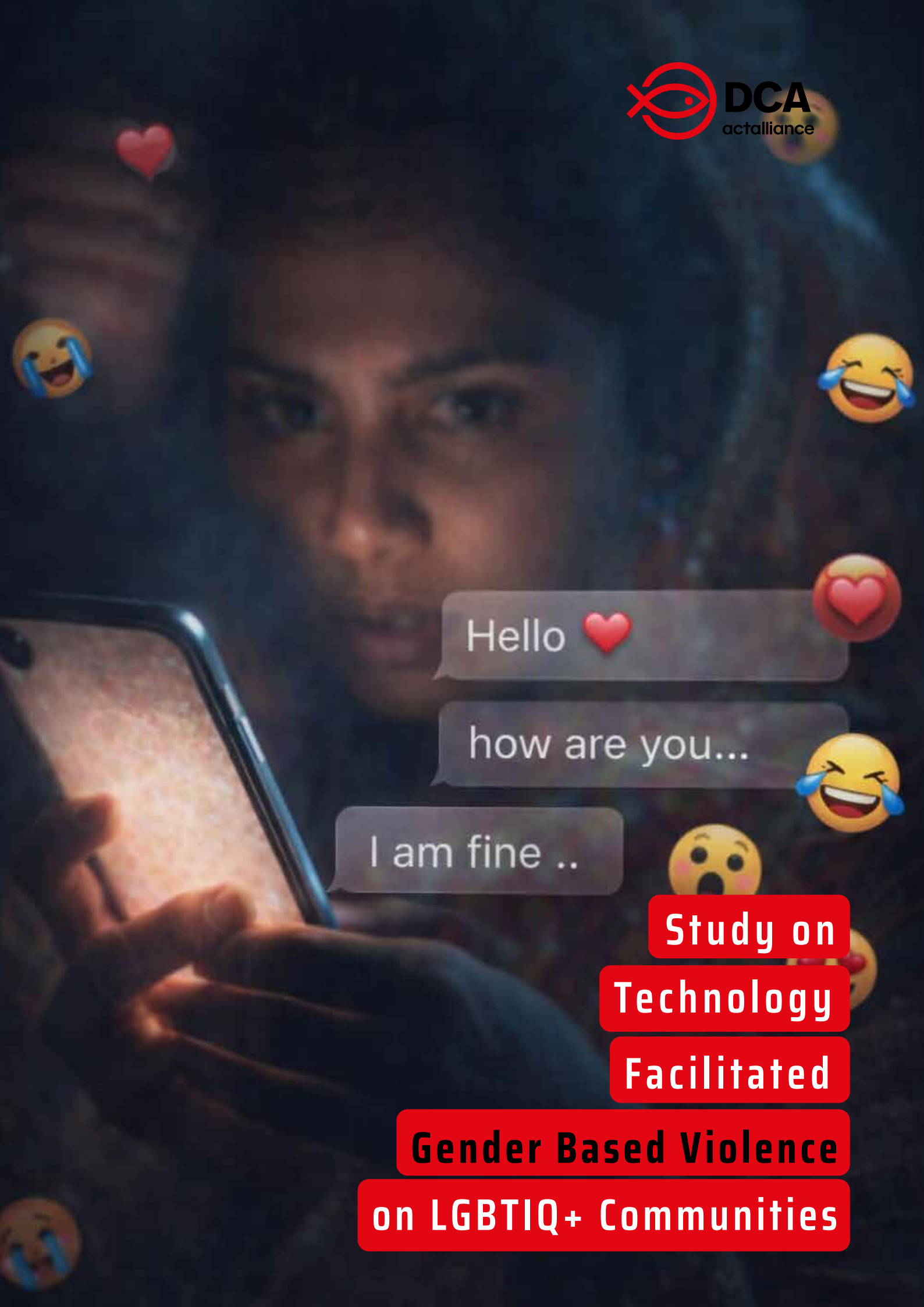


Study on Technology Facilitated Gender Based Violence on LGBTIQ+ Communities

Published by
DanChurchAid (DCA) Nepal

Technical Team: Manjil Sherchan, Surya Kumari Sunar, Sarah Alamri and Samjhana Bista

Citation
DCA. (2026). Technology Facilitated Gender Based Violence on LGBTIQ+ Communities in Nepal.

Acknowledgement
We would like to thank you the government representatives, all respondents and participants in the questionnaire survey, key informant interviews and focus group discussions including those who participated in this study from Janakpur (Madhesh Province), Bhairahawa (Lumbini Province) and Kathmandu (Bagmati Province).

ABBREVIATIONS

BDS	Blue Diamond Society
CSO	Civil Society Organisations
DCA	DanChurchAid
ETA	Electronic Transactions Act of Nepal
FGD	Focus Group Discussion
FGSMN	Federation of Gender and Sexual Minorities Nepal
FIR	First Incident Report
GBV	Gender Based Violence
HRW	Human Rights Watch
ILGA	International Lesbian, Gay, Bisexual, Trans and Intersex Association
IT	Information Technology
KII	Key Informant Interview
LGBTIQ+	Lesbian, Gay, Bisexual, Transgender, Intersex, Queer, and other identities
MOWCSC	Ministry of Women, Children, and Senior Citizens
NCII	Non-consensual sharing of intimate imagery
NHRC	National Human Rights Commission
OHCHR	Office of the United Nations High Commissioner for Human Rights
SOGIESC	Sexual Orientation, Gender Identity and Expressions Sex Characteristics
TFGBV	Technology Facilitated Gender Based Violence
UN	United Nations

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Technology-Facilitated Gender-Based Violence (TFGBV) has emerged as a pervasive yet under-recognised form of harm in Nepal's rapidly digitising society. For LGBTIQ+ communities, digital spaces serve as essential platforms for connection, identity expression, livelihood, and access to information. However, these same spaces expose users to harassment, blackmail, impersonation, non consensual image sharing, and most significantly, threats of outing. Despite Nepal's constitutionally progressive protections for gender and sexual minorities, social stigma, family rejection, and gaps in digital rights legislation heighten vulnerability and suppress help seeking.

DanChurchAid (DCA) commissioned this study to understand how LGBTIQ+ individuals experience TFGBV, the contexts that shape these harms, and the extent to which existing systems-legal, institutional, community-based offer safety. The study maps the "digital-social continuum" in which online violence is inseparable from offline discrimination, economic exclusion, and identity-based stigma.

A mixed-methods research design, combining qualitative and quantitative approaches were used to examine TFGBV as experienced by LGBTIQ+ communities in Nepal. Qualitative methods include six Focus Group Discussions (FGDs) in Janakpur (Madhesh Province) and Bhairahawa (Lumbini Province) and seven Key Informant Interviews (KIIs) in Kathmandu (Bagmati Province). The provinces were selected to capture diversity in LGBTIQ+ communities and to reflect Nepal's widest variation in literacy, digital access, social norms, and service ecosystems, factors that strongly shape TFGBV risk, reporting safety, and access to support. These qualitative findings were complemented by a cross-sectional quantitative survey, which captured broader patterns related to digital platform use, exposure to online abuse, perceived safety in digital spaces, and awareness of relevant policies and support mechanisms. The quantitative survey included 79 LGBTIQ+ respondents from multiple provinces of Nepal, as self-reported in the survey dataset, allowing for a broader geographic spread than the qualitative component. The study followed a descriptive and intersectional analytical approach, recognising that experiences of TFGBV are shaped by intersecting factors such as sexual orientation, gender identity, and geographic location. The analysis applied an intersectional, survivor-centred lens, emphasising confidentiality, informed consent, and triangulation of data.

Key Findings

1. Pervasive but Normalised Violence: TFGBV is a near-universal experience for the community, with 85.7% of respondents reporting lifetime exposure. However, a significant "awareness gap" exists; while victims experience harm, only 37.1% were familiar with the formal term "TFGBV." Violence is often minimised as a routine consequence of being LGBTIQ+ in Nepal, particularly when digital abuse is perceived as "lesser" than physical violence.

2. Outing as a Weapon: The most potent form of digital harm identified is the threat of non-consensual disclosure of SOGIESC, colloquially referred to as outing. Perpetrators leverage the non-acceptance of their identities by the family and society to silence victims. For many, the risk of digital visibility triggering offline family rejection or homelessness is the primary factor driving self-censorship and withdrawal from digital spaces.

3. Intra-Community Volatility: In a significant departure from traditional GBV narratives, 23.2% of perpetrators were identified as members of the LGBTIQ+ community. Due to the social taboo surrounding same-sex domesticity, relationships are often precarious; upon dissolution, digital platforms become sites for "revenge" through blackmail or the sharing of intimate images.

4. Institutional Distrust and the 2% Reporting Gap: There is a profound failure of formal redress mechanisms. While harassment is rampant, only 2% of victims reported to the police. FGDs revealed that law enforcement is viewed as a source of secondary victimisation characterised by transphobia, ridicule, and a lack of legal sensitivity rather than a site of justice.

5. Digital Spaces for “Community”: Despite the risks, digital platforms are essential "breathing spaces" for solidarity and income. For trans-women in particular, online spaces are critical for livelihoods, creating a "double bind" where they cannot dis-engage from harmful environments without sacrificing economic survival.

6. Critical Gaps in Current Systems:

- Legal Invisibility: Nepal lacks a specific legal definition for TFGBV. Existing laws, like the Electronic Transactions Act (2008), are binary and often weaponised against the very marginalised groups they should protect.
- Capacity Constraints: Civil society organisations (CSOs) are the primary responders but lack the technical digital security expertise, legal aid funds, and standardised case management systems to manage high-risk TFGBV cases effectively.
- Platform Neglect: Reporting tools are perceived as "whack-a-mole" solutions, failing to address persistent harassment or provide local-language moderation that understands the nuances of Nepali queer identities.

Strategic Recommendations

- Legal Reform: Advocate for the inclusion of SOGIESC-sensitive definitions in upcoming cyber laws and the decriminalisation of anonymity, which is a survival tool for queer individuals.
- Institutional Sensitisation: Implement mandatory SOGIESC and digital rights training for the Cyber Bureau and frontline police officials to bridge the trust gap.
- Community-Oriented Protection: Invest in "Digital First Aid" kits and dedicated legal funds for CSOs to move beyond emotional support toward formal accountability.
- Family-Level Interventions: Programmes must address the root cause of digital vulnerability and family-based transphobia to reduce the power of "outing" as a weapon.

This study is the first comprehensive examination of TFGBV affecting LGBTIQ+ communities in Nepal. It provides robust evidence that digital violence is a structural, not incidental, phenomenon shaped by identity-based discrimination and legal invisibility. The findings offer a blueprint for legal reform, institutional strengthening, and community-centred protection. Ensuring safer digital participation for LGBTIQ+ individuals is essential not only for their rights and wellbeing, but also for Nepal’s broader commitments to an inclusive, rights-respecting digital future.

