manage and produce such content, which is frequently monetized for financial gain through views, likes, and subscriptions. This form of tech-facilitated political propaganda highlights the urgent need for legal accountability, digital platform regulation, and civic education to counter hate-driven narratives online.

Figure 8: Key perpetrators of TFGBV (as reported by respondents)



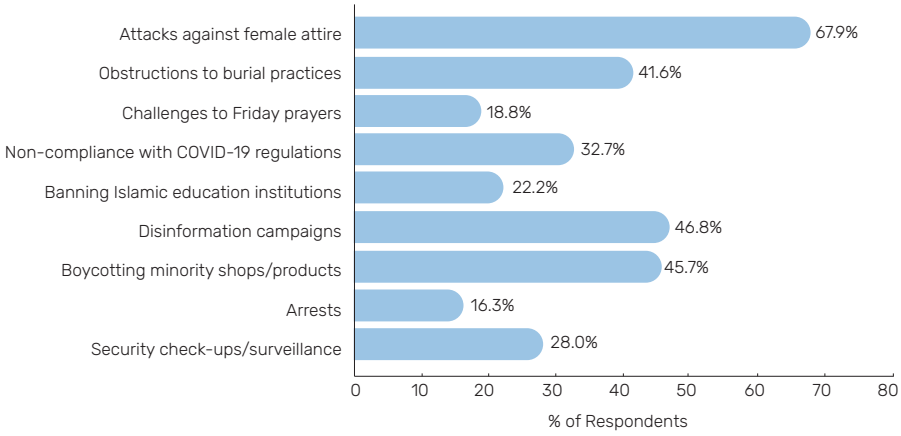
3.3 The nexus of national crises and TFGBV proliferation

Periods of national crisis in Sri Lanka, notably the COVID-19 pandemic, the economic crisis, the "Aragalaya" movement, and Easter Sunday bombings, have witnessed a significant proliferation of online hate content and TFGBV. An analysis of hate content revealed a spike in such content in 2021 to 2022 coinciding with these events. The increased reliance on digital platforms during these times inadvertently exposed more individuals, especially youth, to TFGBV, among other issues. During these crises, social media became a critical space for both political mobilization and the dissemination of misinformation and hate speech. These events spurred increased hateful content targeted at religious and ethnic minorities, medical professionals (such as Dr. Shafi Shihabdeen),[40] and government officials, with narratives often fabricating blame and inciting hostilities.

The study specifically highlights how Muslim communities were subjected to intense online and offline attacks following the Easter Sunday bombings and during the COVID-19 pandemic, with hate content focusing on their attire, burial practices, and alleged non-compliance with regulations. For example, during COVID-19, misinformation and conspiracy theories spread, falsely accusing Muslims of spreading the virus. This led to offline discrimination—denial of services, verbal abuse on public transport, and included official directives which did not permit burial of Muslims who died due to COVID-19 related complications in some districts, which goes against Muslim burial rites. Focus groups and interviews also discussed how the 2019 Easter bombings triggered a sharp escalation in anti-Muslim sentiment, particularly online. Facebook and YouTube were flooded with hate content, portraying Muslims as terrorists and calling for retaliation. Muslim women faced verbal abuse for wearing religious attire; public suspicion made everyday activities unsafe—bus travel, shopping, and even education became points of scrutiny. Politically motivated groups weaponized the tragedy, creating social media posts that exploited public fear to deepen ethnic and religious divides. False narratives (e.g., "Muslims are taking over" or "spreading COVID") were used to justify exclusion from public services, harassment, boycotting of Muslim-owned businesses, and sometimes vigilante violence.

40 Dr. Shihabdeen faced serious allegations in May 2019 when he was accused of allegedly performing unauthorized sterilisation surgeries on (Sinhalese) women, amassing wealth through illicit means, and having connections with a terrorist organization. This led to his immediate suspension and subsequent arrest and detention. Following a prolonged and contentious legal battle, he was acquitted of all charges in 2024 and reinstated to his position at the Kurunegala Teaching Hospital.

Figure 9: Forms of online and offline hate against ethnic/religious minorities during crises (as reported by respondents)



Focus group discussions and interviews underscored how the COVID-19 pandemic drastically altered digital behaviour in Sri Lanka, especially among children, women, and marginalized communities. Digital access expanded rapidly, with phones provided to children for online learning. This unmonitored access led to exposure to violent content, creation of risky online relationships, and increased vulnerability to abuse. WhatsApp, IMO, and Zoom-based school groups were reportedly misused by students, teachers, and outsiders. Several cases involved teachers soliciting or misusing children's personal data, leading to grooming, sextortion, and blackmail. Women and girls, particularly Muslim women, reported heightened targeting—mocked for their attire (hijab, burqa), scrutinized in online classes, and isolated from mainstream digital conversations.

Digital platforms have been used by various disinformation actors to manipulate public sentiment and divert attention from broader socio-economic issues. This represents a threat to social cohesion and democratic discourse at the macro level. As highlighted in focus group discussions and interviews, Sri Lanka's ongoing economic collapse has driven many, especially unemployed youth—to exploit social media for income, sometimes through unethical or violent means. As reported by the respondents, politicians and extremist groups fund youth to manage Facebook pages and create hate content targeting minorities (ethnic, religious, sexual, or caste-based). Pages originally created for entertainment are sold to political entities once a large following is built. Unemployed youth, especially between school and university or job phases, were identified by respondents as drawn into content creation for hate pages to earn money. The role of mainstream media outlets in amplifying hate content on their social media channels, often operating without adequate regulation or oversight, further exacerbated this issue. Moreover, government officials, tasked with communicating or disseminating government directives, have also been targets and proliferators of misinformation, resulting in a sense of distorted information reality.

These findings showcase how sustained risk factors such as economic inequality, ethnic and religious conflicts, and political instability, coupled with situational triggers such as pandemics exacerbate gender-based violence and gender, sexual and ethnic minorities both online and offline spaces. The confluence of these risk factors and triggers are important considerations to inform prevention and response efforts against TFGBV.

TFGBV instigated through media institutions

The focus group and interview data reveal that media institutions in Sri Lanka—both traditional and digital—are deeply implicated in the production and amplification of hate speech, online violence, and systemic discrimination. Rather than serving as neutral information platforms, these institutions often reinforce social hierarchies and marginalize vulnerable communities, including women, LGBTQIA+ individuals, ethnic and religious minorities, rural populations, and survivors of abuse.

Participants noted that both mainstream media and social platforms regularly violate basic ethical principles. Driven by commercial incentives, private media outlets frequently publish sensationalized or fabricated stories, sometimes exposing the identities of survivors—including minors and LGBTQIA+ individuals—without consent. These violations often include sexually explicit content, defamatory language, and hate speech, with little to no consequences for media houses or content creators.

Mainstream media further normalize discriminatory narratives under the guise of cultural commentary or religious critique. Women, especially those in public life, are routinely targeted with sexualized language, body shaming, and invasive coverage of their personal lives. Similarly, LGBTQIA+ individuals and minority communities—particularly Muslims and Tamils—are vilified, especially in the wake of events like the Easter Sunday attacks or the COVID-19 pandemic.

Social media has become a particularly powerful tool for political manipulation. Many divisive or hate-filled posts originate from accounts funded by politically motivated actors. These accounts, which often begin as harmless entertainment pages, are later weaponized to spread extremist content, discredit minority groups, and distract from governance failures. Youth and university students are sometimes recruited to create and manage these posts, highlighting how hate speech is institutionalized and commodified.

The digital media ecosystem further encourages this behaviour through profit-driven algorithms. Platforms like YouTube, Facebook, and TikTok reward inflammatory content with higher visibility and monetization, making hate speech against women, LGBTQIA+ people, and ethnic minorities a profitable venture. Content that incites outrage or perpetuates stereotypes tends to generate more views, likes, and subscriptions, reinforcing a cycle of abuse for economic gain.

Efforts to report and remove harmful content are often ineffective. Participants shared that reporting systems on major platforms are slow, not user-friendly, and inaccessible in local languages. Automated moderation tools frequently miss hate speech written in Sinhala, Tamil, or mixed language formats like “Sinenglish.” Even when content is re-

moved, it often resurfaces quickly through other accounts, revealing a system ill-equipped to handle context-specific abuse.

The impact on survivors is devastating. Many individuals—especially women and LGBTQIA+ people—experience severe emotional, social, and professional consequences. Fear of being re-targeted or disbelieved prevents many from speaking out or seeking legal redress. Public perceptions are heavily influenced by this toxic media environment, further entrenching stigma and silence.

3.4 Systemic deficiencies in prevention and response

Despite existing efforts of both State and non-State actors in Sri Lanka, the study reveals significant systemic deficiencies that impede effective prevention and response to TFGBV. These gaps manifest across legal, institutional, operational, and societal dimensions, creating a challenging environment for victim-survivors and allowing perpetrators to act with relative impunity. This section discusses a few critical systemic deficiencies with a view of understanding key barriers for effective prevention and response of TFGBV.

Findings from FGDs underpin that Sri Lanka›s legal landscape is inadequately equipped to address the complexities and evolving nature of TFGBV. For one, there are definitional gaps on TFGBV, making legal interpretation and enforcement difficult. Particularly, laws such as the Obscene Publications Ordinance No. 4 of 1927 and the Penal Code are archaic and do not adequately regulate complexities of TFGBV. Laws such as the Personal Data Protection Act, No. 9 of 2022 may be limited to holding organizations accountable and inadequate to address offences such as doxxing perpetrated by individuals and informal groups. While the Online Safety Act (OSA) No. 9 of 2024, aims to strengthen the legal framework, it has garnered criticism from legal professionals and civil society, who argue that certain provisions could infringe upon human rights and fundamental freedoms, including freedom of information and expression. 45 per cent of the respondents believed that the OSA will be used to curb freedom of expression (Table 83). During KIIs, experts noted that gaps in the law may only become apparent upon full implementation. Such ambiguities in the law allow selective enforcement or complete inaction, especially regarding gender and minority-specific targeting. For example, with regard to TFGBV faced by LGBTIQA+ communities, insights from the FGDs revealed that there were uncertainties regarding the protection of minority sexual groups from online harassment by the Online Safety Act. Concerns were also shared regarding gaps in terms of media regulation, particularly with regard to mainstream media with an online presence. During KIIs, government stakeholders pinpointed that the proposed Broadcasting Regulatory Authority Bill has the ability to regulate television and radio. However, civil society actors, activists and human rights defenders have

raised concerns regarding the potential implications of the proposed bill on freedom of expression and broader transparency in the legislative process.[41] Findings also reveal gaps in the legislative framework with regard to gender-sensitive language. KIIs with the Ministry of Women and Child Affairs underscored the need to have a clear policy framework to address TFGBV, focusing specifically on gender sensitive language. This stresses the need to strengthen gender-responsive laws and policies, action plans and budgets underscoring commitment and mechanisms to address TFGBV.

The research also reveals institutional and operational limitations, including deficits in government institutions mandated to address TFGBV. Lack of specialized expertise in law enforcement is a critical concern. Law enforcement officials, including police personnel, frequently lack the necessary technical expertise, computer literacy, digital forensics capacity, gender sensitivity, and knowledge of legal frameworks to effectively handle TFGBV complaints, conduct investigations, and distinguish between hate and non-hate content. Judicial processes are slow, often causing survivors to abandon their cases due to prolonged trauma and fear of re-victimization in court. Low conviction rates and a lack of effective redressal mechanisms discourage survivors from reporting. A KII with a representative from the Cyber Crimes Investigations Division (CCID), revealed that in relation to online gender-based violence and girls from 2021 to 2023 there were 1,203 sexual harassment cases, 1,404 circulations of nude Pictures cases. It was stressed that despite CCID being the only government agency with a trusted partner relationship with Meta (formerly the Facebook company), there were challenges in addressing complaints. Authorities noted that unless content was graphic in nature, there have been added challenges in addressing complaints because Meta uses Google Translate for language translation, which often fall short in translating colloquial Sinhala/Tamil and misses important context and nuances of language that cannot be machine translated. Amid these challenges, lack of technical expertise, equipment and funding for specific data extraction programmes have created barriers for authorities to adequately respond to complaints and grievances made by victims/survivors.

Equally concerning is the roll-back of Meta policies on third-party fact-checking, hate speech and abuse. Similar to X.com, Meta has relaxed its rules related to hate speech and abuse specifically when it comes to sexual orientation and gender identity as well as immigration status, as these were considered as "out of touch with mainstream discourse".[42] Meta also removed a sentence from its policy rationale explaining why it bans certain hateful conduct. The now-deleted sentence acknowledged that hate speech "creates an environment of intimidation and exclusion, and in some cases may promote offline violence." This roll-back is particularly worrisome given that this research report indicates that sexual orientation and gender identity are key targets in the proliferation of hateful content, with real-life consequences.

41 https://www.cpalanka.org/statement-on-the-proposed-online-safety-bill/#:~:text=In%202021%2C%20the%20Cabinet%20approved,robust%20and%20safe%20online%20space.
42 https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/

Another aspect that impacts prevention and response mechanisms is the limited geographical reach and resources for authorities. The CCID operates only in five districts (Colombo, Kandy, Ampara, Matara, and Kurunegala), leaving large parts of the country without direct access to specialized cybercrime units. The CCID also faces limitations in staffing, particularly a lack of female officers, inadequate office space, limited internet facilities, and insufficient licensed software tools for data extraction. An FGD with a Former Journalist in Ampara highlighted this, stating, "There is no cyber-crimes unit in Samanthurai, people need to travel long distances to Ampara town, if women have to complain, they often are dissuaded by the distance to travel and to complain in unfamiliar surroundings." KIIs also revealed that training for authorities, to handle specific issues related to TFGBV should cover all provinces. It was noted during KIIs that at the time of the study, only 6 provinces had received training on handling LGBTQIA+ complaints, three more were yet to be covered.[43]

Survivors also reported that authorities were ineffective in taking necessary actions even within the existing legal framework. A participant from a FGD with a women's organization articulated this challenge by stating that

"Even the police officers do not address our concerns when we go to them with complaints about these hateful contents. Even police officers are unsure of how to respond to these incidents. They are ignorant of the incident's legal history and the process for filing a complaint."

Moreover, 39 per cent of the study's survivors reported that they were afraid to go to the police to file a complaint and 41 per cent of the survivors stressed that they were afraid of personal information being shared (Table 76). Thus, it is evident that concerns exist with regard to re-victimisation once a complaint has been made with the authorities, which impedes reporting of TFGBV complaints due to fear(s) and stigma. Added to this is survivors lacking access to gender-sensitive legal aid, psychosocial services, and safe reporting channels - especially for survivors from rural and marginalized communities. The few services available are not consistently gender-sensitive or LGBTQIA+ inclusive. This results in many avoiding reporting due to fear of blame, stigma, or retaliation, and because existing systems are not survivor-centered and ready to respond to TFGBV cases. While platforms like SLCERT and NCPA offer hotlines and online portals, these are underutilized due to lack of awareness of such forms of support and trust.

43 The details of the trainings and provinces were not specified during the KIIs.

Barriers to Reporting TFGBV and Inadequate Survivor Support

The study reveals a number of barriers that discourage survivors from reporting TFGBV incidents and accessing crucial support:

Fear of victim-blaming and stigma: A significant proportion of survivors (38.9 per cent) were "scared to go to make a complaint" to the police, with 40.7 per cent expressing "fear of information being shared" (Table 76). This fear is deeply rooted in societal stigma and the risk of victim-blaming, which often leads to survivors being treated as perpetrators themselves. An FGD with Women's organization stated, "Even the police officers do not address our concerns when we go to them with complaints about these hateful contents... They start questioning the person who came to lodge the complaint and start criticizing the victims and put the blame on him." A KII with a survivor also mentioned that after being physically assaulted and reporting to the police, they were told "ah oya ohoma inna nisa nay ohoma wennay" (these things happen because of how you are) and no action was taken.

Lack of trust in authorities: Survivors reported a lack of trust in the police (24.1 per cent) and perceived a "lack of protection for women, girls and sexual minorities" (22.2 per cent) (Table 76). This erosion of trust is exacerbated by instances of ineffective action by authorities (16.7 per cent) and even alleged links to perpetrators (5.6 per cent) or demands for bribes (1.2 per cent). A KII with an LGBTQIA+ community member noted, "When they go to complain the issues to authorities, they take the gender identities rather than taking the complaint." The same KII also mentioned, "when they take the complaint, they handle the case on the way they like. Sometimes they directly contact the perpetrators and tell that so and so has complained against you. Then our community members are facing high security risk." Another survivor from Jaffna shared an experience where a girl committed suicide after her phone's pictures were leaked, and the police "dismissed the complaint and placed the blame on the victim›s parents."

Limited access to psychosocial support: Awareness and utilization of counselling services among survivors are extremely low with only 5.7 per cent of survivors seeking counselling (Table 77). Many survivors cope internally (29.9 per cent), citing embarrassment (14 per cent), fear/lack of trust in speaking with unknowns (17.5 per cent), or fear of family disapproval (3.1 per cent) as reasons for not seeking help (Table 78). This is critical given that 75 per cent of survivors who sought technical support reportedly contemplated ending their lives if the problem was not resolved. A KII with Grassrooted Trust indicated that while their clients in rural settings access counselling, "within school setting, within university settings however, the stigma around counselling or around accessing mental health, any kind of mental health support appears to be still very prevalent." They further noted that school counsellors are often perceived as "gossips," leading to breaches of confidentiality.

Protracted legal proceedings: The legal process is often prolonged, with court cases years to be resolved and causing protracted distress to survivors. This disincentivizes legal action, with only 33 per cent of survivors reporting to law enforcement and a mere 6 per cent pursuing criminal charges (Table 80; Table 81). An FGD with a Community Service organization highlighted a case from 2019 still pending, noting that "Since the case has an impact on the survivor's social life and mental health, it must be resolved at least within six months." They added that "due to the length of time it takes to file a lawsuit, there is a high

chance that the parties will drop their case, allowing the offender to live with impunity."

Low public awareness of reporting mechanisms: 39.3 per cent of survey respondents were unaware of where to seek assistance for social media harassment (Table 79), despite 57 per cent feeling unsafe online. This highlights a critical need for accessible and well-publicized reporting pathways. Findings from KIIs and FGDs reveal a lack of confidence in the system. An FGD with Factory Workers stated, "We do not know that there are other institutions or persons to say these things," often resorting to simply removing SIM cards or logging out of accounts.

Lack of family support and social stigma: KII with the NCPA shows that women and children often receive minimal care from families if they become victims of TFGBV. Fear of judgment, lack of parental understanding, and fear of repercussions often discourage young girls from disclosing abuse, exacerbating their emotional trauma and leading to disruption of their education. A survivor's KII detailed how her family's reaction to her personal photos being leaked made her "feel ashamed that something like that is out there." Another survivor mentioned,

"I don't think any of us complained to our parents because I don't think at the time we could rely on our parents to have the right reaction, "especially due to perceived "fault" for having certain pictures or engaging in activities deemed inappropriate by parents.

Findings from KIIs also revealed that there was no central and secure data management system on complaints, records of survivors, or incidents, leading to duplication of complaints and a severe lack of centralized data. This means responsible institutions operate in silos with limited coordination and information sharing, leading to reduced accountability and responsiveness to TFGBV complaints. An official from the Ministry of Women, Child, and Youth Affairs conceded, "Now we do not have a proper mechanism to trace offensive content or contents targeting women, children, and minority communities in social media. In our reporting system, we have only one category called online harassment." This absence of robust data management systems hampers effective response and policymaking. A KII with CERT also echoed this, recommending "one platform where CERT, CCID, National Child Protection Authority (NCPA)….can access" to nullify duplication and improve response rates. KIIs also revealed that NCPA was not a trusted reporting partner with META, requiring complaints to be routed through the CCID, causing unnecessary delays in content removal. A KII with Hithawathi, an NGO working on TFGBV, highlighted that it is "not easy to remove already uploaded photos or videos from the platforms" and that "it generally takes 2 to 3 days." The KII further stated that "Unless that goes against their [platform's] community guidelines, they don't even take down," referring to social media platforms, and that platforms like YouTube are "very difficult to work with" for content removal.

A key consideration in this regard is platform accountability and content moderation - especially in Sinhala and Tamil languages - which is a larger policy issue. There are no binding codes of conduct or enforcement mechanisms to regulate platform or media behaviour. Tech companies and social media platforms lack accountability for failing to moderate hate content in Sinhala and Tamil. There is a lack of legal accountability and content moderation mechanisms for mainstream and digital media who often amplify hate speech and gendered disinformation without consequences. During KIIs survivors raised concerns regarding the lengthy, technical and complicated reporting mechanisms in platforms such as Facebook. One survivor described Facebook›s response to an obscene message as merely saying they "would look into it" with no clear action. It is evident from the findings of the study that, in addition to State actors such as the CCID, at the time the research non-state actors such as Hashtag Generation and Hithawathi, had "trusted partner" status with some platforms (e.g., Meta, TikTok), enabling faster content removal. However, awareness of these channels remained low among the general public, especially those outside of urban settings. Evidently direct access by victims to platforms is often limited. Gaps in digital literacy spanning from safe online practices to holding platforms accountable heightens vulnerabilities and contributes to the normalization of online abuse and the proliferation of TFGBV. There is a critical need to strengthen community-based organizations and first respondents with capacities and resources to address online violence and their offline impacts. The current landscape necessitates a strategic shift towards a proactive prevention and response framework. This includes a robust legal system, enhanced institutional capacity, and survivor-centered support systems. The pervasive and intersectional nature of TFGBV demands a comprehensive and multi-sectoral response that transcends traditional approaches to gender-based violence.

04

RECOMMENDATIONS & WAY FORWARD

This study identified a range of risk factors, triggers, and enabling conditions that contribute to online violence in Sri Lanka. These include harmful and discriminatory social norms and behaviours related to gender, sexuality, ethnicity, and other intersectional identities, as well as political affiliations, recurring national crises, and systemic deficiencies in addressing TFGBV. While responding to violence after it occurs remains important, participants also highlighted numerous barriers to reporting and accessing justice or support. Existing response mechanisms were seen as inadequate, poorly equipped, and under-resourced, unable to address either the scale or the offline consequences of online abuse. Therefore, a shift toward prevention—stopping violence before it occurs and preventing repeated harm—is an urgent next step.

Prevention requires sustained, long-term efforts to shift social norms, attitudes, and beliefs that legitimize inequality and violence, particularly those targeting gender and intersecting identities. These efforts must operate across the socio-ecological spectrum:

- **At the individual level:** interventions should promote digital literacy, consent education, and resilience, especially among women, girls, and marginalized communities vulnerable to online harm.
- **At the relationship level:** there is a need to foster respectful online communication, challenge power dynamics, and support healthy digital boundaries, particularly within intimate relationships.
- **At the community level:** schools, workplaces, and digital spaces must be transformed into safe, inclusive environments with clear protocols for reporting and responding to TFGBV.
- **At the societal level:** broader structural change is necessary, including the enforcement of gender-equitable laws, greater accountability for digital platforms, and media reforms that counter misogynistic, racist, and homophobic narratives.

By addressing TFGBV across all levels of the socio-ecology, prevention becomes comprehensive, sustainable, and responsive to the intersecting forms of oppression that shape the digital lives of women and marginalized groups.

Advancing the prevention of violence is only possible when there is continuous learning about the effectiveness of policies and programmes designed to address it. This requires sustained investment in monitoring and evaluation of prevention and response efforts across the short, medium, and long term. Such learning is critical to inform and adapt future violence prevention strategies. Global evidence shows that significant reductions in the lifetime prevalence of gender-based violence (GBV) can be achieved through long-term, well-designed prevention interventions—typically over programmatic cycles of 3 to 5 years.

However, as prevention efforts intensify, the demand for response services may initially increase, due to greater awareness and reporting in the short and medium term.

Measuring progress in prevention therefore requires intentional tracking of key indicators: [44] in the short term, this includes changes in the enabling environment, such as the adoption of supportive laws and policies; in the medium term, it involves assessing shifts in the underlying drivers of violence, such as gender inequality and harmful social norms. This kind of targeted, evidence-driven monitoring is especially critical in addressing TFGBV, where emerging risks and interventions must be closely observed to ensure effectiveness.

4.1 Global normative frameworks to prevent and respond to TFGBV

Further, over the past few years, globally there has been significant normative progress in addressing TFGBV.[45]

- The 2023 Commission on the Status of Women (CSW67) Agreed Conclusions and UN General Assembly Resolution A/78/213 recognized the urgent need to address gender-based violence and girls in digital spaces. These instruments acknowledged various forms of digital gender-based violence—including harassment, stalking, and non-consensual image sharing—and called for states and tech platforms to take proactive, rights-based, and AI-conscious measures to prevent such harm. They marked an important shift in prioritizing innovation and digital inclusion for gender equality while highlighting the risks technology poses when misused.

- In 2024, international momentum grew with multiple UN resolutions, regional frameworks, and global compacts explicitly addressing TFGBV. The UN's Safe, Secure and Trustworthy AI resolution and the Global Digital Compact emphasized inclusive, safe digital environments and accountability in AI development. The Human Rights Council and the UNGA further urged stronger legislation, platform regulation, and cross-sector cooperation.

- Regional frameworks such as the EU digital service acts and the African Union Convention on Ending VAWG introduced binding obligations for online safety, platform accountability, and transparency in AI content, reinforcing a collective move toward coordinated global governance to eliminate digital gender-based violence and girls.