Chapter 1: Introduction

1.1 Background

Technology-Facilitated Gender-Based Violence (TFGBV) is an emerging concern in Nepal's digital landscape. TFGBV exists as a continuum of violence[1] which covers rampant online abuses from hate speech, cyberstalking, doxxing, non-consensual sharing of intimate images (NCII), extortion by/for sexual contact (sextortion), and specifically for LGBTIQ+ communities in the form of "outing"- exposing their sexual/gender identity to others without consent. These acts often escalate in their harms and directly facilitate physical attacks, and in the case of jurisdictions where same-sex relationships and people with diverse sexual orientation, gender identity or expression, and sex characters (SOGIESC) are criminalised, may even lead to state persecution[2]. The violence and discrimination faced by LGBTIQ+ individuals in the digital space is merely the reflection of the patterns of violence and discrimination they have been facing in our society at large[3]. The lack of recognition or understanding of TFGBV to have the same gravity as any other form of GBV usually until it escalates to physical or economic harm - minimises and allows these violent cycles to persist[4].

Nepal, despite having one of the most progressive laws in Asia for LGBTIQ+ inclusion[5], continues to be influenced by the patriarchal social and legal structures. Binary approaches to legal drafting and interpretation have disproportionately left LGBTIQ+ populations vulnerable. Despite the Constitution of Nepal (2015) explicitly prohibiting discrimination based on sexual orientation and gender identity, there remain significant gaps in policy and enforcement. The policies that do exist also exist in a punitive criminal justice system that comes into action only to "punish" perpetrators after any harm has occurred and does not take a victim-centric approach for prevention and mitigation of harm. Consequently, LGBTIQ+ victims often encounter stigma or insensitive treatment when seeking help, leading to low reporting rates and a general distrust of formal justice mechanisms.

In this context, DanChurchAid (DCA) commissioned a comprehensive study to document the nature of TFGBV among LGBTIQ+ communities and to identify strategies for improving their digital safety and rights. The study sought to understand the perspectives and experience of LGBTIQ+ individuals and communities in the digital space, and how their lived experiences compare to the legal realities of Nepal.

1.2 Objectives

The objectives of the study were as follows:

- Assess the status of TFGBV in LGBTIQ+ communities in Nepal, and document the common forms of technology-facilitated abuse encountered by LGBTIQ+ individuals, their prevalence, and the contexts/platforms in which they occur. This includes understanding the severity and range of online threats or harassment faced by sexual and gender minorities.

- Identify gaps, challenges, and opportunities in exercising digital rights for LGBTIQ+ individuals. Examine the factors that hinder or enable LGBTIQ+ individuals to access and use digital spaces safely. This involves identifying key challenges (such as inadequate legal protections, low digital literacy, social stigma, or lack of trust in reporting mechanisms) as well as any supportive practices or

1. Baekgaard, Kristine. Technology-Facilitated Gender-Based Violence. Georgetown Institute for Women Peace and Security.
2. Ibid.
3. Body & Data. "Identities Experiencing Internet: Nepal Survey Report" Body & Data, 2021.
4. Body & Data. "Mapping Laws Relevant to Online Violence in Nepal" Body & Data, 2021.
5. ILGA Asia. "Nepal: Marriage Registration for Same-Sex Couples after Seminal Court Ruling – ILGA ASIA." Ilgaasia.org, July 2024.

resources (for instance, community support networks, helplines, or safe online platforms) that could be leveraged to improve online safety.

- Recommend interventions to enhance digital safety and digital rights of LGBTIQ+ individuals/community. These include policy or legal reforms, capacity-building activities (e.g. digital security training for community members), advocacy campaigns, or community-led initiatives that address TFGBV and promote a safer online environment for LGBTIQ+ individuals in Nepal.

1.3 Literature Review

Patriarchal social structures and colonial-era legal legacies have persisted across the South Asian Region, with national penal codes and biased legal structures being instrumentalised against LGBTIQ+ individuals and systematically marginalising sexual and gender minorities. A Kerala High Court decision in 2025 stated that families can be a place of violence for LGBTIQ+ individuals ; research shows that heteronormative and cisgender standards within family and community units in the region has often led to either invisibilisation or "corrective" disciplinary methods like forced marriage, psychological coercion, and "honour-based abuse" being reinforced against LGBTIQ+ youths and adults. The lack of gender-neutral language in domestic violence laws across India, Bangladesh, Nepal, and Sri Lanka often leaves victims without formal legal recourse, as protection frameworks are typically designed around a cis-heteropatriarchal societal expectations. Intersectional studies further show that trans and gender-diverse individuals, particularly those from marginalised castes or religious minorities, face the most severe forms of violence, that spans both digital and physical geographies.

Digital harm does not exist in a vacuum; it is an extension of structural patriarchal violence that persists in the society. Literature on TFGBV traditionally frames these harms in the patterns of violence faced by women with digital spheres replicating the traditional gender hierarchies which weaponise digital platforms and tools to control the behaviours of women, and by extension any gender marginalised group, in the digital spheres. UN Women has characterised TFGBV as a tool of "silencing" to restrict women's exercise of their basic rights like freedom of expression and public participation in "digital squares".

The marginalisation faced by LGBTIQ+ population borrows similar narratives of "gender-based" discrimination but has an increased dimension of the violence also being tied to the lack of recognition of their "identity" itself. While the foundational drivers, power imbalances and discriminatory norms remain identical, the manifestations for queer individuals include distinct "identity-based" harms. For instance, Baekgaard (2023-2024) seeks to expand the principle of bodily autonomy to include "identity autonomy," specifically addressing the non-consensual "outing" of a victim's orientation or gender status. Self-identification and exploration of their identity is an important part of queer identity formation[15] and violence can occur as a constant denial of their lived identity as well as exposure of said identity without their consent. In societies where

6. OHCHR. 'LGBTIQ women' OHCHR.
7. SCC Times. 'Sexual orientation an innate part of identity of LGBTQ+ persons': Kerala HC upholds Right of choice and Right to live life of a queer woman'. June 2024.
8. The University of Melbourne & UNFPA. "Understanding technology-facilitated gender-based violence in Asia: A qualitative study" UNFPA. 2024.
9. Equality Now. "Sexual violence in South Asia: Legal and other barriers for justice to victims" Equality Now. 2021.
10. Baekgaard, Kristine. Technology-Facilitated Gender-Based Violence. Georgetown Institute for Women Peace and Security.
11. Body & Data (2021). "Mapping Laws Relevant to Online Violence in Nepal" Body & Data, 2021.
12. UN Women (2023). "Evidence to Action: Addressing Violence Against LGBTIQ+ People in Nepal." UN Nepal, 2023.
13. Kasa, Luvo (2025). "Tradition or Oppression? The Role of Cultural Norms in Sexual Violence against Queer Communities." Edelweiss Applied Science and Technology, vol. 9, no. 8, Aug. 2025, pp. 822–29.
14. Baekgaard, Kristine (2023-2024). Technology-Facilitated Gender-Based Violence. Georgetown Institute for Women Peace and Security. \
15. Body & Data. "Identities Experiencing Internet: Nepal Survey Report" Body & Data, 2021.

LGBTIQ+ identities are still criminalised and/or have low social acceptance, the consequences of outing can result in immediate physical danger, loss of livelihood, familiar rejection to criminal prosecution in more hostile environments. A 2023 Human Rights Watch study on Non-consensual Intimate Image (NCII) and sexual extortion has explored how perpetrators and states weaponise social stigma and "morality" codes to target those whose identities are marginalised by the state or society in some countries (for example in MENA region), including by police themselves posing as queer individuals online to arrest.

Civil society Organisations (CSOs), such as Body & Data, have documented how TFGBV functions as a tool to control women's digital autonomy, often leading to "digital chilling effects" where victims withdraw from the public sphere to avoid social stigma. Current international standards, such as the Yogyakarta Principles, advocate for the right to use the internet and communications technology without fear of identity-based violence, yet these are seldom codified into domestic statutes that treat digital privacy as a generic, rather than gendered, right. In Nepal, literature on TFGBV highlights a critical disconnect between the outdated Electronic Transactions Act (2008) and the evolving nature of digital harm (such as the Record Nepal , 2022; UNESCO, 2025).

The framework for platform accountability remains fragmented and voluntary. While this study does not delve into the intricacies of digital platforms and accountability measures, it needs to be noted that the UN Guiding Principles on Business and Human Rights (UNGPs) require tech companies to respect basic human rights. There is, however, no binding international law to enforce this. Consequently, LGBTIQ+ users are often left at the mercy of algorithms that fail to recognise queer-coded hate speech or prioritise the removal of outing- related content, leaving them in a state of digital and physical precarity. For example, in January 2025, Meta revised its content moderation policies to allow discriminatory statements labelling LGBTIQ+ individuals as "mentally ill" . In contrast, proposed domestic regulatory efforts in Nepal – such as Social Media Bill- have primarily focused on policing online expression end-user level . These proposals have faced significant criticism and received backlash from CSOs and the broader public.

This study found a distinct lack of literature on how LGBTIQ+ identities and movements are not a singular marginalised identity, but exist as an alliance of multiple distinct yet intersecting identities; the nuances of their online experiences differ. Paudel and Kayastha (2023) state that the political climate around privacy related regulations homogenises the experiences of marginalised people and undermines their lived experiences and highlight a distinct need to centre the rights and consent of the people when implementing regulations for digital spaces. As technologies evolve and the use-cases for digital platforms and services evolve, the gaps in policy get more apparent; the Government of Nepal is still relying on legislation from 2008 to prosecute TFGBV cases. Adapting these principles for LGBTIQ+ community necessitates an intersectional shift that expands the "gender-based" lens to encompass sexual orientation and gender identity.

16. Human Rights Watch. "All This Terror Because of a Photo": Digital Targeting and Its Offline Consequences for LGBT People." HRW, 2023.
17. Body & Data. "Mapping Laws Relevant to Online Violence in Nepal" Body & Data, 2021.
18. International Commission of Jurists (ICJ. Yogyakarta Principles - Principles on the application of international human rights law in relation to sexual orientation and gender identity, 2007.
19. The Record (2022). Addressing Gender Violence in Cyberspace. ecordnepal.com/addressing-gender-violence-in-the-cyberspace. Retrieved on 27 Feb 2026.
20. UNESCO (2025). Strengthening Digital Safety for Nepali Women: Addressing Technology-facilitated gender-Based Violence. https://www.unesco.org/en/articles/strengthening-digital-safety-nepali-women-addressing-technology-facilitated-gender-based-violence. Retrieved on 27 Feb 2026.
21. UN OHCHR. Guiding Principles on Business and Human Rights. United Nations, 2011.
22. Torek, Belle. "Meta's New Policies: How They Endanger LGBTQ+ Communities and Our...." HRC, 15 Jan. 2025.
23. UNESCO. "Social Media Bill 2081: Legal Analysis" 2025.
24. Paudel, Shambhawi and Shubha Kayashta (2023). "Privacy in the Digital Age and as Understood by Marginalized Groups in Nepal" 2023.