44 https://asiapacific.unwomen.org/en/digital-library/publications/2021/07/making-progress-in-prevention-possible
45 https://www.unwomen.org/en/digital-library/publications/2025/06/normative-advances-on-technology-facilitated-violence-against-women-and-girls

4.2 Global normative frameworks for TFGBV programming

UNFPA framework for TFGBV programming

The prevention and mitigation pillar under the UNFPA framework for TFGBV programming, includes: (1) designing safer technologies, (2) enhancing digital literacy, (3) closing the gender digital divide, and (4) addressing harmful social and gender norms.[46] According to the UNFPA Framework, effective TFGBV prevention programming must be deeply rooted in the several foundational elements including:

a. **Gender-based violence principles:** Programs must be survivor-centered and trauma-informed, prioritizing safety, confidentiality, ethical data handling, respect, and holistic support. They must also be non-discriminatory, informed by an intersectional analysis to ensure accessibility and adaptation to diverse needs. Prevention efforts should be participatory, engaging diverse stakeholders including survivors and grassroots organizations in design, implementation, and evaluation. Accountability through feedback mechanisms is crucial, and a gender-transformative approach is essential for promoting gender equality, human rights, and systemic change, advocating for technology design that prioritizes safety, privacy, and human rights.

b. **Personnel and organizational well-being:** Ensuring the mental health and resilience of teams dealing with TFGBV cases through self-care initiatives like access to mental health professionals and resources, and collective care through robust support systems, continuous learning, and comprehensive training on trauma-informed care and digital safety.

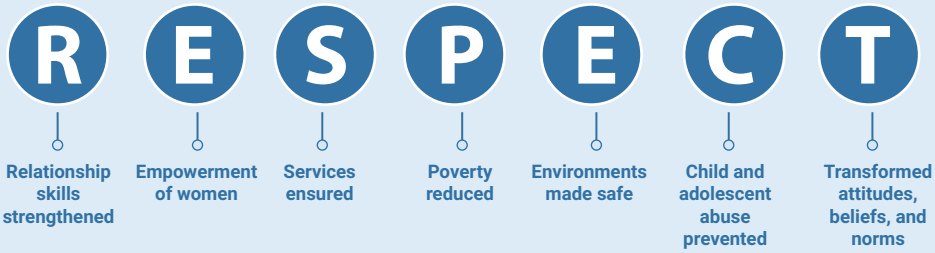
c. **Coordination and partnerships**: Fostering multi-stakeholder engagement with local NGOs, civil society organizations, women's rights organizations, and the tech companies/platforms. Building strong coordination mechanisms among government agencies, NGOs, and tech companies/platforms is crucial for multi-sectoral and survivor-centered programming, fostering trust through transparency and consistent communication. Integration of TFGBV organizations into existing gender-based violence multi-sectoral coordination mechanisms is encouraged.

Furthermore, data and evidence remains crucial for effectively preventing TFGBV as they ensure that prevention and mitigation interventions are informed by current data and trends, thereby enhancing their effectiveness and overall impact.[47] As such study offers valuable insights to provide the necessary foundation to design, implement, and continuously improve TFGBV prevention policies and programs, ensuring they are effective, responsive to evolving threats, and centered on the needs and rights of survivors.

46 https://www.unfpa.org/sites/default/files/pub-pdf/A%20Framework%20for%20TFGBV%20programme ming.pdf
47 https://www.unfpa.org/sites/default/files/pub-pdf/UNFPA_Measuring%20TF%20GBV_%20A%20Discussion%20Paper_FINAL.pdf; https://www.unfpa.org/sites/default/files/pub-pdf/An%20Infographic%20Guide%20to%20TFGBV.pdf

Applying the RESPECT violence prevention framework to prevent TFGBV

The RESPECT framework,[48] developed by UN Women and the World Health Organization (WHO), offers a comprehensive evidence-based approach to preventing gender-based violence . Each letter in RESPECT represents a strategy for prevention:



Applying the RESPECT framework to TFGBV prevention ensures a holistic, multi-level approach that blends legal, educational, technological, and community-driven strategies. It recognizes that violence in digital spaces is rooted in the same gender inequalities, power imbalances, and social norms that drive violence offline—and must be tackled accordingly. Only through systemic transformation, survivor-centered services, and empowered communities can we build a digital world that is safe, inclusive, and just for all.

To prevent TFGBV using the RESPECT framework, we can adapt and apply each strategy to digital and online contexts:

R – Relationship skills strengthened

(Online Conflict Resolution and Digital Communication)

- Promote digital communication skills and respectful online interaction in relationships through school curricula and community training.
- Integrate digital consent education in relationship-building programmes to address issues such as non-consensual image sharing and cyberstalking.
- Train youth and couples on resolving digital conflicts without resorting to threats, coercion, or public shaming, especially in intimate or break-up contexts.

E – Empowerment of women (Digital Literacy and Online Agency)

- Build digital literacy and cyber safety skills for women and girls, including LGBTQIA+ and ethnic minority women, so they can navigate online spaces safely and assertively.
- Support women in tech and digital rights advocacy through leadership development and funding for feminist digital organizing.
- Enable marginalized women to reclaim digital spaces through online activism, storytelling, and counter-speech initiatives.

48 RESPECT framework is: RESPECT Women: Preventing violence against women | UN Women – Headquarters

S – Services ensured (Survivor-Centered Tech-Responsive Services)

- Ensure survivor-friendly reporting and response mechanisms for TFGBV within law enforcement, hotlines, and support centers.
- Develop multi-lingual, confidential helplines and counseling services that understand the dynamics of online harassment and non-consensual image distribution.
- Train service providers—social workers, health professionals, police, and legal actors—on recognizing and addressing TFGBV.

P – Poverty reduced

(Bridging the Digital Divide and Economic Empowerment)

- Invest in inclusive access to technology and affordable internet, so economic marginalization doesn't compound digital exclusion or exposure to TFGBV.
- Support women-led digital enterprises and provide training in safe online entrepreneurship, especially for women in rural and low-income settings.
- Reduce economic vulnerability to digital exploitation (e.g., through transactional relationships, image-based abuse) by ensuring economic safety nets and income-generating programs.

E – Environments made safe

(Safe Online Platforms and Regulatory Frameworks)

- Mandate platform accountability to remove harmful content and protect users from online abuse, especially marginalized genders.
- Advocate for privacy-by-design and gender-sensitive product development in apps, games, and online services.
- Strengthen data protection and cybercrime laws to cover online stalking, doxxing, AI-generated sexual content, and hate speech.
- Promote gender-safe online environments in schools, workplaces, and public institutions through codes of conduct and response protocols.

C – Child and adolescent abuse prevented

(Digital Safety for Girls and LGBTQIA+ Youth)

- Integrate comprehensive digital safety education in school curricula that addresses online grooming, image-based abuse, and cyberbullying.
- Work with parents and caregivers to foster open communication about online risks without punitive control over girls' or LGBTQIA+ youths' digital freedoms.
- Promote youth leadership in developing peer-led digital safety campaigns that reflect their lived experiences.

T – Transformed attitudes, beliefs, and norms
(Shifting Online Culture and Gender Norms)

- Challenge harmful gender stereotypes and normalize consent, diversity, and respect through online media, influencers, and public campaigns.
- Promote bystander intervention and positive digital citizenship to encourage people to speak out against TFGBV.
- Support counter-narratives and feminist content to reshape digital dis course and reclaim online spaces from misogyny, homophobia, and racism.

Good practices and lessons for policy and programmatic interventions:

UN Women's Safe Cities and Safe Public Spaces initiative: launched in 2010, the programme is aimed at reducing all forms of gender-based violence and girls in public and urban spaces across cities globally. While primarily focused on physical spaces, the initiative has progressively integrated digital strategies to address overlaps between online harassment and public space safety: In some cities, partners now incorporate reports of online harassment and surveillance issues into their safety audits. And cities increasingly adopt policies encouraging private-sector and platform accountability, urging social media platforms to monitor and remediate TFGBV, and align with broader human rights and digital safety frameworks. In Quezon City, the largest city in Metro Manila in the Philippines, the Safe City Programme empowered grassroots women, girls, researchers, and local government partners to gather data on sexual harassment and push for stronger legal protections. Building on this momentum, the Philippines government passed the Safe Spaces Act in 2019, which formally recognized and defined gender-based sexual harassment in public spaces as well as in digital spaces and detailed sanctions against such violence. This was among the first laws in the Southeast Asia region to explicitly recognize TFGBV.

Australia's eSafety Commissioner's "Technology, gendered violence and Safety by Design" Industry Guide: In September 2024, Australia's online safety regulator, the eSafety Commissioner, released a comprehensive resource titled "Technology, gendered violence and Safety by Design." This guide serves as a crucial blueprint for technology companies, aiming to enhance their understanding and approach to proactively addressing TFGBV. It meticulously outlines how "Safety by Design" principles can be integrated into the very foundation of technology development, enabling companies to anticipate, detect, and ultimately eliminate TFGBV before it manifests. Drawing upon established principles and practices from the eSafety Commissioner's earlier "Safety by Design" initiative, launched in 2018, this guide directly exemplifies the good practice of prioritizing user safety as a foundational element in technology development. This approach shifts the onus from reactive response to proactive prevention, embedding safety considerations from the initial design phase of digital platforms and services.

World Wide Web Foundation's Tech Policy Design Lab and efforts towards safety by design:[49] In 2021, the World Wide Web Foundation hosted this lab, which convened global civil society stakeholders, researchers, and government representatives alongside major tech companies such as Meta, Google, TikTok, and Twitter (now X). A key focus was to establish a global accountability mechanism to combat Online Gender-Based Violence effectively. The lab developed strategies including encouraging tech companies to address underlying structural problems (which may require changes in business models), exploring design interventions through collaborative efforts, and strengthening global accountability by combining regulation, awareness, and best business practices. This initiative directly supports the good practice of engaging with the technology sector to close the divide between platforms and TFGBV practitioners and highlights efforts towards 'Safety by Design' within the industry itself.

49 https://webfoundation.org/our-work/projects/tech-policy-design-lab/#:~:text=The%20Lab%20is%20a%20collaborative,empowering%20online%20world%20for%20everyone.

ANNEXURES

Annexure I:
Existing legal framework

The following laws in Sri Lanka are being used to handle technology-facilitated violence.

1. The Constitution of Sri Lanka
2. The Penal Code Ordinance No. 11 of 1887 (as amended)
3. The Prevention of Terrorism (Temporary Provisions) Act No. 48 of 1979
4. Police Ordinance (No. 16 of 1865)
5. International Covenant on Civil and Political Rights Act No. 56 of 2007
6. The Obscene Publications Ordinance No. 4 of 1927 (as amended)
7. Computer Crimes Act, No. 24 of 2007
8. Personal Data Protection Act No. 9 of 2022
9. Public Security Ordinance, No. 25 of 1947
10. Children and Young Persons (Harmful Publications) Act No. 48 of 1956
11. Convention on Preventing and Combating Trafficking in Women and Children for Prostitution Act No. 30 of 2005
12. The Assistance for and Protection of Victims and Witnesses Act No. 4 of 2015
13. Online Safety Bill Act No. 9 of 2024

The officials of law enforcement authorities mainly use Sections 285, 286, 345, 360, 372, 385, 399, 483, 486, and 487 of the Penal Code Ordinance to take legal actions against the perpetrators . The Obscene Publications Act Section 02 and 03 is used for in the case of creating, sharing and selling obscene pictures . Investigations relating to violent content leading to unauthorized access to computers, offences committed against national security, dealing with personal data and unauthorized disclosure of information will be covered under Sections 03, 04, 05, 06, 07 and 10 of the Computer Crime Act of 2007 .

The Police relies on the Penal Code to charge offenders and ICCPR Act is used very rarely as ICCPR offers no bail option and is difficult to seek relief. IGP Circular 2740/2022 is used by the various departments of the police to handle complaints received from a transgender-person/ persons who have undergone harassment though innuendo or verbal comments. The various steps required to be undertaken during the investigation have been specified this Circular .

Annexure II:
Development of the online tracking system and data extraction

Features of the hate content tracking programme

A software that has been developed for tracking hate content can efficiently extract data from multiple social media platforms, including Google, Facebook, YouTube (and YouTube Shorts), and X.com, to classify and analyse hate content with a particular focus on gender-targeted hate content. At its core, the system integrates an AI-driven automatic hate content classification model, leveraging the Cross-Lingual Language Model (XLM-R) with RoBERTa architecture as its representer and a Bi-directional Long Short-Term Memory (BiLSTM) network as its classifier. Equipped with pre-trained knowledge, the software ensures robust performance across diverse datasets. Data persistence is handled by a movable and lightweight SQLite database, making the system portable and efficient. Additionally, it features intuitive data visualization tools, enabling users to filter and explore data through on-screen graph-based visualizations. For further analysis and reporting, visualizations can be exported to PNG format, ensuring seamless integration with external workflows.

The AI model

The model consists of two components namely XLM-R (Figure 17) and BiLSTM (Figure 18). XLM-R comes with a cross-language (over 100 languages) knowledge. It knows the usual patterns of characters and their occurrences in words for around 100 languages including both English and Tamil. The knowledge related to Sinhala was introduced by fine tuning the model with around 500,000 Sinhala sentences. The XLM-R is used as the language representer that should be used for tokenizing the sentences.

The classification was done using a BiLSTM model. BiLSTM captures context from both past and future words in a sentence, improving understanding for tasks like translation or classification. Then many samples of hate content, gender targeted hate content and non-hate content contents were showed to the model with supervised training. The model learned the patterns of characters, words, sentences, emoticons and other punctuations of samples from different classes.

Figure 10: XLM-R Model

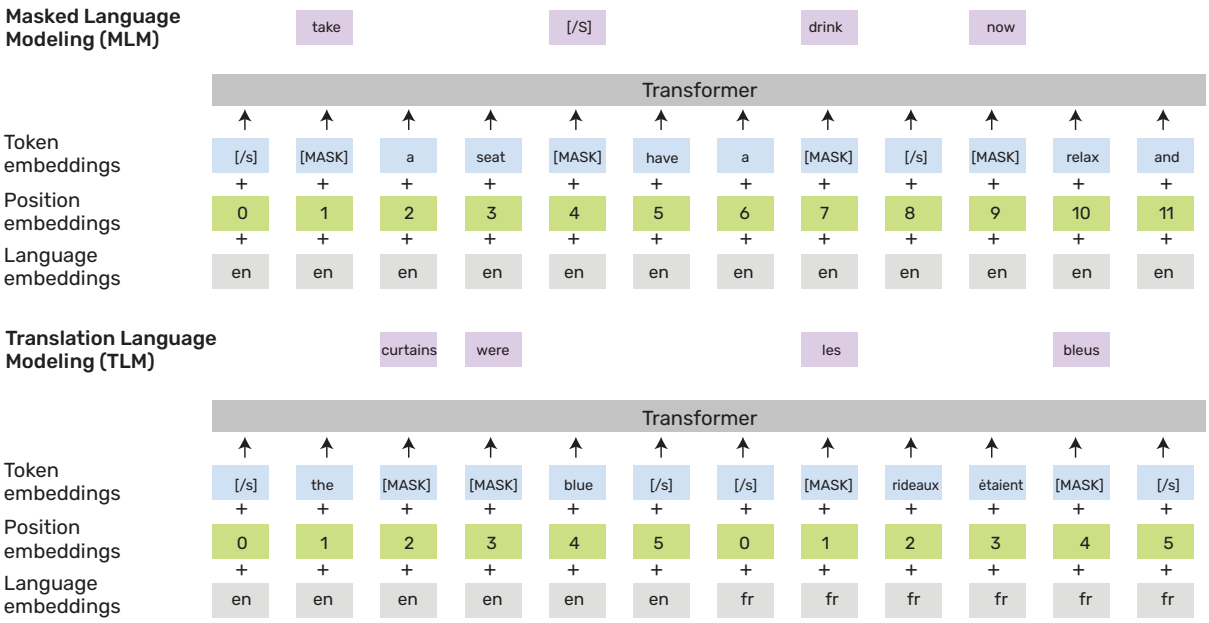
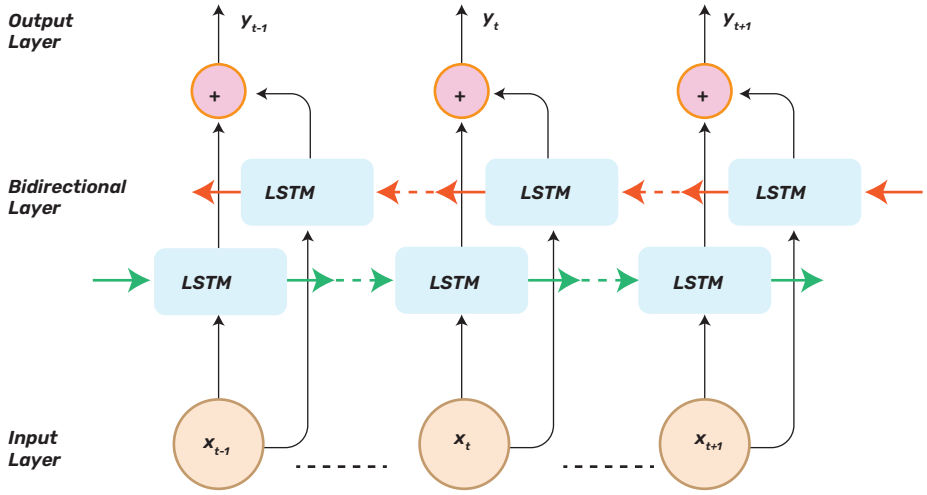


Figure 11. BiLSTM Model



The model classifies the content independently from the context while handling any ambiguity with the inferred probability. The inference done based on the observed training data under the error posed at the convergence of the model.

Process of Data Extraction

Keywords used in the extraction

A collection of keywords in all three languages that are usually being used in hateful content was used throughout the data extraction process. In order to obtain the list of keywords, first a random set of posts and contents were gathered manually and then manually classify the content to potential hate content. Then the stopping words and non-significant words were removed from the classified content. The remaining words were taken as the list of keywords. This process allowed the software to gather relevant posts and comments.

Facebook

The program extracts posts with the metadata, comments and reactions from public pages without login into an account. For this study, a list of pages that have a history of hateful content, were used to extract data. To find these lists of pages, the keyword collection was used as the search query in Facebook, page search section, and selected all relevant pages with their links (URLs).

YouTube, YouTube Shorts:

The sampling was done by issuing the search terms from the collection of keywords. The headless browser facilitated this data collection, bypassing user interaction. Video URLs, titles, and comments can be extracted from both YouTube videos and YTShorts.

Google

The sampling was done by issuing the search terms from the collection of keywords. The headless browser facilitated this data collection, bypassing user interaction. The link and the short description associated with each of the search results can be extracted.

X.com

Although the official Application Programmable Interface (API) is costly, the headless browser technique provided with the tracking software can extract X's posts from the profiles specified by a set of URLs without login into an account. The ordering and appearance of the content are based on the user agent's metadata (browser type, device type and geographical location etc. of the tracker).

Instagram and TikTok:

Data from Instagram and TikTok was extracted using a custom-made Google Chrome plugin, which is not part of the tracker program, and manually parsed. Due to challenges related to CAPTCHA verification imposed by the platforms, making an automated scraping tool is not feasible on these platforms. The content was selected as they appeared to a fresh account without any followers or followings.

Data annotation

The collected data was classified and annotated by university students who specialize in Information and Communication Technology (ICT). These students, being active on social media, were able to accurately tag the data for various categories of hate content, including Gender, Race, Age, Disability, Sexuality, Ethnicity, Nationality, Religion, and Profession. Moreover, all the annotators were fluent in the English language. The content from the other languages were annotated by the respective native speakers.

Model training:

The extracted data was integrated with the data gathered from other sources such as the open datasets published by Kaggle community. Then the dataset was pre-processed by removing any content in a Language (in its Unicode representation) other than English, Sinhala or Tamil and removing the contents with only periods, commas and nonprintable characters. The pre-processed complete dataset was then augmented by introducing the transliterated versions of Sinhala and Tamil content that are classified into any of the positive classes into the original dataset. This specific augmentation was carried out due to the lack of positive data to the relevant positive categories as well as the content can be appeared in both the native characters as well as the transliterated forms. The size of the dataset exceeds 50,000 data points after dataset integration and augmentation.

The XLM-R model was fine-tuned by utilizing around 500,000 Sinhala sentences from four Sinhala corporas in order to provide the support for Sinhala language. It is noteworthy that the XLM-R base model supports English and Tamil languages out of the box. Then, a BiLSTM (Bidirectional Long Short-Term Memory) AI model was trained using the annotated dataset that is tokenized using the fine-tuned XLM-R model. The BiLSTM is designed to detect hate content in future datasets by recognizing patterns in text that correspond to hate content. The bidirectional nature of the LSTM model allows it to consider both the preceding and following context within posts and comments, enhancing detection accuracy. The model currently supports classifying the provided content to hate content and further it is gender targeted or not.

Training Setup

The model was trained on a workstation utilizing a NVIDIA RTX 3090 24GB GPU, i7 12th Gen high-performance processor with 64GB RAM. The optimization process converged within 10 hours and the best solution was taken as the final model.

Analysis

The annotated data was analysed to detect trends in gender-based hate content and cyberbullying. This analysis aimed to uncover patterns over time and across different social media platforms, identifying the evolution of online hate content and the intersection of different categories of hate content with gender category.

Evaluation metrics

The model was evaluated by recording the accuracy, recall and precision.

Accuracy = (Number of Correct Predictions) / (Total Number of Predictions)
Recall = True Positives / (True Positives + False Negatives)
Precision = True Positives / (True Positives + False Positives)

High accuracy denotes the model is good at predicting a given sample into its correct category regardless of the category being hateful or not hateful. Higher recall denotes the model is good at predicting the hateful contents. Higher precision denotes that the model is good at predicting the hateful contents while maintaining low false positives (incorrectly predicting as a hateful content).

Annexure III: List of KIIs conducted

No.	Name of the Institution/ Person	No. of KIIs
1	Bureau for the Prevention of Abuse of Children and Women	1
2	Ministry of Mass Media	1
3	Sri Lanka Police - Computer Crime Investigation Division	1
4	Sri Lanka Police - Head of Training/ Former IGP	2
5	Hashtag Generation	1
6	Telecommunication Regulatory Commission	1
7	Sri Lanka Computer Emergency Readiness Team	1
8	Ministry of Women's Affairs	1
9	National Child Protection Authority	2
10	National Committee on Women	2
11	Hithawathi – Not for Profit organization	1
12	The Grassrooted Trust – Not for Profit organization	1
13	Women Politicians, Colombo	2
14	TFGBV Survivors, Colombo	4
15	Women Activist, Colombo	1
16	Human Rights Commission, Colombo	1
17	Provincial Government Media Reporter, DS Office, Galle	1
18	Media Activist, Galle	2
19	Migrant Worker, Gale	1
20	District Officer, Foreign Employment Bureau, Galle	1
21	Human Rights First Aid Centre, Galle	1
22	Counsellor, Ampara	1
23	Journalist/ Social Media Activists, Ampara	1
24	Mediator, Ampara	1
25	Program Manager - NGO, Ampara	1
26	Religious Leader, Ampara	1
27	Counsellor, Gender-based violence, Jaffna	1
28	Social Service Officer, GA Office, Jaffna	1
29	Social Media Activist, Jaffna	1
30	Founder Member of NGO & Public Health Officer, Jaffna	1
31	Women Activist, Kandy	1
32	TFGBV Survivors, Kandy	2
33	Professionals, Kandy	2
	Total	43

Annexure IV: List of FGDs conducted

No.	Name of the Respondent Group/ organization	No. of KIIs
1	LGBTQIA+ Community, Colombo	1
2	Factory Workers, Katunayake	1
3	Ruhunu Rural Women's Front, Galle	1
4	Jasmin Women Foundation, Galle	2
5	Human and Natural Resources Development Foundation, Galle	1
6	Youth Group, Ampara	1
7	Muslim Women Foundation, Ampara	1
8	University Students, Jaffna	1
9	LGBTQIA+ Community, Jaffna	2
10	Ekamuthu Women Society/ Factory Workers, Kandy	2
11	University Students, Kandy	1

Annexure V: Data visualization

Table 1 - Number of complaints received during the last 5 Years – Institution Wise

Year	2019	2020	2021	2022	2023	2024 Sep
SLCERT	2,969	15,965	17,157	15,674	20,219	17,058
NGO	-	-	870	1,838	2,440	1,686
NCW	106	290	306	121	218	138
NCPA	-	-	-	282	189	105

Source: Based on data provided by the institutions during the study

Table 2 - Social media platforms use by respondents

Social Media Platform	Frequency	% out of responses	% out of 361 Respondents
Facebook	301	16.1%	83.4%
Twitter	28	1.5%	7.8%
YouTube	321	17.2%	88.9%
TikTok	209	11.2%	57.9%
Telegram	101	5.4%	28.0%
Google	199	10.7%	55.1%
WhatsApp	348	18.6%	96.4%
Botim	8	0.4%	2.2%
Snapchat	98	5.2%	27.1%
Instagram	133	7.1%	36.8%
LinkedIn	54	2.9%	15.0%
IMO	54	2.9%	15.0%
Other	14	0.7%	3.9%
Total	**1868**	**100.0%**	

Table 3 - Disaggregation of data by gender - Social media platforms use by respondents