Chapter 2: Research Methodology

2.1 Study Design and Approach

This study adopted a mixed-methods research design, combining qualitative and quantitative approaches to examine technology-facilitated gender-based violence (TFGBV as experienced by LGBTIQ+ community in Nepal. Qualitative methods including Focus Group Discussions (FGDs) and Key Informant Interviews (KIIs) were employed to generate in-depth insights into lived experiences, perceptions, coping strategies, and institutional responses to TFGBV. These qualitative findings were complemented by a cross-sectional quantitative survey, which captured broader patterns related to digital platform use, exposure to online abuse, perceived safety in digital spaces, and awareness of relevant policies and support mechanisms.

The study followed a descriptive and inter-sectional analytical approach, recognising that experiences of TFGBV are shaped by intersecting factors such as sexual orientation, gender identity, and geographic location. A participatory orientation was adopted to ensure that the perspectives of LGBTIQ+ individuals informed key stages of the research process, including the development of data collection tools and the interpretation of findings, thereby grounding the analysis in lived realities.

The research was guided by a rights-based and survivor-centred framework, with careful attention to issues of safety, confidentiality, and informed consent. Rather than seeking to estimate prevalence, the study aimed to identify patterns of experience, institutional gaps, and structural barriers affecting prevention, reporting, and access to redress. In recognition of the documented mistrust between LGBTIQ+ communities and formal institutions, the analysis also considered how past experiences with authorities influence reporting behaviours and coping strategies.

Findings were triangulated across data sources to enhance analytical rigor, and all research activities adhered to established ethical and do-no-harm principles.

2.2 Study Locations and Population

Primary qualitative data were collected through FGDs conducted in Janakpur (Madhesh Province) and Bhairahawa (Lumbini Province). The provinces were selected to capture diversity within the LGBTIQ+ community and to reflect Nepal's widest variation in literacy, digital access, social norms, and service ecosystems, factors that strongly shape TFGBV risk, reporting safety, and access to support. KIIs were conducted in Kathmandu, reflecting the concentration of national-level state institutions and civil society organisations engaged in digital rights, LGBTIQ+ rights, and protection mechanisms. The quantitative survey included respondents from multiple provinces of Nepal, as self-reported in the survey dataset, allowing for a broader geographic spread than the qualitative component.

The study population included:

- LGBTIQ+ individuals aged 18 years and above who actively use digital platforms
- Representatives of CSOs working on LGBTIQ+ rights, digital rights, and gender-based violence
- Representatives of relevant state institutions involved in digital governance, protection, and human rights.

2.3 Sampling and Participant Profile

A purposive sampling strategy was employed for qualitative data collection to ensure inclusion of participants with relevant lived experience of digital engagement and exposure to online risks.

Focus Group Discussions (FGDs)

A total of six FGDs were conducted:

- **Janakpur:** Three segregated FGDs: one with trans women, one with gay participant, and one with lesbian participant
- **Bhairahawa:** Three FGDs with mixed LGBTIQ+ participants

Each FGD included 7–8 participants. All participants were 18 years or older, with the majority being below 35 years of age. Participant profiling was intentionally limited to broad age categories to reduce risks of identification.

Key Informant Interviews (KIIs)

A total of seven KIIs were conducted with representatives from CSOs and state institutions.

Quantitative Survey Respondents

The quantitative survey included 79 respondents, all of whom:

- Confirmed being 18 years or older
- Self-identified as part of the LGBTIQ+ community

The survey sample is not statistically representative and is used to illustrate patterns and perceptions rather than population-level estimates.

2.4 Data Collection Methods

2.4.1 Focus Group Discussions (FGDs)

FDGs were conducted to explore:

- Patterns of digital use
- Positive and negative online experiences
- Community understanding of TFGBV
- Coping strategies and informal support mechanisms
- Barriers to report and seeking redress

FGDs in Janakpur were conducted in Maihtili, while those in Bhairahwa were conducted in Nepali. Each FGD lasted approximately for an hour. All FGDs were audio recorded and facilitated using a semi-structured discussion guide.

2.4.2 Key Informant Interviews (KIIs)

KIIs were conducted with the following institutions:

- Cyber Bureau
- Blue Diamond Society
- Federation of Sexual and Gender Minorities Nepal
- Body and Data
- Digital Rights Nepal
- Ministry of Women, Children and Senior Citizens
- National Human Rights Commission

Of the seven KIIs, four were conducted in person, two online, and one by phone. Interviews lasted 30–45 minutes on average and were conducted in Nepali. KIIs explored institutional perspectives on TFGBV trends, response mechanisms, policy implementation challenges, and coordination gaps between state and non-state actors.

2.4.3 Quantitative Survey

A cross-sectional quantitative survey was conducted to complement qualitative findings and capture broader patterns related to TFGBV among LGBTIQ+ communities in Nepal. The survey included 79 respondents from multiple provinces. Out of all respondents, the highest participation was from Lumbini Pradesh (30 respondents, 42.86%), followed by Bagmati Pradesh (16 respondents, 22.86%) and Madesh Pradesh (18 respondents, 25.71%). Smaller proportions of respondents were from Gandaki Pradesh (4 respondents, 5.71%) and Sudurpaschim Pradesh (2 respondents, 2.86%). The questionnaire consisted primarily of closed- ended questions, including Likert-scale and multiple-choice items. Key thematic areas covered:

- Digital platform usage
- Experiences and forms of online abuse
- Perceived safety in digital spaces
- Awareness of policies, social attitudes, and support mechanisms related to TFGBV

Informed consent was obtained at the outset of the survey, and participation was fully voluntary. The survey was designed to produce descriptive insights rather than statistically generalisable findings.

2.4.4 Desk Review

A desk review was undertaken to contextualise the primary findings within relevant legal, policy, and research frameworks. Key sources included existing and proposed legislation in Nepal, as well as applicable international human rights treaties and principles. The review also encompassed academic literature, CSO reports and selected blogs and writings from LGBTIQ+ individuals that critically reflect their lived experiences online. A comprehensive bibliography with all the reference materials is provided in Annex-1.

The desk review covered materials from the last 10 years, with particular emphasis on the most recent five years, reflecting the evolving nature of digital risks and policy responses. Specific legal instruments are discussed in the findings chapter where relevant.

2.5 Data Analysis Framework

All FGD and KII recordings were fully transcribed, and qualitative data were analysed using thematic analysis. This involved iterative coding to identify recurrent patterns, divergences, and cross-cutting themes related to TFGBV, digital rights, and institutional responses. Coding was conducted by the lead researcher with support from the research team, with internal cross- checking of a subset of transcripts to ensure consistency and reliability in interpretation. Where required, qualitative data were translated to ensure accuracy and coherence in analysis.

Quantitative survey data were analysed using descriptive statistical methods, focusing on frequencies and response patterns across key variables. Analysis was conducted using standard data analysis tools (python) to generate summary tables and, where sample size permitted, basic disaggregation by selected sub-groups (such as age group or gender identity) to identify indicative patterns. No inferential or causal analysis was undertaken, and findings are presented as descriptive rather than representative.

A concurrent mixed-methods analytical approach was employed, enabling qualitative and quantitative findings to be analysed in parallel and subsequently integrated through triangulation. This approach facilitated comparison and cross-validation across community narratives, survey patterns, and institutional perspectives, thereby reducing reliance on any single data source and strengthening the overall robustness of the findings.

The analysis was informed by an intersectional lens, examining how overlapping identities and contexts such as gender identity, sexual orientation, and geographic location shape experiences of TFGBV, access to support, and reporting behaviours. Particular attention was paid to themes related to mistrust in formal institutions, barriers to reporting, impacts on mental health and behaviour, and community-based coping and support mechanisms. Throughout the analytical process, findings were continually assessed against the study objectives to ensure relevance and coherence. An internal validation process was undertaken to review preliminary interpretations and ensure analytical rigor. This validation focused on consistency across data sources and alignment with documented lived experiences, contributing to the credibility and robustness of the findings.

By integrating qualitative narratives with quantitative patterns, the mixed-methods approach enabled a nuanced understanding of TFGBV affecting LGBTIQ+ communities in Nepal. The methodology, refined during the inception phase in consultation with DCA, supports an analysis that captures both the depth of lived experience and the broader contours of the issue, while adhering to ethical, trauma-informed, and do-no-harm principles.

2.6 Ethical Considerations and Safeguarding Measures

The study followed ethical and safeguarding protocols appropriate for research involving violence and marginalised populations. While no formal external ethics approval was obtained, ethical protocols were adhered to throughout the research process.

Key measures included:

- Written informed consent for FGDs and verbal consent for KIIs
- Clear communication regarding voluntary participation, the right to withdraw, and confidentiality
- Anonymisation of all participant data
- Avoidance of personally identifiable information
- Use of participant-led and non-coercive questioning techniques

No formal referral pathways were shared with the participants. However, the facilitators conducted discussions with care and sensitively to minimise distress and mitigate the risk of re-traumatisation.

2.7 Limitations of the Study

This study has several limitations. Findings are not statistically generalisable, as the research prioritises qualitative depth and descriptive insight over representativeness. Experiences of TFGBV may be underreported due to stigma, fear of exposure, or normalisation of online abuse. The quantitative survey is subject to self-reporting bias and excludes individuals without access to digital technologies.

Additionally, the rapidly evolving nature of digital platforms means that risks, practices, and policy responses may change beyond the study period. Despite these limitations, the study provides robust, contextually grounded insights into TFGBV affecting LGBTIQ+ communities in Nepal and identifies critical gaps in policy, protection, and institutional response.

Chapter 3: Digital Ecosystem and Online Presence of LGBTIQ+ Communities

This chapter examines how LGBTIQ+ individuals engage with digital technologies, the purposes these engagements serve, and the ways in which digital spaces function as sites of visibility, opportunity, and risk. The findings draw on FGDs conducted which were triangulated with results from a cross-sectional quantitative survey with 79 respondents. The analysis prioritises patterns and lived experiences rather than population level prevalence, reflecting the diverse social, geographic, and identity contexts shaping digital engagement.