Gender	Man	% of 85 respondents	Woman	% of 221 respondents	LGBTQIA+	% of 55 respondents	Total
Facebook	78	92%	169	76%	54	98%	301
Twitter	8	9%	10	5%	10	18%	28
YouTube	77	91%	201	91%	43	78%	321
TikTok	54	64%	113	51%	42	76%	209
Telegram	30	35%	53	24%	18	33%	101
Google	51	60%	123	56%	25	45%	199
WhatsApp	81	95%	218	99%	49	89%	348
Botim	0	0%	4	2%	4	7%	8
Snapchat	20	24%	63	29%	15	27%	98
Instagram	36	42%	75	34%	22	40%	133
LinkedIn	17	20%	34	15%	3	5%	54
IMO	19	22%	23	10%	12	22%	54
Other	5	6%	6	3%	3	5%	14
Total Respondents	**85**		**221**		**55**		**361**

Table 4 - Disaggregation of data by ethnicity - Social media platforms use by respondents

Ethnicity	Sinhala	% out of 190	Tamil	% out of 90	Muslim	% out of 81	Total
Facebook	166	87%	77	86%	58	72%	301
Twitter	16	8%	5	6%	7	9%	28
YouTube	171	90%	77	86%	73	90%	321
TikTok	109	57%	66	73%	34	42%	209
Telegram	69	36%	12	13%	20	25%	101
Google	119	63%	47	52%	33	41%	199
WhatsApp	183	96%	86	96%	79	98%	348
Botim	3	2%	2	2%	3	4%	8
Snapchat	50	26%	31	34%	17	21%	98
Instagram	77	41%	25	28%	31	38%	133
LinkedIn	33	17%	6	7%	15	19%	54
IMO	28	15%	15	17%	11	14%	54
Other	6	3%	6	7%	2	2%	14
Total Respondents	**190**		**90**		**81**		**361**

Table 5 - Disaggregation of data by ethnicity - Time spend on social media

Ethnicity	Many times during the day/night	%	Once a day	%	Every other day	%	Weekly	%	Total
Sinhala	169	89%	16	8%	3	2%	2	1%	190
Tamil	50	56%	23	26%	17	19%	0	0%	90
Muslim	58	72%	22	27%	1	1%	0	0%	81
Total Respondents	**277**	**77%**	**61**	**17%**	**21**	**6%**	**2**	**1%**	**361**

Table 6 - No. of hours spent on social media

No. of Hours	Frequency	% out of 361Respondents
Less than 1 hour	36	10.0%
1-2 hours	85	23.5%
3-4 hours	129	35.7%
5-6 hours	72	19.9%
Over 7 hours	39	10.8%
Total Respondents	**361**	**100%**

Table 7 - Type of content make you or others feels unsafe or targeted

Offensive Content	Frequency	% out of Responses	% out of 361 Respondents
Comments that threatened individuals	75	15.5%	20.8%
Offensive discourse targeting a group based on race, ethnicity, religion, sex or gender	139	28.7%	38.5%
Offensive images, cartoons, memes, objects, gestures and symbols disseminated online or offline	170	35.1%	47.1%
Content that encourages violence towards a person or community	39	8.1%	10.8%
A content that intended to damage individual emotionally	27	5.6%	7.5%
Others	2	0.4%	0.6%
I do not know	32	6.6%	8.9%
Total Responses	**484**	**100%**	

Table 8 - Disaggregation of data by ethnicity - Type of content make you or others feels unsafe or targeted

Content	Sinhala	% out of 190	Tamil	% out of 90	Muslim	% out of 81	Total	%
Comments that threatened individuals	55	29%	12	13%	8	10%	75	21%
Offensive discourse targeting a group based on race, ethnicity, religion, sex or gender	58	31%	38	42%	43	53%	139	39%
Offensive images, videos, cartoons, memes, objects, gestures and symbols disseminated offline or online	106	56%	35	39%	29	36%	170	47%
Content that encourages violence towards a person or community	13	7%	12	13%	14	17%	39	11%
A content that intended to damage individual emotionally	20	11%	3	3%	4	5%	27	7%
Others	1	1%	0	0%	1	1%	2	1%

Table – 9 Disaggregation of data by gender - Type of content make you or others feels unsafe or targeted

Content	Men	% out of 85	Women	% out of 221	LGBT-QIA+	% out of 55	Total	%
Comments that threatened individuals	17	20%	44	20%	14	25%	75	21%
Offensive discourse targeting a group based on race, ethnicity, religion, sex or gender	31	36%	84	38%	24	44%	139	39%
Offensive images, videos, cartoons, memes, objects, gestures and symbols disseminated offline or online	37	44%	104	47%	29	53%	170	47%
Content that encourages violence towards a person or community	13	15%	21	10%	5	9%	39	11%
A content that intended to damage individual emotionally	3	4%	20	9%	4	7%	27	7%
Others	1	0%	2	0%	0	0%	2	1%

Table - 10 Disaggregation of data by women's ethnicity - Type of content make you or others feels unsafe or targeted

Content	Sinhala	% out of 119	Tamil	% out of 48	Muslim	% out of 60	Total	% out of 227
Comments that threatened individuals	32	27%	6	13%	7	12%	45	20%
Offensive discourse targeting a group based on race, ethnicity, religion, sex or gender	37	31%	19	40%	31	52%	87	38%
Offensive images, videos, cartoons, memes, objects, gestures and symbols disseminated offline or online	67	56%	18	38%	23	38%	108	48%
Content that encourages violence towards a person or community	8	7%	6	13%	8	13%	22	10%
A content that intended to damage individual emotionally	15	13%	3	6%	4	7%	22	10%
Others	1	1%		0%	1	2%	2	1%

Table 11 - Method used to target the survivors

Method	Frequency	% out of Responses	% of 103 Survivors
Doctored videos and images (Morphing/Deep fakes)	26	9.6%	25.2%
Unauthorized personal information exposure (Doxxing)	25	9.3%	24.3%
Cyber blackmail (Sextortion, Revenge porn)	21	7.8%	20.4%
Creating fake profiles	38	14.1%	36.9%
Sharing obscene text messages and videos	38	14.1%	36.9%
Image based abuse	24	8.9%	23.3%
Cyber grooming	9	3.3%	8.7%
Gender trolling	25	9.3%	24.3%
Hacking	6	2.2%	5.8%
Anonymous letter	3	1.1%	2.9%
Face to face	13	4.8%	12.6%
Posters and leaflets,	2	0.7%	1.9%
Phone Calls	35	13.0%	34.0%
Other, please specify	5	1.9%	4.9%
Total Responses	**270**	**100%**	

Table 12 - Disaggregation of data by gender – Method used to target the survivors (103 Respondents)

Content Type	Man	% of 17	Woman	% of 58	LGBTQIA+	% of 28	Total
Doctored videos and images (Morphing/ Deepfakes)	4	24%	8	14%	14	50%	26
Unauthorized personal information exposure (Doxxing)	4	24%	9	16%	12	43%	25
Cyber blackmail (Sextortion, revenge porn)	4	24%	13	22%	4	14%	21
Creating fake profiles	10	59%	19	33%	9	32%	38
Sharing obscene text messages and videos	5	29%	23	40%	10	36%	38
Image based abuse	5	29%	11	19%	8	29%	24
Cyber grooming	0	0%	7	12%	2	7%	9
Gender trolling	1	6%	13	22%	11	39%	25
Hacking	0	0%	4	7%	2	7%	6
Anonymous letter	0	0%	3	5%	0	0%	3
Face to face	0	0%	10	17%	3	11%	13
Posters and leaflets,	1	6%	1	2%	0	0%	2
Phone Calls	2	12%	21	36%	12	43%	35
Other	0	0%	5	9%	0	0%	5
Total Respondents	**36**		**147**		**87**		**270**

Table 13 - Disaggregation of data by ethnicity - Method used to target the survivors (103 Respondents)

Content Type	Sinhala	% of 68	Tamil	% of 25	Muslim	% of 10	Total
Doctored videos and images (Morphing/Deepfakes)	16	24%	7	28%	3	30%	26
Unauthorized personal information exposure (Doxxing)	18	26%	5	20%	2	20%	25
Cyber blackmail (sextortion, revenge porn)	15	22%	5	20%	1	10%	21
Creating fake profiles	26	38%	9	36%	3	30%	38
Sharing obscene text messages and videos	29	43%	7	28%	2	20%	38
Image based abuse	19	28%	3	12%	2	20%	24
Cyber grooming	9	13%	0	0%	0	0%	9
Gender trolling	15	22%	7	28%	3	30%	25
Hacking	5	7%	1	4%	0	0%	6
Anonymous letter	2	3%	0	0%	1	10%	3
Face to face	8	12%	2	8%	3	30%	13
Posters and leaflets,	0	0%	0	0%	2	20%	2
Phone Calls	23	34%	7	28%	5	50%	35
Other	3	4%	0	0%	2	20%	5
Total	**188**		**53**		**29**		**270**

Table 14 - Social media platforms used to target the survivors

Social Media Platform	Frequency	% of Responses	% of 103 survivors
Facebook	79	45.4%	76.7%
YouTube	4	2.3%	3.9%
Instagram	11	6.3%	10.7%
TikTok	15	8.6%	14.6%
WhatsApp	54	31.0%	52.4%
IMO	4	2.3%	3.9%
Snapchat	1	0.6%	1.0%
Botim	1	0.6%	1.0%
Telegram	3	1.7%	2.9%
Other	2	1.1%	1.9%
Total Responses	**174**	**100%**	

Table 15 - Disaggregation of data by ethnicity – Social media platforms used to target the survivors

Social Media Platform	Sinhala	% of 68 Respondents	Tamil	% of 25 Respondents	Muslim	% of 10 Respondents	Total
Facebook	51	75%	22	88%	6	60%	79
YouTube	2	3%	2	8%	0	0%	4
Instagram	8	12%	2	8%	1	10%	11
TikTok	9	13%	5	20%	1	10%	15
WhatsApp	40	59%	8	32%	6	60%	54
IMO	3	4%	0	0%	1	10%	4
Snapchat	1	1%	0	0%	0	0%	1
Botim	1	1%	0	0%	0	0%	1
Telegram	3	4%	0	0%	0	0%	3
Other	1	1%	1	4%	0	0%	2
Total Responses	**119**		**40**		**15**		**174**

Table 16 - Respondents' opinion on the risk of being subjected to content

Response	Frequency	% out of 361 Respondents
Yes	223	61.8%
No	125	34.6%
I do not know	13	3.6%
Total Respondents	**361**	**100%**

Table 17 - Disaggregated data by ethnicity and gender - Do not know the risk of being subjected to violent content

Gender	Sinhala	% out of 190	Tamil	% out of 90	Muslim	% out of 81	Total	% out of 391
Men	17	9%	10	11%	7	9%	34	15%
Women	29	15%	19	21%	26	32%	74	33%
LGBTQIA+	2	1%	3	3%	2	2%	7	3%

Table 18 - Disaggregation of data based on district - Respondents' opinion on the risk of being subjected to content

District	Yes	% out of respondents in each district	No	% out of respondents in each district	I do not know	% out of respondents in each district	Total
Ampara	27	52%	24	46%	1	2%	52
Colombo	82	64%	44	34%	3	2%	129
Jaffna	29	55%	23	43%	1	2%	53
Kandy	56	73%	20	26%	1	1%	77
Galle	29	58%	14	28%	7	14%	50
Total	**223**	**62%**	**125**	**35%**	**13**	**4%**	**361**

Table 19 - Disaggregation of data based on age - Respondents' opinion on the risk of being subjected to content

Age	Yes	% out of respondents in each age group	No	% out of respondents in each age group	I do not know	% out of respondents in each age group	Total
18 - 24	81	53%	64	42%	8	5%	153
25 - 29	56	60%	36	39%	1	1%	93
30 - 35	43	80%	9	17%	2	4%	54
36 - 45	30	75%	9	23%	1	3%	40
46 - 59	13	62%	7	33%	1	5%	21
Total	**223**	**62%**	**125**	**35%**	**13**	**4%**	**361**

Table 20 - Disaggregation of data based on ethnicity - Respondents' opinion on the risk of being subjected to content

Ethnicity	Yes	% out of respondents in each ethnicity	No	% out of respondents in each ethnicity	I do not know	% out of respondents in each ethnicity	Total
Sinhala	135	71%	48	25%	7	4%	190
Tamil	46	51%	42	47%	2	2%	90
Muslim	42	52%	35	43%	4	5%	81
Total	**223**	**62%**	**125**	**35%**	**13**	**4%**	**361**

Table 21 - Disaggregation of data based on gender - Respondents' opinion on the risk of being subjected to content

Gender	Yes	% out of respondents in each gender group	No	% out of respondents in each gender group	I do not know	% out of respondents in each gender group	Total
Man	50	59%	32	38%	3	4%	85
Woman	126	57%	86	39%	9	4%	221
LGBTQIA+	47	85%	7	13%	1	2%	55
Total	**223**	**62%**	**125**	**35%**	**13**	**4%**	**361**

Table 22 - Opinion on the contribution of social media for individuals to commit violence

Response	Frequency	% out of 361 Respondents
Yes	324	89.8%
No	27	7.5%
I Do not wish to disclose	1	.3%
Do not know	9	2.5%
Total Respondents	**361**	**100%**

Table 23 - Types of gender-based violence, girls and sexual minorities

Violence	Frequency	% of Responses	% out of 361 Respondents
Cyber harassment	223	24.0%	61.8%
Revenge porn	278	30.0%	77.0%
Threats of rape	83	8.9%	23.0%
Sexual assault or murder	108	11.6%	29.9%
Blackmailing for demanding payment or other benefits	231	24.9%	64.0%
Others, please specify	3	0.3%	0.8%
I don't like to mention	2	0.2%	0.6%
Total Responses	**928**	**100%**	

Table 24 - Disaggregation of data by gender - Types of gender-based violence, girls and sexual minorities

Content	Men	% out of 85	Women	% out of 221	LGBT-QIA+	% out of 55	Total	% out of 361
Cyber harassment	54	64%	133	60%	36	65%	223	62%
Revenge porn	68	80%	170	77%	40	73%	278	77%
Threats of rape	18	21%	59	27%	6	11%	83	23%
Sexual assault or murder	25	29%	67	30%	16	29%	108	30%
Blackmailing for demanding payment or another benefits	56	66%	139	63%	36	65%	231	64%
Others, please specify	2	2%	1	0%	0	0%	3	1%

Table 25 - Online forum or social media groups engage in targeting people

	Frequency	% out of 361 Respondents
Yes	151	41.8%
No	185	51.2%
I Do not wish to disclose	1	0.3%
I do not Know	23	6.4%
Refused to Answer	1	0.3%
Total Respondents	**361**	**100%**

Table 26 - Disaggregation of data by women from various ethnic groups complaints - Online forum or social media groups engage in targeting people

Gender	Sinhala	% out of 116	Tamil	% out of 46	Muslim	% out of 59	Total	% out of 221
Woman	46	39%	20	43%	24	41%	90	41%
Total	**116**		**46**		**59**			

Table 27 - Individuals and institutions creating and sharing hate contents

Individual/ Institution	Creating Content			Sharing Content		
	Frequency	% out of Responses	% out of 361 Respondents	Frequency	% out of Responses	% out of 361 Respondents
Men	259	19.2%	71.7%	283	18.7%	78.4%
Women	99	7.4%	27.4%	146	9.7%	40.4%
Girls	60	4.5%	16.6%	98	6.5%	27.1%
Boys	169	12.6%	46.8%	204	13.5%	56.5%
Non Binary	69	5.1%	19.1%	95	6.3%	26.3%
Extremists	228	16.9%	63.2%	225	14.9%	62.3%
Political figures	171	12.7%	47.4%	164	10.8%	45.4%
Media	206	15.3%	57.1%	231	15.3%	64.0%
Religious Institutions	61	4.5%	16.9%	50	3.3%	13.9%
Educational Institutions	19	1.4%	5.3%	12	0.8%	3.3%
Other, Please specify	1	0.1%	0.3%	1	0.1%	0.3%
I do not know	4	0.3%	1.1%	3	0.2%	0.8%
Total Responses	**1346**			**1512**	**100**	

Table 28 - Disaggregation of data by women from various ethnic groups complaints - Individuals and institutions creating violent contents

Individual/ Institution	Sinhala	% out of 116	Tamil	% out of 46	Muslim	% out of 59	Total	% out of 221
Men	77	66%	36	78%	40	68%	153	69%
Women	30	26%	17	37%	15	25%	62	28%
Girls	26	22%	3	7%	14	24%	43	19%
Boys	65	56%	15	33%	26	44%	106	48%
Non Binary	27	23%	2	4%	11	19%	40	18%
Extremists	73	63%	24	52%	38	64%	135	61%
Political Figures	60	52%	14	30%	26	44%	100	45%
Media	72	62%	22	48%	37	63%	131	59%
Religious Institutions	20	17%	6	13%	11	19%	37	17%
Educational Institutions	5	4%	2	4%	5	8%	12	5%
Other	1	1%	0	0%	0	0%	1	0%
	116		46		59		221	

Table 29 - Disaggregation of data by women from various ethnic groups complaints - Individuals and institutions sharing violent contents

Individual/ Institution	Sinhala	% out of 116	Tamil	% out of 46	Muslim	% out of 59	Total	% out of 221
Men	85	73%	37	80%	45	76%	167	76%
Women	49	42%	17	37%	24	41%	90	41%
Girls	40	34%	5	11%	20	34%	65	29%
Boys	71	61%	22	48%	36	61%	129	58%
Non Binary	36	31%	5	11%	15	25%	56	25%
Extremists	73	63%	23	50%	38	64%	134	61%
Political Figures	60	52%	11	24%	27	46%	98	44%
Media	81	70%	22	48%	41	69%	144	65%
Religious Institutions	19	16%	3	7%	7	12%	29	13%
Educational Institutions	4	3%	2	4%	3	5%	9	4%
Other	0	0%	0	0%	0	0%	0	0%
	116		46		59		221	

Table 30 - Motive behind posting violent content in social media platforms

Motive	No. of Responses	% out of Responses	% out of 361 Respondents
They want attention	151	8.1%	41.8%
They have a political agenda	194	10.4%	53.7%
To gain political advantages	218	11.7%	60.4%
To gain prominence in society	154	8.3%	42.7%
For financial gain	156	8.4%	43.2%
To control/humiliate minority ethnic communities	183	9.8%	50.7%
Humiliate Women, Girls, boys and LGBTQIA+ community	238	12.8%	65.9%
To control minority religious group	165	8.9%	45.7%
Superiority/ inferiority complex	150	8.0%	41.6%
Other psychological issues	126	6.8%	34.9%
Personal grievances against women, girls, LGBTQIA+ community	216	11.6%	59.8%
Others	3	0.2%	0.8%
Total Responses	**1954**		

Table 31 - Disaggregation of data based on ethnicity - Motive behind posting violent content in social media platforms

Motive	Sinhala	% out of 190 respondents	Tamil	% out of 90 respondents	Muslim	% out of 81 respondents	Total
They want attention	81	43%	37	41%	33	41%	151
They have a political agenda	98	52%	47	52%	49	60%	194
To gain political advantages	114	60%	52	58%	52	64%	218
To gain prominence in society	90	47%	30	33%	34	42%	154
For financial gain	115	61%	23	26%	18	22%	156
To control/humiliate minority ethnic communities	73	38%	55	61%	55	68%	183
Humiliate Women, Girls, boys and LGBTQIA+ community	130	68%	57	63%	51	63%	238
To control minority religious group	67	35%	37	41%	61	75%	165
Superiority/ inferiority complex	56	29%	57	63%	37	46%	150
Other psychological issues	65	34%	35	39%	26	32%	126
Personal grievances against women, girls, LGBTQIA+ community	126	66%	52	58%	38	47%	216
Total Responses	**1015**		**482**		**454**		**1951**

Table 32 - Disaggregation of data by women from various ethnic groups complaints - Motive behind posting hate content in social media platforms

Motive	Sinhala	% out of 116	Tamil	% out of 46	Muslim	% out of 59	Total
They want attention	51	44%	18	39%	22	37%	91
They have a political agenda	61	53%	23	50%	36	61%	120
To gain political advantages	70	60%	26	57%	36	61%	132
To gain prominence in society	53	46%	19	41%	29	49%	101
For financial gain	71	61%	13	28%	12	20%	96
To control/humiliate minority ethnic communities	40	34%	26	57%	41	69%	107
Humiliate Women, Girls, boys and LGBTQIA+ community	80	69%	28	61%	36	61%	144
To control minority religious group	39	34%	20	43%	43	73%	102
Superiority/ inferiority complex	39	34%	31	67%	31	53%	101
Other psychological issues	42	36%	22	48%	19	32%	83
Personal grievances against women, girls, LGBTQIA+ community	72	62%	24	52%	24	41%	120
Total Respondents	**116**		**46**		**59**		

Table 33 - Factors in initiating offensive content online and offline

Factors	Online and Offline		
	Frequency	% out of Responses	% out of 361 Respondents
Cultural Background	209	13.3%	57.8%
Gender	231	14.8%	64.0%
Sexual orientation	254	16.2%	70.4%
Education attainment	97	6.2%	26.7%
Employment attainment	65	4.1%	17.9%
Disability	52	3.3%	14.3%
Self-esteem issues	117	7.5%	32.4%
General perception	163	10.4%	45.0%
Group identities	120	7.6%	33.1%
Political affiliation	166	10.6%	46.0%
Security environment	27	1.7%	7.5%
To control over resources (Land/ business)	33	2.1%	9.1%
Laws regulations and their enforcement	30	1.9%	8.3%
I do not know	5	0.3%	1.2%
Total Responses	**1566**	**100.0%**	

Table 34 - Disaggregation of data by ethnicity - Factors in initiating offensive content online and offline

Factors	Sinhala	% of 190	Tamil	% of 90	Muslim	% of 81	Total
Cultural Background	95	50%	59	65%	56	69%	209
Gender	127	67%	53	59%	52	64%	231
Sexual orientation	142	75%	63	69%	50	61%	254
Education attainment	45	24%	28	31%	24	30%	97
Employment attainment	36	19%	15	17%	14	17%	65
Disability	17	9%	18	20%	17	21%	52
Self-esteem issues	74	39%	20	22%	24	29%	117
General perception	103	54%	28	31%	32	40%	163
Group identities	57	30%	34	37%	30	36%	120
Political affiliation	96	51%	32	35%	39	48%	166
Security environment	15	8%	8	8%	5	6%	27
To control over resources	20	10%	7	8%	7	8%	33
Laws regulations and their enforcement	21	11%	4	4%	6	7%	30
Total Number of Respondents	**845**		**365**		**351**		**1561**

Table 35 - Disaggregation of data by women from various ethnic groups complaints - Factors in initiating content online

Factors	Sinhala	% out of 116	Tamil	% out of 46	Muslim	% out of 59	Total
Cultural Background	62	53%	19	41%	15	25%	207
Gender	40	34%	22	48%	23	39%	230
Sexual orientation	89	77%	32	70%	39	66%	263
Education attainment	32	28%	12	26%	18	31%	94
Employment attainment	21	18%	7	15%	10	17%	55
Disability	11	9%	7	15%	12	20%	49
Self-esteem issues	43	37%	8	17%	19	32%	110
General perception	74	64%	12	26%	27	46%	168
Group identities	31	27%	7	15%	18	31%	110
Political affiliation	56	48%	12	26%	26	44%	159
Security environment	11	9%	3	7%	2	3%	25
To control over resources	7	6%	1	2%	3	5%	23
Laws regulations and their enforcement	13	11%	2	4%	5	8%	30
Total Number of Respondents	**116**		**46**		**59**		**221**

Table 36 - Hate content and gender targeted hate content for the from 2021 to 2024

Year	Total no. of content	Hate content	% of Hate content	Gender targeted content	% of Gender hate speech out of total content	% of Gender hate speech out of hate content
2021	541	66	12.2%	48	8.9%	72.7%
2022	2,095	245	11.7%	37	1.8%	15.1%
2023	4,578	278	6.1%	17	0.4%	6.1%
2024	12,531	531	4.2%	73	0.6%	13.7%
Total	**19,744**	**1,120**	**5.7%**	**175**	**0.9%**	**15.6%**

Table 37 - Disaggregation of data by language - Hate content and gender targeted hate content – Sinhala Language

Year	Total no. of content	Hate content	% of Hate content	Gender targeted content	% of Gendered hate content out of total content	% of Gendered hate content out of hate content
2021	489	66	8.8%	48	9.8%	72.7%
2022	748	60	8.0%	23	3.1%	38.3%
2023	2,828	216	7.6%	13	0.5%	6.0%
2024	8,753	364	3.9%	41	0.5%	11.3%
Total	**12,818**	**706**	**5.5%**	**125**	**1.0%**	**18%**

Table 38 - Disaggregation of data by language - Hate content and gender targeted hate content – Tamil Language

Year	Total no. of content	Hate content	% of hate content	Gender targeted content	% of Gendered hate content out of total content	% of Gendered hate content out of hate content
2021	29	0	0.0%	0	0.0%	0.0%
2022	626	59	9.4%	13	2.1%	22.0%
2023	702	20	2.8%	3	0.4%	15.0%
2024	2,342	116	5.0%	32	1.4%	27.6%
Total	**3,699**	**195**	**5.3%**	**48**	**1.3%**	**25%**

Table 39 - Disaggregation of data by language - Hate content and gender targeted hate content – English Language

Year	Total no. of content	Hate content	% of hate content	Gender targeted content	% of Gendered hate content out of total content	% of Gendered hate content out of hate content
2021	23	0	0.0%	0	0.0%	0.0%
2022	721	126	17.5%	1	0.1%	0.8%
2023	1,048	42	4.0%	1	0.1%	2.4%
2024	1,436	51	3.6%	0	0.0%	0.0%
Total	**3,228**	**219**	**6.8%**	**2**	**0.1%**	**1%**