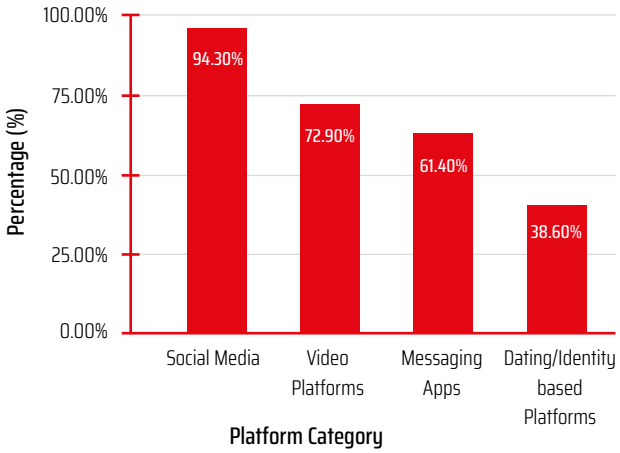
Digital spaces hold particular significance for LGBTIQ+ communities in Nepal due to limited access to safe physical spaces, persistent stigma within families and communities, and uneven trust in formal institutions. For many participants, online platforms fill gaps left by social, familial, and state systems, becoming central spaces for connection, information, and survival rather than optional or recreational environments.

3.1 Patterns of Internet and Platform Usage

Both qualitative and quantitative findings indicate that LGBTIQ+ individuals are frequent users of the internet and engage across multiple digital platforms on a regular basis. Participants across all FGDs characterised internet use as deeply embedded in everyday life, serving as a critical medium for communication, entertainment, information access, and social interaction.

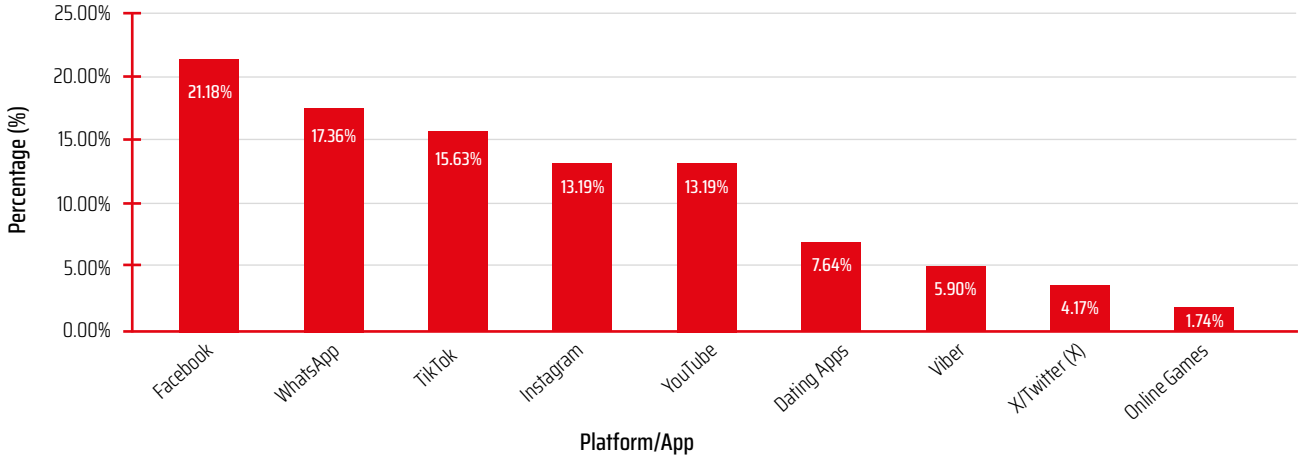
Survey findings confirm a high level of digital engagement across multiple online platforms. Social media dominates weekly usage patterns, with 94.3% of respondents reporting use of social media platforms, followed by video platforms at 72.9% and messaging applications at 61.4%. A considerable proportion of respondents also reported using dating or identity-based platforms (38.6%), highlighting exposure to more private and interaction-driven digital spaces. In terms of specific applications, Facebook was the most frequently used platform (61 respondents; 21.18%), followed by WhatsApp (50; 17.36%), TikTok (45; 15.63%), and Instagram and YouTube (38 each; 13.19%). Usage of dating apps such as Grindr, Tinder, and similar platforms was also notable (22; 7.64%), alongside Viber (17; 5.90%) and X/Twitter (12; 4.17%), while online gaming platforms were least reported (5; 1.74%). Overall, the findings indicate that respondents are highly active across mainstream social platforms, messaging channels, and video-based applications spaces where technology-facilitated risks are also increasingly prevalent.

Figure 1: Digital Platform Use by Functional Category (%)



Source: Questionnaire Survey, 2026

Figure 2: Weekly Use of Online Platforms and Apps Among Respondents



Source: Questionnaire Survey, 2026

FGD discussions suggest that these patterns of use are shaped not only by individual preference but also by platform dominance and accessibility. Mainstream platforms such as Facebook and TikTok were described as difficult to avoid because they are central to social life and information exchange. Messaging applications were generally used for more private communication, while dating applications were used to connect with others sharing similar sexual orientations or gender identities.

Participants consistently reported using multiple platforms at the same time, with each platform serving a distinct purpose. This layered digital engagement reflects both opportunity and constraint. While digital spaces expand possibilities for connection, participants described navigating them cautiously due to persistent exposure to harassment, monitoring, and misuse of personal information.

Alongside these patterns, participants in Bhairahawa described similar strategies for managing identity across platforms, particularly distinguishing between public facing social media and dating applications. As one participant explained,

"On Facebook we use our real names, but on dating apps we use nicknames. Some of us keep two accounts, one for family and one for the LGBTIQ+ community." (FGD participant, Mixed group, Bhairahawa)

Dating applications emerged as a particularly complex part of this digital ecosystem. Across both Janakpur and Bhairahawa, participants described dating apps as necessary for meeting others with similar identities, especially in contexts where offline spaces for LGBTIQ+ socialisation are limited or absent. At the same time, these platforms were frequently associated with harassment, coercion, blackmail, and threats of outing. Survey data indicate that while approximately one third of respondents regularly use dating applications, a substantially larger proportion reported negative online experiences. This disparity suggests that continued use is driven more by limited alternatives than by perceptions of safety.

A comparative analysis of the two study locations indicates contextual variation in the experience of digital engagement. Participants in Janakpur more frequently described family monitoring of phones and online activity, contributing to more restrictive patterns and heightened fearsof exposure. In Bhairahawa, participants reported comparatively greater discretion and mobility, although

experiences of online harm were broadly similar across both locations. These findings underscore the influence of local social norms and environments in shaping digital behaviour.

As one participant from Janakpur explained,

"We have two accounts, one for our family as a man, and one where we show who we really are."

(FGD participant, Trans woman, Janakpur)

3.2 Purpose of Online Engagement

FGD participants consistently highlighted that digital platforms serve critical social and emotional functions in their lives. Online spaces were described as enabling connection with peers, exploration and expression of sexual orientation and gender identity, and access to a sense of belonging that is often unavailable in offline family or community environment. This section examines the positive roles that digital technologies play in the lives of LGBTIQ+ individuals, highlighting how online spaces enable connection, identity expression, access to information, and mutual support. Drawing on survey findings, FGDs, and KIIs, it focuses on the ways technology functions as an enabling and protective means, particularly in contexts where offline spaces remain restrictive or unsafe.

Survey findings indicate that digital platforms are a primary means through which LGBTIQ+ individuals access community and social connection. Engagement with online platforms was widespread: 94.3% of respondents reported using social media platforms, 61.4% used messaging applications, and 38.6% used dating or identity-based applications. This high level of engagement reflects the central role of online spaces in maintaining relationships, forming peer networks, and reducing social isolation.

FGD participants across Janakpur and Bhairahawa consistently described online platforms as spaces where they could connect with others who share similar identities and experiences connections that are often unavailable offline. Participants emphasised that digital spaces help counter feelings of isolation, particularly for individuals who are not open about their identity within their families or communities.

"Online, we can finally talk to people who understand us. Offline, that space does not exist."

(FGD participant, Janakpur)

"Through the phone, we feel less alone. We know others like us are there."

(FGD participant, Bhairahawa)

Qualitative findings further highlight that digital spaces provide important opportunities for self- expression and emotional affirmation. Survey data show that a substantial proportion of respondents engage with platforms that allow selective identity presentation, including dating and identity-based applications (38.6%), indicating that online environments enable exploration of identity and relationships in ways that are constrained offline. Participants described online platforms as environments where they could express their gender identity, explore language and terminology, and receive validation from peers. For many, these spaces offered the first opportunity to encounter positive representations of LGBTIQ+ identities and to articulate their own experiences.

FGDs also revealed that online peer networks function as informal support systems. Participants described turning to online friends or groups during moments of distress, uncertainty, or personal crisis, particularly when offline support was unavailable or unsafe.

"Online, we can be ourselves. We don't have to explain everything."

(FGD participant, Trans woman, Janakpur)

Survey and qualitative data further show that digital technologies are an important source of information related to health, rights, and services. High engagement with social media (94.3%) and messaging applications (61.4%) suggests that these platforms function as key channels for sharing information and advice. Participants reported using online spaces to access information on sexual and reproductive

health, mental health, legal rights, and LGBTIQ+-friendly services. KIIs reinforced this finding, noting that digital platforms often serve as the first point of contact for information and referrals, particularly for individuals living outside urban centres where offline services may be limited or inaccessible. Participants emphasised that anonymity and privacy in online spaces make it easier to seek sensitive information without fear of immediate judgement or exposure.

"We search online first, because asking in real life is not safe."

(FGD participant, Bhairahawa)

Collectively, these findings demonstrate the central enabling function of digital in the lives of LGBTIQ+ individuals. Digital environments facilitate social connection, identity exploration and expression, access to affirming information, and emotional support. In many cases, they operate as comparatively safer, more accessible or more affirming alternatives to offline environments. Acknowledging these positive dimensions is analytically important for explaining sustained and active engagement with digital platforms, even in the presence of significant risks..

3.3 Digital Spaces as Sites of Visibility and Risk

Digital engagement among LGBTIQ+ individuals is characterised by active and strategic management of visibility. Across FGDs, participants described maintaining multiple digital identities to reduce risk. These included family-facing profiles aligned with socially acceptable gender norms, separate accounts used with trusted peers or partners, and anonymous or pseudonymous profiles, particularly on dating platforms.

Survey findings support this pattern. Only 51.4% of respondents reported using mostly real names and identities online. A further 31.4% reported using a mix of real and anonymous identities, while 14.3% relied primarily on anonymity. These figures indicate that online participation is widespread but carefully negotiated, reflecting efforts to balance connection with safety.

"Trans people cannot hide. That's why we are targeted more."

(FGD participant, Trans woman, Janakpur)

Both qualitative and quantitative findings indicate that increased visibility heightens vulnerability. Trans women and trans men were described as facing heightened exposure due to the difficulty of concealing gender expression, while gay and lesbians were sometimes able to reduce risk through concealment, often at significant emotional cost.

Survey data provide indicative support for this pattern. Nearly half of trans women respondents reported feeling unsafe online, and more than 90% reported having experienced online harassment or violence at least once. These dynamics illustrate how risk is unevenly distributed within LGBTIQ+ communities, shaped by gender identity, visibility, and social context rather than platform use alone.

Chapter Summary

This chapter explores how LGBTIQ+ individuals in Nepal use digital spaces and how technology creates both opportunities and risks. Findings show that online platforms are essential for connection, identity expression, and accessing information in a context shaped by stigma, discrimination, and social surveillance.

- Patterns of Digital Engagement: Survey findings indicate high level of internet use, primarily for communication and social interaction. Social media platforms were the most widely used (94.3%), followed by video-based platforms (72.9%) and messaging applications (61.4%). Among specific platforms, Facebook emerged as the most commonly used, followed by WhatsApp and TikTok. This reflects the central role of mainstream platforms in maintaining relationships, accessing information, and participating in both general and community-specific online networks.
- Identity Management and Online Safety Practices: Participants described actively managing their online presence to balance the need for connection with the risks associated with visibility. A common strategy involved

maintaining multiple accounts, including a public-facing profile aligned with family and societal expectations, and a private or pseudonymous account used to engage with LGBTIQ+ networks. This layered approach reflects the reality that digital spaces are closely connected to offline life, and that exposure online can carry profound consequences in family and community settings.

- Dating Applications as High-Risk but Necessary Platforms: Dating applications were used by 38.6% of respondents and were consistently described as both important and risky. Participants noted that dating apps offer one of the few accessible avenues to meet peers and explore relationships in a context where safe offline spaces are limited. At the same time, these platforms were repeatedly identified as high-risk environments where users are vulnerable to coercion, blackmail, harassment, and threats of outing. The findings suggest that dating applications occupy a particularly complex position, offering connection while also enabling severe forms of TFGBV.
- Geographic Context and Variations in Digital Risk: While the types of online harm reported were broadly similar across study sites, participants described differences in how digital risk is experienced and managed depending on local social context. In Janakpur, participants reported higher levels of family monitoring and stronger social surveillance, resulting in more cautious and restricted digital engagement. In Bhairahawa, participants reported comparatively greater mobility and discretion, factors that shaped how they navigated privacy and online spaces. These findings suggest that digital practices are not determined solely by platform architecture; rather, they are mediated bv local social norms, family dynamics, and the degree of community visibility.
- Digital Platforms as Key Sources of Information and Support: Across FGDs, participants emphasised that digital spaces serve as an essential source of emotional support, peer connection, and identity affirmation. Online platforms were also described as critical channels for accessing sensitive information related to sexual and reproductive health, mental wellbeing, legal rights, and queer-friendly services. For many participants, this information was considered difficult or unsafe to seek in offline settings due to stigma and fear of exposure.

Conclusion

Overall, the findings show that digital spaces function as environments of conditional safety for LGBTIQ+ individuals in Nepal. Online platforms provide vital opportunities for connection, belonging, and access to life-relevant information, but they also expose users to heightened risks of harassment, exploitation, and outing. As a result, participants are required to adopt deliberate and often exhausting strategies to manage visibility and protect themselves, highlighting the need for stronger safeguards and more inclusive digital and institutional protection systems.

Chapter 4: Experience of TFGBV

This chapter examines how LGBTIQ+ individuals experience TFGBV, how they understand and interpret such harm, and how it affects their emotional wellbeing, social relationships, and behaviour. The analysis draws on FGDs and is triangulated with findings from a cross-sectional quantitative survey of 79 respondents. Quantitative findings are used to illustrate patterns among respondents and to corroborate qualitative insights. They should not be interpreted as population prevalence estimates.

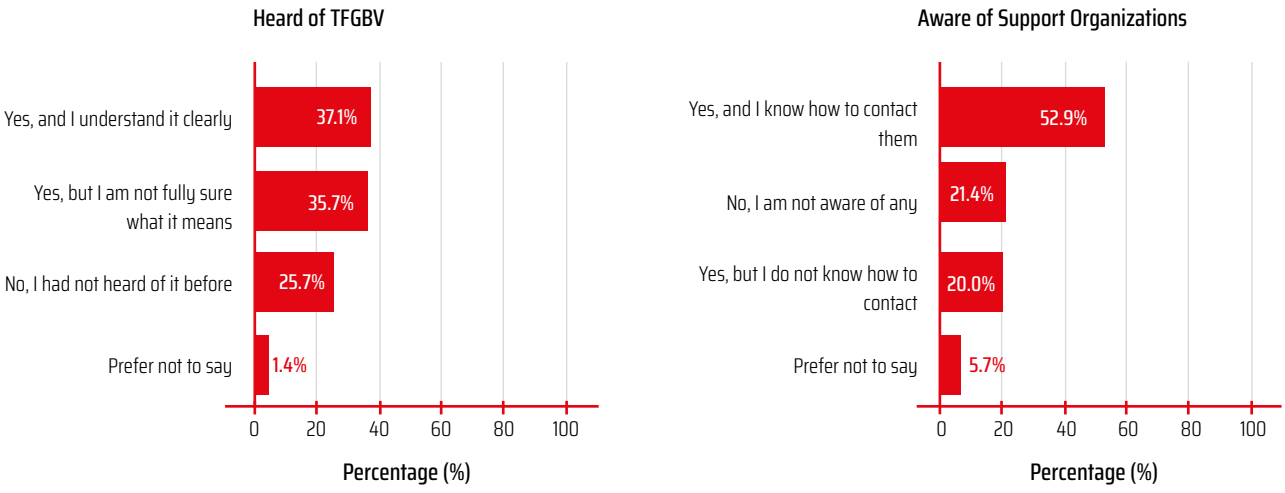
In this study, TFGBV is understood not as isolated incidents but as a continuum of behaviours that often unfold progressively. Participants described experiences that begin with harassment or unsolicited messages and escalate into threats, blackmail, impersonation, or outing. Online harm was frequently described as inseparable from offline consequences, particularly in contexts where exposure of sexual orientation or gender identity can lead to family rejection, violence, or loss of livelihood.

4.1 Community Understanding and Perceptions of TFGBV

Across FGDs, participants demonstrated a strong experiential understanding of TFGBV, even when formal terminology was unfamiliar. Harassment, sexualised messages, coercion, threats, blackmail, impersonation, and non-consensual image related harms were discussed as common and recognisable experiences. Participants emphasised that these acts are rarely perceived as isolated events and are often part of repeated patterns that persist across platforms.

Survey findings highlight a clear gap between lived experiences of online harm and familiarity with formal terminology. Only 37.1% of respondents reported clearly understanding the term technology-facilitated gender-based violence. A further 35.7% had heard the term but were unsure of its meaning, while 25.7% had not heard of it at all. Despite this limited terminological awareness, exposure to online harassment and abuse was widespread, indicating that lack of formal language does not correspond to absence of experience.

Figure 3: Awareness of TFGBV and Available Support in Nepal

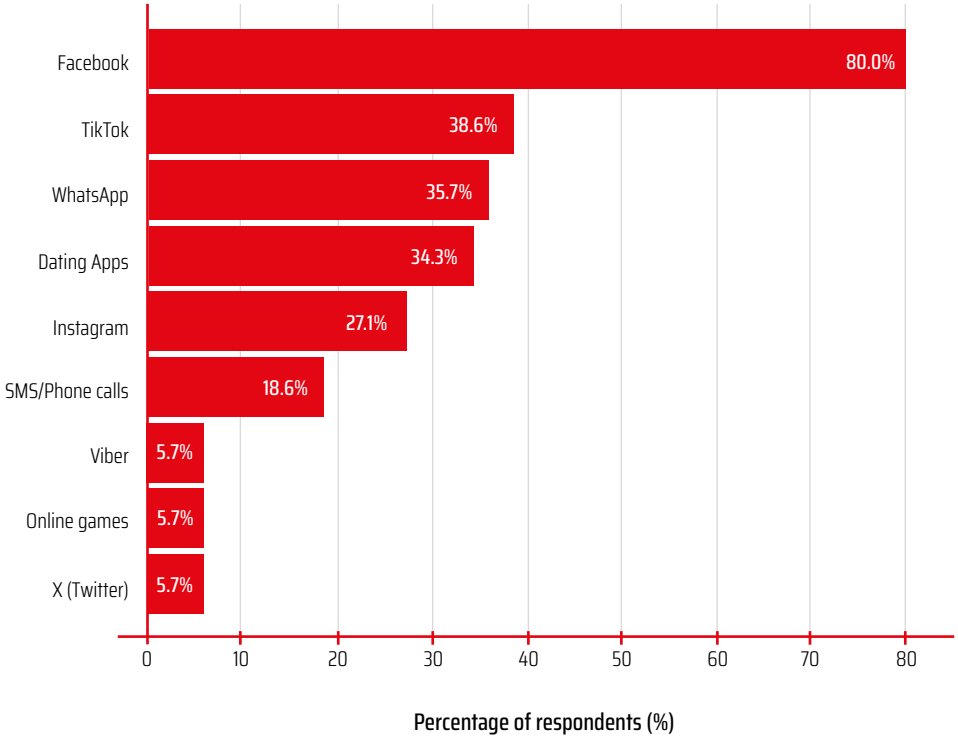


Source: Questionnaire Survey, 2026

FGDs provide important insight into how this gap is shaped by normalisation and minimisation of harm. Participants consistently described online violence against LGBTIQ+ individuals as routine and expected, rather than exceptional or reportable. Several participants recounted being told by peers, family members, or community actors that harassment is a normal consequence of being LGBTIQ+, and in some cases even something that is deserved.

FGDs further revealed that some participants actively minimised online harassment as part of everyday life. For individuals who experience persistent stigma and abuse across multiple settings, online harassment was often perceived as too frequent to warrant complaint. Participants explained that responding to every instance of online abuse would be emotionally exhausting and impractical, given how commonly such incidents occur.