Table 40 - Intersectional analysis of gender targeted hate content

Social Media Platform	Face-book	%	YouTube & Shorts	%	Google	%	Instagram	%	TikTok	%	Total	%
Race	1	1%	0	0%	13	2%	1	2%	0	0%	15	1%
Age	1	1%	1	0%	2	0%	0	0%	0	0%	4	0%
Disability	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%
Sexuality	12	6%	26	8%	77	14%	5	10%	39	60%	159	13%
Ethnicity	10	5%	0	0%	21	4%	1	2%	0	0%	32	3%
Nationality	2	1%	1	0%	99	18%	1	2%	0	0%	103	9%
Religion	1	1%	0	0%	1	0%	1	2%	0	0%	3	0%
Profession	15	8%	35	11%	55	10%	10	20%	1	2%	116	10%
Sexist	77	39%	114	36%	210	37%	12	24%	22	34%	435	37%
Other	78	40%	138	44%	86	15%	18	37%	3	5%	323	27%
Total	**197**	**100%**	**315**	**100%**	**564**	**100%**	**49**	**100%**	**65**	**100%**	**1,190**	**100%**

Table 41 - Social media is a safe space for everyone

Is social media a safe space?	Frequency	% out of 361 Respondents
Yes	38	10.5
No	207	57.3
May be	112	31.0
I Do not wish to disclose	1	.3
Do not know	3	.8
Total Respondents	**361**	**100.0**

Table 42 - Disaggregation of data by gender - Social media is a safe space for everyone

Gender Identity	Is social media safe space for everyone?								Total
	Yes	%	No	%	May be	%	Do not Know	%	
Man	7	8%	49	58%	29	34%	0	0%	85
Woman	25	11%	124	56%	69	31%	3	1%	221
LGBTQAI+	6	11%	34	62%	14	25%	1	2%	55
Total	**38**	**11%**	**207**	**57%**	**112**	**31%**	**3**	**1%**	**361**

Table 43 - Disaggregation of data by ethnicity – Social media contributes to violence

Ethnicity	Yes	%	May be	%	No	%	I do not know	%	Total
Sinhala	126	66.3%	45	23.7%	17	8.9%	2	1.1%	190
Tamil	54	60.0%	28	31.1%	7	7.8%	1	1.1%	90
Muslim	57	70.4%	16	19.8%	8	9.9%	0	0.0%	81
Total	**237**	**65.7%**	**89**	**24.7%**	**32**	**8.9%**	**3**	**0.8%**	**361**

Table 44 - Most affected minority groups on hate content both online and offline

Ethnicity	Ethnic minorities	%	Religious minorities	%	Sexual minorities	%	Persons with disabilities	%	I do not know	%	Total
Sinhala	52	27%	49	26%	144	76%	26	14%	15	8%	190
Tamil	47	52%	26	29%	72	80%	12	13%	3	3%	90
Muslim	37	46%	49	60%	46	57%	13	16%	3	4%	81
Total	**136**	**38%**	**124**	**34%**	**262**	**73%**	**51**	**14%**	**21**	**6%**	**361**

Table 45 - Respondents personally targeted on hate content

Response	Frequency	% out of 361 Respondents
Yes	103	28.5%
No	256	70.9%
I Do not wish to disclose	2	0.6%
Total Respondents	**361**	**100.0%**

Table 46 - Disaggregation of data by ethnicity – Survivors' ethnicity

Ethnicity	No. of Survivors	% of 103 Survivors	% of 361 Respondents
Sinhala	68	66%	19%
Tamil	25	24%	7%
Muslim	10	10%	3%
Total Respondents	**103**	**100%**	**29%**

Table 47 - Disaggregation of data by ethnicity - Survivors' ethnicity

Ethnicity	Age										No. of Survivors
	18 - 24	%	25 - 29	%	30 - 35	%	36 - 45	%	46 - 59	%	
Sinhala	27	40%	21	31%	9	13%	9	13%	2	3%	68
Tamil	8	32%	7	28%	4	16%	6	24%	0	0%	25
Muslim	4	40%	3	30%	2	20%	0	0%	1	10%	10
	39	38%	31	30%	15	15%	15	15%	3	3%	103

Table 48 - Disaggregation of data by gender - Survivors' ethnicity

Age	No. of Survivors	% of 103 Survivors	% of 361 Respondents
Man	17	17%	5%
Woman	58	56%	16%
LGBTQIA+	28	27%	8%
Total Respondents	**103**	**100%**	**29%**

Table 49 - Disaggregation of data by region – No. of survivors

Age	No. of Survivors	% of 103 Survivors	% of 361 Respondents
Ampara	7	7%	2%
Colombo	43	42%	12%
Jaffna	19	18%	5%
Kandy	17	17%	5%
Galle	17	17%	5%
Total Respondents	**103**	**100%**	**29%**

Table 50 - Disaggregation of data by gender – Frequency of social media usage

Ethnicity	How often do you use social media?								No. of Survivors
	Many times during the day/night	%	Once a day	%	Every other day	%	Weekly	%	
Man	68	80%	14	16%	2	2%	1	1%	85
Woman	165	75%	43	19%	12	5%	1	0%	221
LGBTQIA+	44	80%	4	7%	7	13%	0	0%	55
Total	**277**	**77%**	**61**	**17%**	**21**	**6%**	**2**	**1%**	**361**

Table 51 - Frequency of been targeted online

Frequency	No. of Survivors	% of 103 Victims
Daily	5	4.9%
Every other day	7	6.8%
Weekly	6	5.8%
Monthly	10	9.7%
On account of a specific incident	75	72.8%
Total Respondents	**103**	**100.0**

Table 52 - Disaggregation of data by frequency of usage - Survivors' social sedia usage frequency

Frequency	No. of Survivors	% of 103 Survivors	% of 361 Respondents
Many times during the day/night	87	84%	24%
Once a day	11	11%	3%
Every other day	5	5%	1%
Weekly	0	0%	0%
Total Respondents	**103**	**100%**	**29%**

Table 53 - Age of the respondent when exposed to violent content

Age	Frequency	% of 103 Victims
Under 18	9	8.7%
18 - 24	58	56.3%
25 - 29	17	16.5%
30 - 35	10	9.7%
36 - 45	7	6.8%
46 - 59	2	1.9%
Total Respondents	**103**	**100.0**

Table 54 - Initial reaction to being targeted on violent content

Reaction	Frequency	% of Responses	% of 103 Victims
Hurt	53	16.5%	51.5%
Anger	54	16.8%	52.4%
Disappointment	32	9.9%	31.1%
Fear	63	19.6%	61.2%
Feeling Insecure	69	21.4%	67.0%
Humiliation	51	15.8%	49.5%
Total Responses	**322**	**100.0%**	

Table 55 - Comfortable with someone from the LGBTQIA+ community - (Without LGBTQIA+ respondents)

Situation	Sinhala	%	Tamil	%	Muslim	%	Total	%
As part of your family	110	67%	39	58%	32	42%	181	59%
As one of your friends	116	71%	39	58%	33	43%	188	61%
As one of your work colleagues	120	74%	46	69%	47	62%	213	70%
As your doctor	91	56%	43	64%	42	55%	176	58%
As your Member of Parliament	76	47%	29	43%	34	45%	139	45%
As a teacher of your children	78	48%	28	42%	24	32%	130	42%
Average		60%		56%		46%		56%

Table 56 - Respondents targeted offline

Response	Frequency	% of 103 Victims
Yes	56	54.4%
No	45	43.7%
No response	2	1.9%
Total Respondents	**103**	**100.0%**

Table 57 - Frequency of being targeted offline

Frequency	No. of Survivors	% of 56 Survivors
Daily	4	7.1%
Every other day	4	7.1%
Weekly	7	12.5%
Monthly	9	16.1%
On account of a specific incident	32	57.2%
Total Respondents	**56**	**100.0%**

Table 58 - Disaggregation of data by gender and ethnicity – Targeted offline

Gender Identity	Targeted Offline	% of survivors	Ethnicity	Targeted Offline	% of survivors
Man	8	47%	Sinhala	33	49%
Woman	27	47%	Tamil	18	72%
LGBTQIA+	21	75%	Muslim	5	50%
Total	**56**			**56**	

Table 59 - Disaggregation of data by gender – Frequency of offline targeting

Gender Identity	More Frequently	% out of survivors	On account of a specific incident	% out of survivors	Total
Man	3	38%	5	62%	8
Woman	7	26%	20	74%	27
LGBTQIA+	14	67%	7	33%	21
Total	**24**	**43%**	**32**	**57%**	**56**

Table 60 - Offline actions impacting the survivors daily life

Offline Action	Frequency	% of Responses	% of 103 Victims
Not leaving the safety of one's home	13	4.8%	12.6%
Staying away from work	11	4.1%	10.7%
Had to leave one's home	15	5.6%	14.6%
Leaving one's job	9	3.3%	8.7%
Personal relationships being affected	52	19.3%	50.5%
Being ostracized	43	15.9%	41.7%
Give-up education	6	2.2%	5.8%
Stopped using social media	66	24.4%	64.1%
Blocked the sender	54	20.0%	52.4%
Other, please specify	1	0.4%	1.0%
Total	**270**	**100%**	

Table 61 - Disaggregation of data by gender – Offline actions impacting the survivors daily life

Gender	Not leaving the safety of one's home	Staying away from work	Had to leave one's home	Leaving one's job	Personal relation-ships being affected	Being ostracized	Give-up educa-tion	Stopped using social media	Blocked the sender	Total
Man	2	1	1	1	8	5	1	12	5	36 (13%)
Woman	5	4	6	3	25	23	4	42	39	151 (56%)
LGBT-QIA+	6	6	8	5	19	15	1	12	10	82 (31%)
Total	**13**	**11**	**15**	**9**	**52**	**43**	**6**	**66**	**54**	**269**

Table 62 - Content result negatively in the day-to-day lives of the targeted communities and people

Negative Impact	Frequency	% of Responses	% out of 361 Respondents
Motivates violence	269	20%	74.5%
Mobilize individuals for harmful acts offline	168	12%	46.5%
Impacts mental health	308	23%	85.3%
Creates divisions between society	161	12%	44.6%
Disputes in family	215	16%	59.6%
Marginalizes individuals	245	18%	67.9%
Total Responses	**1,366**	**100%**	

Table 63 - Economic loss due to online and offline targeting

Response	Frequency	% of 103 Survivors
Yes	31	30.1%
No	71	68.9%
Refuse to answer	1	1.0%
Total Respondents	**103**	**100%**

Table 64 - Type of economic loss due to targeting

Economic Loss	Frequency	% of 31 Survivors
Unable to engage in employment/ loss of employment	12	38.7%
Decrease in the number of customers	1	3.2%
Reputation damaged	14	45.2%
Damage to personal or business property	1	3.2%
Others	3	9.7%
Total Respondents	**31**	**100.0%**

Table 65 - Mobile, Internet and Social Media Usage 2019 and 2021

Year	2019 (In Millions)	2020 (In Millions)	2021 (In Millions)	Increase (In Millions) (%)
Mobile Phone Users	28.7	31.8	30.4	1.7 (5.9%)
Internet Users	7.1	10.1	10.9	3.8 (53.5%)
Active Social Media Users	6.2	6.4	7.9	1.7 (27.4%)
	2019	**2020**	**2021**	**Increase**
Internet Penetration	34.0%	47.0%	50.8%	16.8%
Total Respondents	**31**	**100.0%**		

Source: https://datareportal.com/digital-in-sri-lanka

Table 66 - Recent incidents targeted to specific communities

Response	Frequency	% out of 361 Respondents
Yes	305	84.5%
No	28	7.8%
I do not wish to disclose	3	0.8%
I do not know	25	6.9%
Total	**361**	**100%**

Table 67 - Disaggregation of data by ethnicity - Recent incidents targeted to specific communities

Ethnicity	In your opinion do you feel these incidents have affected the specific communities?								No. of Survivors
	Yes	%	No	%	I Do not wish to disclose	%	I do not know	%	
Sinhala	154	81%	17	9%	1	1%	18	9%	190
Tamil	80	89%	5	6%	2	2%	3	3%	90
Muslim	71	88%	6	7%	0	0%	4	5%	81
Total	**305**	**84%**	**28**	**8%**	**3**	**1%**	**25**	**7%**	**361**

Table 68 - Disaggregation of data different women ethnicities - Specific incidents that have affected the specific communities

Gender	Sinhala	% out of 116	Tamil	% out of 46	Muslim	% out of 59	Total	% out of 221
Woman	93	80%	39	85%	50	85%	182	82%
Total	**116**		**46**		**59**			

Table 69 - Frequency of violent content associated with particular incidents

Frequency	Responses	% out of 361 Respondents
All the time	38	10.5%
Frequently	114	31.6%
Sometimes	139	38.5%
Rarely	49	13.6%
Never	6	1.7%
I Do not know	15	4.2%
Total	**361**	**100.0%**

Table 70 - Disaggregation of data by ethnicity - Frequency of violent content associated with particular incidents