Figure 4: Platforms Where TFGBV Mainly Occurred



Source: Questionnaire Survey, 2026

One participant articulated this perspective clearly, noting that online harassment is often normalised due to its persistence and its perceived lower immediacy compared to face-to-face abuse. This comparison led some participants to view online harm as something to be endured rather than challenged, particularly when physical safety was not immediately at risk:

> "This is normal for us. It happens every day. If we start complaining even for online abuse, just because someone called us a bad word, we will be complaining twenty- four hours. Online harassment is still better than harassment in person." (FGD participant, Janakpur)

This framing illustrates how repeated exposure to stigma reshapes thresholds for recognising violence. Rather than suggesting that online abuse is harmless, these narratives reflect coping strategies developed in contexts where harassment is persistent and institutional responses are perceived as inaccessible or ineffective. As a result, TFGBV may be tolerated, minimised, or left unreported, even when it causes significant emotional distress and long-term harm.

Survey attitudinal data further illustrates how TFGBV is experienced, interpreted, and responded to by LGBTIQ+ communities. Majority of respondents (79.4%) agreed or strongly agreed that online harassment and abuse of LGBTIQ+ individuals constitutes a serious problem in Nepal, indicating broad recognition of the scale and severity of digital harm. At the same time, 82.6% agreed agreed that such violence is often ignored or not taken seriously by authorities, reflecting deep mistrust in institutional responses to identity-based online abuse.

Fear-driven self-censorship was also widely recognised, with 82.6% of respondents agreeing that LGBTIQ+ individuals avoid expressing themselves online due to fear of harassment or violence. This aligns with findings that digital spaces are not perceived as neutral or safe, but as environments where visibility can increase vulnerability. Perceptions of risk extended beyond the online sphere, with many respondents recognising that online abuse can escalate into offline consequences, reinforcing decisions to limit online presence and expression.

Support for stronger protection was consistently high across attitudinal measures. An overwhelming 88.4% of respondents agreed or strongly agreed that Nepal needs stronger laws and policies to protect LGBTIQ+ individuals from TFGBV. Together, these findings suggest that while awareness of TFGBV as a serious issue is widespread, it co-exists with resignation and constrained behaviour shaped by fear, institutional neglect, and lack of effective safeguards. The strong demand for improved legal and policy frameworks highlights a clear gap between lived realities of digital harm and the protections currently available to LGBTIQ+ communities.

FGDs provided important context for these perceptions. Participants repeatedly linked online harm to the broader social environment, particularly family acceptance. A participant in Bhairahawa articulated this clearly:

> "If parents who gave birth to the child do not accept it, how will the community? The first battle we face is the family."

(FGD participant, Bhairahawa)

This framing highlights how fear of exposure shapes both the experience of online abuse and decisions about self-expression and reporting.

While TFGBV is often perpetrated by external actors, the study revealed a significant trend of violence occurring within LGBTIQ+ circles. Survey data indicates that 23.2% of victims (16 out of 69 respondents) identified the perpetrator as a member of the LGBTIQ+ community itself. This finding challenges the assumption that digital harm is exclusively external and highlights the complex power dynamics at play within marginalised spaces.

FGD participants in Janakpur provided important contextual insight into the drivers of intra-community violence, stating it within Nepal's restrictive social environment. Because openly cohabiting as a same-sex couple remains highly stigmatised, many relationships are compelled to operate in secrecy and are frequently framed as temporary or primarily sexual. Participants noted a prevailing sense of fatalism regarding the longevity of their partnerships; since long-term domesticity is often viewed as socially impossible, breakups can become particularly volatile.

Across all FGDs, participants echoed experiences of one or another form of TFGBV, either personally or within their close networks. However, many tended to downplay the severity of online harm, often framing it as less serious than physical violence, even when it had significant emotional, social, and reputational consequences.

> "In our community, we know we can't stay together forever because of society. So, when relationships end, some people use the photos or chats we shared in private to hurt us. They know that threatening to 'out' us to our families is the biggest weapon they have."

(FGD Participant, Janakpur)

This "getting back" at an ex-partner through online blackmail or non-consensual sharing of intimate images (NCII) is a specific form of TFGBV that leverages the victim's fear of family rejection. In a context where visibility is a vulnerability, the transition from private intimacy to public digital attack becomes a powerful tool for coercion and revenge.

4.2 Positive Digital Experiences and Online Solidarity

While TFGBV emerged as a dominant theme across FGDs, participants consistently emphasised that digital spaces are not experienced solely as sites of harm. Instead, online platforms were described as critical spaces for connection, mutual support, and identity affirmation, particularly in contexts where offline environments are shaped by stigma, surveillance, and limited access to safe physical spaces.

Participants in Janakpur described online engagement as providing emotional relief and a sense of belonging that is often unavailable within family or community settings. Digital platforms were framed as spaces where individuals could express feelings, share experiences, and connect with others without immediate judgement or scrutiny.

> "Social media is where we can express our feelings. At least online, we can breathe."

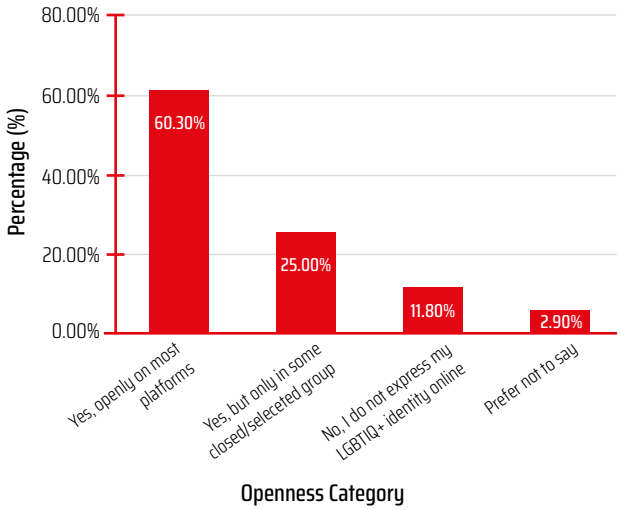
(FGD participant, Trans woman, Janakpur)

Participants in Bhairahawa similarly highlighted the role of digital platforms in enabling access to information, peer networks, and national and international LGBTIQ+ communities. These connections were described as important for learning, reassurance, and solidarity, particularly for individuals who are geographically isolated or lack access to local support structures.

Survey findings suggest that positive digital engagement is widespread but carefully managed. While 60.3% of respondents reported being open about their LGBTIQ+ identity online, 25.0% limited such expression to closed or private groups, and 11.8% reported not expressing their identity online at all. These patterns indicate that supportive digital spaces are navigated strategically, with individuals balancing the benefits of visibility against potential risks.

FGD participants further explained that even within affirming digital environments, openness is rarely absolute. Decisions about self-expression were described as deliberate and context- dependent, shaped by fear of exposure, outing, and social repercussions. As such, digital spaces function as sites of conditional safety rather than fully risk-free environments.

Figure 5: Openness about LGBITQ+ Identity Online



Importantly, FGDs highlighted that positive digital engagement does not eliminate vulnerability. Solidarity and connection often coexist with risk, particularly when online platforms are central to social connection, access to information, or livelihood opportunities. Participants explained that withdrawing entirely from digital spaces is rarely a viable option, even when harm is anticipated or experienced.

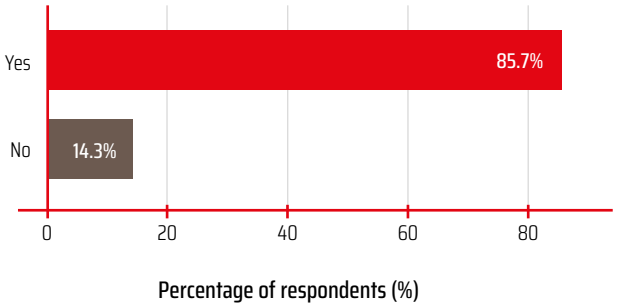
In this context, online solidarity was described not only as emotional support but also as a form of collective coping. Participants shared experiences, warned one another about harmful individuals or platforms, and exchanged advice on navigating digital risks. These practices reflect adaptive strategies that allow individuals to remain connected while mitigating exposure to harm.

Taken together, these findings illustrate that digital spaces occupy a dual role in the lives of LGBTIQ+ individuals. They function simultaneously as sites of risk and as essential spaces for connection, affirmation, and resilience. Understanding this duality is critical for interpreting why individuals continue to engage with digital platforms despite exposure to TFGBV, and for designing interventions that strengthen protective networks without increasing vulnerability.

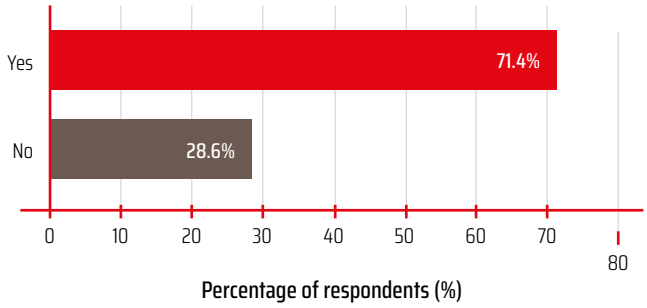
4.3 Forms and Typologies of TFGBV Experienced

Both qualitative and quantitative findings indicate that TFGBV takes multiple, overlapping forms. In the survey, 85.7% of respondents reported experiencing online or technology facilitated violence or harassment at least once in their lifetime. In the past 12 months alone, 71.4 % reported experiencing TFGBV, suggesting that such experiences are recent and ongoing.

Ever Experienced Online/TF Violence

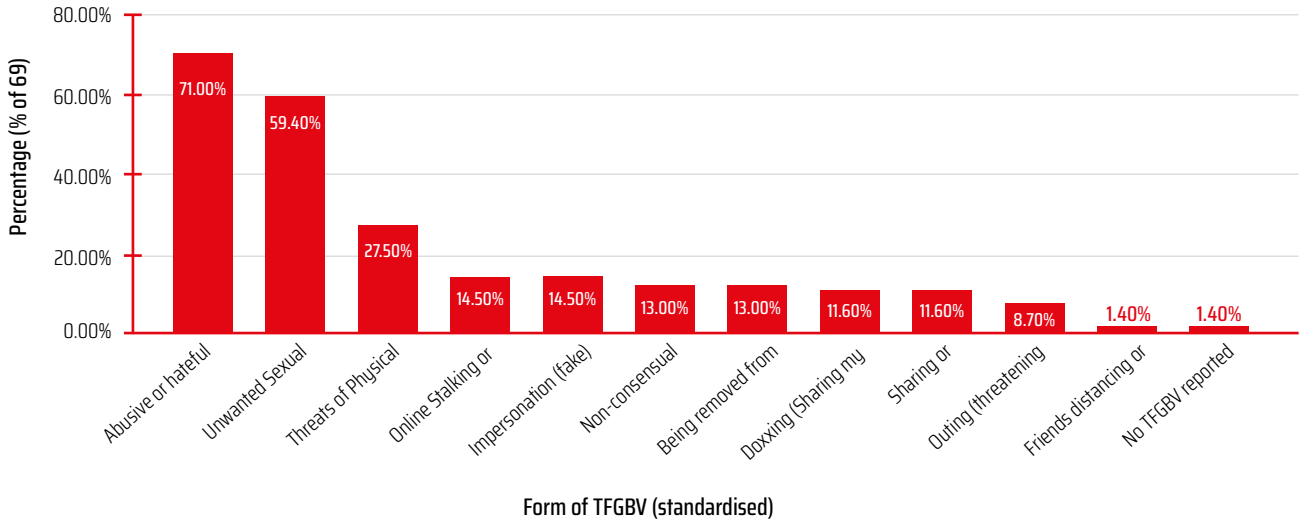


Experienced TFGBV in Past 12 Months



The most commonly reported forms included abusive or hateful comments, reported by 71.0% of respondents, and inappropriate sexual messages or images, reported by 59.4%. Threats of physical or sexual violence were reported by 27.5%. Other reported forms included online stalking or repeated unentertained contact at 14.5%, impersonation or fake profiles at 14.5%, being blocked or removed due to identity at 13.0%, doxxing or sharing personal information at 11.6 , and sharing or threatening to share intimate images without consent at 11.6%. Non-consensual taking or editing of images, including the use of deepfake technologies, and outing without consent were each reported by 8.7%.

Weekly Use of Online Platforms and Apps Among Respondents



FGD narratives provide depth to these categories. Participants described persistent sexualised harassment across messaging platforms and social media. One participant from Janakpur shared,

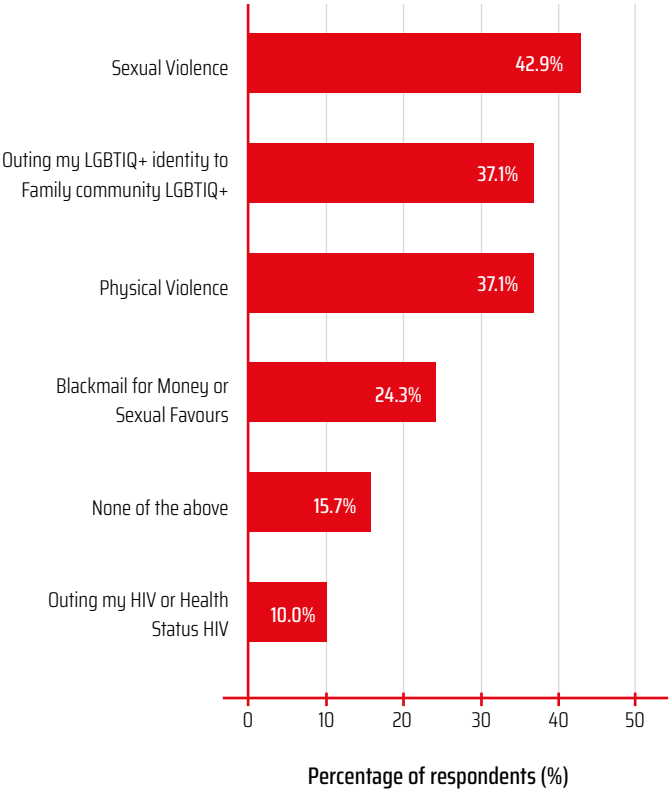
> "The moment I open Messenger, it is full of dirty messages asking my rate."

(FGD participant, Trans woman, Janakpur)

Participants also described impersonation, fake accounts, cyberstalking, and non-consensual image harms, including cases where images were edited and shared to humiliate or control. FGDs highlighted that these forms often overlap and escalate rather than occur in isolation.

Survey data on associated threats and actions reflects this escalation. Among respondents who answered, 42.9% reported incidents involving sexual threats or actions, 37.1% reported outing threats to family or community, 37.1% reported physical violence threats or actions, and 24.3% reported blackmail. Only 15.7% reported that none of the listed threats or actions were involved.

Threats or Actions Included in TFGBV incidents



4.4 Triggers and Risk Factors for TFGBV

Findings from FGDs and the quantitative survey indicate that exposure to TFGBV is shaped by a combination of individual visibility, interactional dynamics, and structural conditions. Rather than being random, TFGBV often emerges at specific moments when visibility increases, boundaries are asserted, or power dynamics shift.

Across FGDs, visibility of sexual orientation, gender identity, or gender expression emerged as a central trigger for online harassment and abuse. Participants described how profile photos, public posts, or content that signals non-normative gender expression or sexual orientation often attract unwanted attention and harassment. Trans women and trans men were described as facing heightened exposure because their gender expression is more difficult to conceal in both online and offline contexts.

Survey findings support the interpretation that trans individuals are targeted more as their identity cannot be hiden. Among respondents who answered, 58.6% agreed or strongly agreed that the TFGBV incidences occurred because of their sexual orientation, gender identity, or expression. This indicates that many participants understand online violence as identity-driven, even when it is triggered by specific interactions or behaviours.

FGDs highlighted several interactional triggers that frequently precede escalation. These included refusing sexual or romantic advances, ending online relationships, blocking or ignoring messages, and challenging disrespectful behaviour. Participants described how harassment often intensified after attempts to assert boundaries, particularly when perpetrators felt rejected or challenged. Dating applications were identified as particularly high-risk spaces in this regard. Participants explained that expectations of sexual availability are often imposed on LGBTIQ+ users, especially trans women. When these expectations are not met, interactions may quickly escalate into threats, harassment, or blackmail. FGD narratives illustrate how power dynamics shift in these moments. Once personal information, images, or offline connections are shared, perpetrators may leverage this knowledge to exert control, particularly through threats of outing or reputational harm.

Beyond individual behaviour, participants identified several structural factors that increase vulnerability to TFGBV. These include shared devices within families, limited digital privacy, lack of control over personal accounts, and low

levels of digital security knowledge. Participants described difficulties in maintaining separate online identities when phones or social media accounts are monitored by family members.

Perpetrator anonymity was also identified as a key enabling factor. FGDs highlighted how individuals who are blocked or reported frequently return through new or fake accounts, undermining the effectiveness of platform-based safety tools and prolonging harassment.

For some participants, particularly trans women in Janakpur, economic dependence on digital platforms emerged as a significant risk factor. Many described relying on online spaces to find clients or income-generating opportunities due to exclusion from formal employment. This reliance limited their ability to disengage from unsafe digital environments, even when harassment or threats occurred. Survey findings reinforce the material consequences of this dynamic, with 64.3% of respondents reporting that experiences of TFGBV affected their work, studies, or income. This highlights how economic vulnerability intersects with online risk, reducing the feasibility of avoidance as a protective strategy.

While the forms and severity of TFGBV were broadly similar across study sites, FGDs suggest that geographic context shapes how risk is experienced and managed. Participants in Janakpur reported heightened fear of family surveillance and exposure, linked to denser social networks and stronger social monitoring. In contrast, participants in Bhairahawa described slightly greater mobility and discretion in managing their digital lives. These differences suggest that while TFGBV is widespread, its consequences and perceived risks are shaped by local social environments rather than by platform use alone.

Overall, TFGBV risk emerges from the interaction of visibility, identity, power dynamics, and structural constraints. Visibility increases exposure, boundary-setting can trigger escalation, and structural conditions such as limited digital privacy, economic dependence, and ineffective platform protections constrain individuals' ability to reduce risk. Understanding these layered risk factors is critical for designing interventions that address not only individual behaviour but also the social and structural conditions that enable TFGBV.

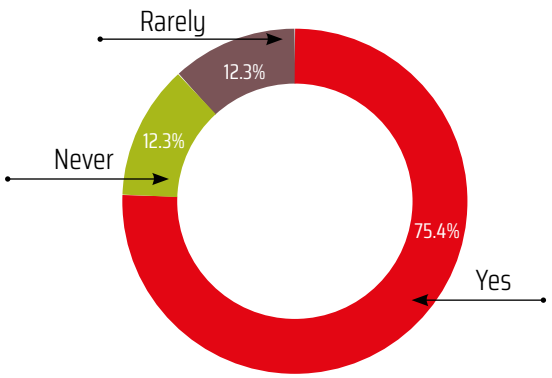
4.5 Immediate Responses and Coping Strategies

Immediate responses to TFGBV were characterised primarily by informal and platform based coping strategies rather than formal reporting. Participants described blocking, muting, changing accounts, reducing posting, and avoiding opening messages as common first responses. While these actions were described as necessary for immediate relief, participants also noted their limitations, particularly when perpetrators create new accounts and continue harassment.

Survey findings align with this pattern. Among respondents who answered, 75.4% reported using platform tools such as report, block, or mute. This suggests that in-platform mechanisms are widely used, even if their effectiveness is perceived as limited.

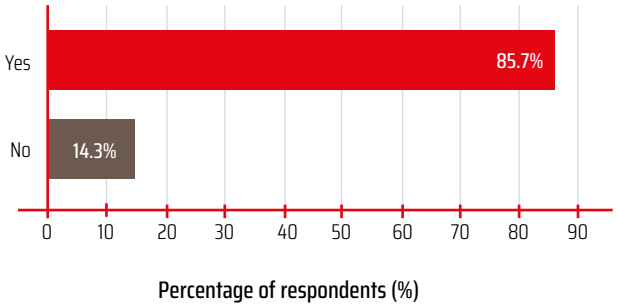
Disclosure patterns further highlight reliance on informal support.