Ethnicity	In your opinion is this type of content associated with particular incidents?												Total
	All the time	%	Frequently	%	Sometimes	%	Rarely	%	Never	%	I Do not Know	%	
Sinhala	12	6%	54	28%	84	44%	26	14%	4	2%	10	5%	190
Tamil	9	10%	25	28%	36	40%	16	18%	1	1%	3	3%	90
Muslim	17	21%	35	43%	19	23%	7	9%	1	1%	2	2%	81
Total	**38**	**11%**	**114**	**32%**	**139**	**39%**	**49**	**14%**	**6**	**2%**	**15**	**4%**	**361**

Table 71 - Social Media contents targeting women, girls, and the LGBTQ community

Incident	Yes	%	No	%	I do not know	%	Total
COVID 19	228	63.2%	109	30.2%	24	6.6%	361
Easter Bombing	230	63.7%	114	31.6%	17	4.7%	361
Aragalaya & Economic Crisis	234	64.8%	118	32.7%	9	2.5%	361

Table 72 - Disaggregation of data different women ethnicities - Specific incidents that have affected the specific communities

Gender	Sinhala	% out of 116	Tamil	% out of 46	Muslim	% out of 59	Total	% out of 221
Easter Bombing	77	66%	21	46%	44	75%	142	64%
COVID 19	79	68%	26	57%	40	68%	145	66%
Economic Crisis	72	62%	29	63%	36	61%	137	62%
Total	**116**		**46**		**59**		**221**	

Table 73 - Disaggregation of data by ethnicity: Religious minorities targeted during the Easter Bombing/COVID 19

Ethnicity	Did you feel religious minorities were targets of offensive content during the Easter Attack/ COVID 19						Total
	Yes	%	No	%	I Do not wish to disclose	%	
Sinhala	149	78%	33	17%	8	4%	190
Tamil	74	82%	14	16%	2	2%	90
Muslim	75	93%	6	7%	0	0%	81

Table 74 - Ways of religious minorities targeted during Easter Bombing/COVID 19

Response	Frequency	% out of Responses	% out of 361 Respondents
Due to female attire	245	21.2%	67.9%
Burials	150	13.0%	41.6%
Holding Friday Prayers in Mosque	68	5.9%	18.8%
Non-compliances with COVID 19 regulations	118	10.2%	32.7%
Banning certain Islamic education institutions	80	6.9%	22.2%
Disinformation campaigns against minority communities	169	14.6%	46.8%
Boycotting shops and products	165	14.3%	45.7%
Arrests	59	5.1%	16.3%
Unwanted security check-ups, surveillance (in public places)	101	8.7%	28.0%
Other, please specify	1	0.1%	0.3%
I do not wish to disclose	1	0.1%	0.3%
Total	1157	100.0	100%

Table 75 - Violent content affecting the minority communities

Content	Frequency	% out of Responses	% out of 361 Respondents
Affect mental health of individuals	246	10.9%	68.1%
Harassed	155	6.9%	42.9%
Bullied	219	9.7%	60.7%
Abused	95	4.2%	26.3%
Experienced violence	185	8.2%	51.2%
Difficulties faced in seeking redress	160	7.1%	44.3%
Restrict their physical mobility, unable to wear attire of choice	233	10.3%	64.5%
Curtailed their religious/cultural/social rights	178	7.9%	49.3%
Stigmatization	226	10.0%	62.6%
Ostracism	188	8.3%	52.1%
Affect family relationship	99	4.4%	27.4%
Financial burden	113	5.0%	31.3%
Fear of reprisal	158	7.0%	43.8%
Total	2255	100.0%	

Table 76 - Complains were not made to authorities

Reasons	Frequency	% of Responses	% of 54*
No trust in the police	13	15.1%	24.1%
Lack of protection for women, girls and sexual minorities	12	14.0%	22.2%
Fear of information being shared	22	25.6%	40.7%
Ineffective in taking necessary actions	9	10.5%	16.7%
Asking for bribes	1	1.2%	1.9%
Link to perpetrators	3	3.5%	5.6%
Scared to go to make a complaint	21	24.4%	38.9%
Others	5	5.8%	9.3%
Total Responses	**86**	**100.0%**	

** Those who did not seek support from authorities*

Table 77 - Types of support to sought by the survivors

Response	Frequency	% of 53 Survivors
Report to authorities	15	28.3%
Seek counselling	3	5.7%
Seek advice from friends and family	25	47.2%
Blocking or cutting off contact with the person	10	18.9%
Total Respondents	**53**	**100.0%**

Table 78 - Reasons for not seeking counselling services

Reasons	Frequency	% of 100* Survivors
Embarrassment to seek counselling	14	14.0%
Embarrassed due to being targeted for abusive content	5	5.2%
Fear/lack of trust speaking with someone unknown	17	17.5%
Fear of family disapproval	3	3.1%
Stigmatization	11	11.3%
Coping internally	29	29.9%
Lack of counselling facilities	7	7.2%
Was not aware of such available counsellors	4	4.1%
Other, please specify	3	3.1%
No response	7	7.2%
Total Respondents	**100**	**100.0**

**Those who did not seek counselling support*

Table 79 - Awareness about the reporting of incidents

Response	Frequency	% out of 361 Respondents
Yes	217	60.1%
No	142	39.3%
I Do not wish to disclose	2	0.6%
Total Respondents	**361**	**100.0**

Table 80 - Institutions to which complaints were reported

Response	Frequency	% of 49* Survivors
Police desk/ Cyber-crimes division of the police (Law enforcement Agency)	16	32.6%
Women's Bureau	4	8.2%
Sri Lanka Computer Emergency Readiness Team (SLCERT)	15	30.6%
Private organizations	7	14.3%
Telecommunications Regulatory Commission (TRC)	2	4.1%
Social Media Providers	5	10.2%
Total Respondents	**49**	**100.0%**

** Those who do not report the incident to authorities*

Table 81 - Steps taken by the authorities

Response	Frequency	% of 49 Survivors
Removed the contents from the social media platform	28	57.1%
Blocked access to the social media account of the content creator and/or person sharing the content.	8	16.3%
Mediation between parties by relevant authorities	7	14.3%
Criminal charges and Prosecution	3	6.1%
Investigated and arrest	2	4.1%
No responses from social media platform	1	2.0%
Total Respondents	**49**	**100.0%**

Table 82 - Awareness of the existing laws to punish offenders of violent content

Awareness on the existing laws to punish offenders	Frequency	% out of 361 Respondents
Yes	119	33.0
No	242	67.0
Total Respondents	**361**	**100.0**

Table 83 - Opinion about the Online Safety Bill

Online Safety Bill will	Frequency	% of Responses	% out of 65 Respondents
Reduce online hate content	43	31.4	66.2
Curb freedom of expression	31	22.6	47.7
Be used against political opponents	27	19.7	41.5
Provide protection for women, girls and sexual minorities	36	26.3	55.4
Total Responses	**137**	**100**	

** Those who know about the Online Safety Act*

Figure 12 - % of Hate content and gender targeted hate content on Facebook - Sinhala Language

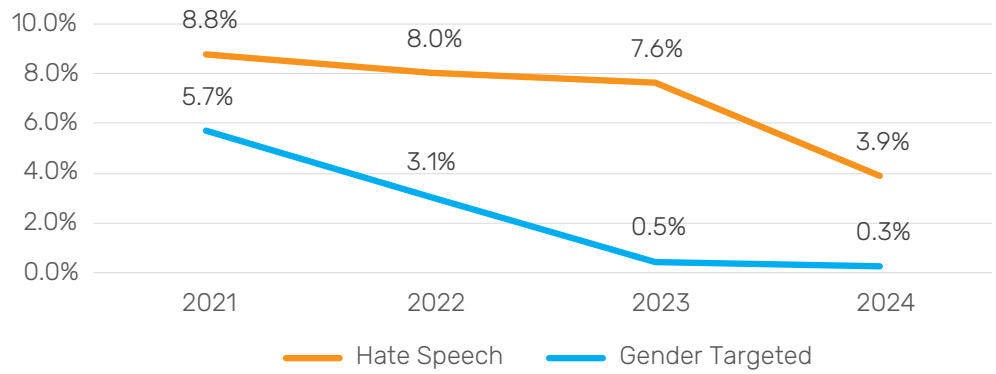


Figure 13 - % of Hate content and gender targeted hate content on Facebook - Tamil

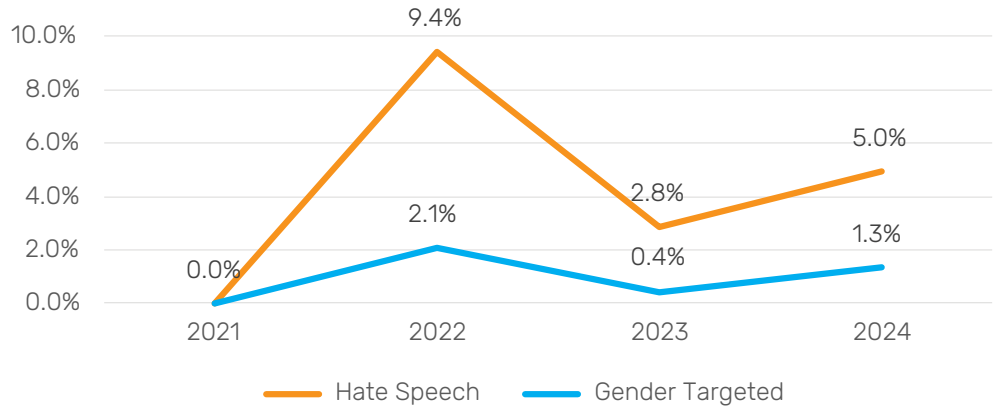
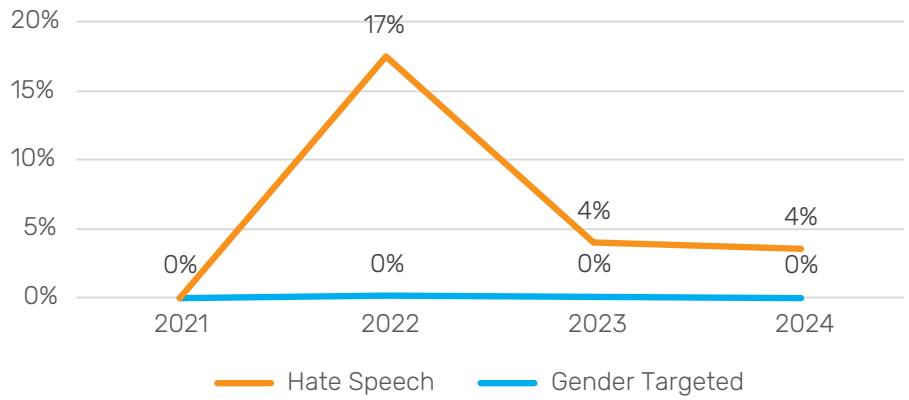


Figure 14 - % of Hate content and gender targeted hate content on Facebook - English language



Reference

Gunasekara, R. (2023). Religious violence against Christians: Disruptions and Distractions-November 2021 to October 2022.

Hattotuwa, S., & Wickremesinhe, R. (2022). Hate Speech and Social Media in Sri Lanka. Acts of Media: Law and Media in Contemporary India, 2022, 141-163.

Imtiyaz, A. R. M. (2020). The Easter Sunday bombings and the crisis facing Sri Lanka's Muslims. Journal of Asian and African Studies, 55(1), 3-16.

Imtiyaz, A. R. M., & Mohamed-Saleem, A. (2024). Islamic Faith as an Ethnic Identity Marker: Overview of Sri Lanka Muslim Identity Formation, Politicization, and Violence. Journal of Asian and African Studies, 00219096241230482.

Mihlar, F. (2024). Contending with identity and minority rights in transitional justice: the case study of Sri Lanka. The International Journal of Human Rights, 1-23.

Mujahidin, M. S. (2023 a). Extremism and Islamophobia Against the Muslim Minority in Sri Lanka. American Journal of Islam and Society, 40(1-2), 213-241.

Mujahidin, M. S. (2023 b). Islamophobia and Acts of Extremism Against Muslim Minorities in Sri Lanka Before and During the Covid-19 Pandemic. Alfuad: Jurnal Sosial Keagamaan, 7(1), 52-70.

Ramakrishna, K. (2023). Buddhist Extremism, Nationalism, and Violence: Lessons from Sri Lanka. Fellowship, 85(2), 33-36.

Stewart, J. (2019). Anti-Muslim hate speech and displacement narratives: Case studies from Sri Lanka and Australia. Australian Journal of Social Issues, 54(4), 418-435.

Zameera, F. (2022). Inadequate Legislation on Hate Speech: Critical Analysis of Sri Lankan Context. Jus Corpus LJ, 3, 366.

Inclusive Development Alternative Solutions (IDEAS) (2019). Young People Countering Hate Speech on Social Media in Sri Lanka. Rapid Context Assessment Report, by Search for common Ground–Sri Lanka