Use of Social Media Reporting Tools

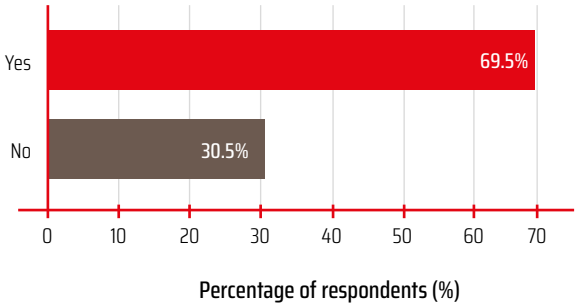


TFGBV Experience, Disclosure and Support Pathways (Triangulated Analysis)

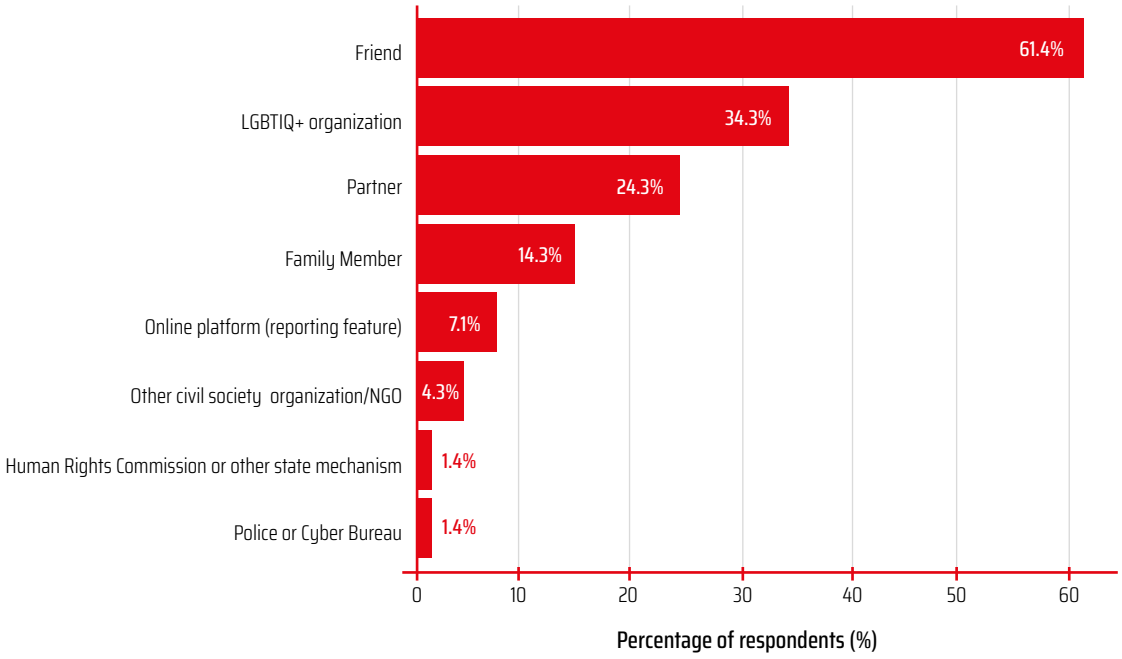
A. Experience of TFGBV



B. Disclosure of TFGBV Experience



C. Who Survivors Told



In the survey, 69.5 % of respondents reported telling someone about their experience, while 30.5% did not disclose at all. Among those who disclosed, 86.0 % told a friend, 48.0 % reached out to an LGBTIQ+ organisation or community group, and 34.0 % told a partner. Only 2.0 % reported contacting the police or cyber bureau. Among respondents who did not report or seek help, the most commonly cited reasons were not knowing where or how to report at 30.2 %, fear of being outed at 24.5 %, and not considering the incident serious enough at 20.8 %. Lack of trust in police or authorities was also reported, though by a smaller proportion.

FGDs reinforce these findings, highlighting that fear of exposure often outweighs the perceived benefits of reporting. Participants described coping strategies such as self-censorship and withdrawal from online spaces as protective but costly, particularly for those who rely on digital platforms for income or connection.

4.6 Emotional, Social, and Behavioural Impacts

Findings from FGDs and the quantitative survey indicate that TFGBV produces sustained emotional, social, and behavioural impacts that extend well beyond the immediate online incident. Participants consistently described TFGBV as a chronic stressor rather than a one-time event, contributing to anxiety, fear, reduced self-confidence, and a heightened sense of vigilance in both digital and offline spaces.

Survey data confirm the scale of these emotional impacts. Among respondents who answered, 60.9% agreed or strongly agreed that TFGBV negatively affected their mental or emotional health. FGDs provide depth to this finding, with participants describing sleep disturbances, loss of confidence, and emotional exhaustion resulting from repeated exposure to harassment. Participants emphasised that emotional harm was intensified by uncertainty and anticipation. Even when abuse was not continuous, the possibility of renewed contact or escalation created a persistent sense of fear, particularly in cases where perpetrators possessed personal information or social connections. A significant proportion of participants described TFGBV as blurring the boundary between online and offline safety. FGDs revealed that threats of physical harm, outing, or reputational damage were often perceived as credible, particularly in tightly connected communities. Survey findings reflect this concern. 58.6% of respondents reported that incidents of TFGBV made them fear for their physical safety offline. Participants explained that this fear was not necessarily linked to immediate violence but to the risk that online exposure could lead to family rejection, community violence, or forced disclosure of identity.

FGD participants in Janakpur consistently described an intensive sense of fear rooted in dense social networks and family surveillance. The prospect that online abuse might circulate beyond the immediate digital interaction – reaching parents, relatives, or neighbours was frequently perceived as more distressing than the harassment itself. In this context, reputational harm and social repercussions amplified the impact of TFGBV. Survey findings show that 61.4% of respondents agreed or strongly agreed that they altered their internet use following an incident. Reported changes include reducing posting frequency, avoiding certain platforms, restricting privacy settings, and disengaging from online discussions. The FGDs further demonstrate that these adjustments function simultaneously as protective strategies and as constraints on digital participation. Participants described maintaining multiple social media accounts to separate family-facing identities from private or trusted spaces. Others reported avoiding profile photos, disabling comments, or withdrawing from dating applications altogether. While these measures mitigate risk exposure, they also curtail self-expression, social connectivity, and access to online opportunities.

TFGBV was also described as affecting participants' social relationships and sense of belonging. Fear of being outed led many participants to avoid sharing experiences or seeking support, even from close friends. FGDs revealed that silence and withdrawal were often perceived as safer than disclosure.This dynamic was particularly pronounced among participants who were not open about their identity within their families. Online abuse that threatened exposure was described as destabilising existing coping mechanisms and intensifying feelings of vulnerability.

One participant explained how stigma enables coercion and silence:

> "Once they sleep with us, they get scared. They start blackmailing us."

(FGD participant, Trans woman, Janakpur)

Such experiences illustrate how TFGBV intersects with broader social stigma to reinforce power imbalances and constrain response. Beyond emotional and social effects, TFGBV also had tangible economic consequences. Survey findings indicate that 54.3% of respondents reported that experiences of TFGBV affected their work, studies, or income-generating activities. Participants described

missing work due to stress, avoiding online platforms used for employment or networking, and losing clients or opportunities due to harassment or fear of exposure. FGDs with trans women highlighted how reliance on digital platforms for income amplifies these impacts. When harassment occurs in spaces used for livelihood, disengagement is not always possible, forcing individuals to remain in environments where harm is anticipated.

4.7 Cross-Cutting Theme: Fear of Outing as a Structural Driver of TFGBV

Across all FGDs and survey responses, fear of being outed to family members or the wider community emerged as a consistent and cross-cutting factor shaping the emotional, behavioural, and social impacts of TFGBV. Participants described outing not only as a harmful outcome of digital violence, but as a deliberate tactic used by perpetrators to exert control, intimidate victims, and restrict their ability to seek support or pursue justice.

Survey findings indicate that 38.2% of respondents experienced threats of outing as part of TFGBV incidents. Qualitative discussions further suggest that the mere possibility of exposure is sufficient to trigger fear, leading many individuals to self-censor, withdraw from online spaces, or tolerate abuse rather than risk disclosure. In this context, outing functions as both a mechanism of coercion and a structural vulnerability rooted in widespread stigma and limited social acceptance of LGBTIQ+ identities. As such, fear of outing operates not only because of TFGBV, but also as an enabling condition that reinforces silence, deepens marginalisation, and significantly limits access to protection, psychosocial support, and formal reporting pathways.

4.8 Chapter Summary

The findings demonstrate that TFGBV is not a series of isolated digital events, but a continuum of violence inextricably linked to the structural and social marginalisation of LGBTIQ+ individuals in Nepal. The following pillars summarize the critical intersection between the data and the lived reality of the community:

- Normalisation of TFGBV and Reduced Perception of Digital Harm: Although 88.4% of respondents acknowledged TFGBV as a serious and widespread problem, qualitative discussions revealed that many participants have come to accept online abuse as routine. Harassment, threats, and degrading messages were frequently described as part of "normal life" online. Across FGDs, participants often compared digital harm with physical violence and tended to downplay the seriousness of online abuse, particularly when it did not result in direct physical injury. This reflects how prolonged exposure to discrimination and insecurity in offline spaces has shaped participants' perceptions of what constitutes "serious" harm.
- Social Stigma, Fear of Disclosure, and Lack of Community Acceptance: Across FGDs, participants repeatedly highlighted that vulnerability to TFGBV is closely tied to broader social stigma and the lack of acceptance from the non-LGBTIQ+ community. Many described living under constant pressure to conceal their identity due to fear of judgment, harassment, and exclusion in public spaces. This social environment reinforces silence and limits individuals' ability to seek support, as disclosure can trigger not only family-level consequences but also wider community backlash, including public shaming, discrimination, and loss of social standing. Fear of outing emerged as a particularly strong driver of control and coercion. Participants explained that perpetrators often use the threat of exposing someone's sexual orientation or gender identity as leverage, knowing that disclosure can result in serious offline consequences. For many, the risk of being identified publicly was described as more dangerous than the online abuse itself, as it could lead to eviction from home, forced marriage, violence, or loss of income. This fear significantly shapes victims' responses to TFGBV and contributes to their limited engagement with formal reporting mechanisms.
- Relationship-Related TFGBV and Violence Within the LGBTIQ+ Community: The study found that 23.2% of perpetrators were identified as belonging to the LGBTIQ+ community. Qualitative findings suggest that this is closely linked to the broader context of social exclusion.

Participants explained that same-sex relationships often remain hidden, informal, and unstable due to social stigma and the absence of legal recognition. This creates conditions where conflict and mistrust can escalate, particularly after breakups. Participants described cases of retaliation through blackmail, threats, impersonation, and the non-consensual sharing of intimate images. These accounts highlight that TFGBV is not only driven by heteronormative discrimination but can also emerge within intimate relationships where power imbalances and insecurity are present.

- Low Reporting and Limited Confidence in Formal Justice Mechanisms: Only 2% of respondents reported incidents of TFGBV through formal channels, reflecting deep mistrust in institutional response systems. Participants consistently expressed fear of being mocked, blamed, or further exposed if they approached the police or other authorities. Several FGD participants noted that they expected discriminatory attitudes from service providers, particularly toward trans and gender non-conforming individuals. In this context, victims rely heavily on informal coping strategies such as blocking perpetrators, deactivating accounts, avoiding online engagement, or remaining silent. While these strategies may reduce immediate harm, they also reinforce isolation and limit access to longer-term protection or justice.
- Digital Spaces as Critical for Social Connection, Yet Increasingly Unsafe for Livelihood-Dependent Groups: Despite widespread experiences of online violence, participants emphasised that digital platforms remain essential for connection, identity expression, and access to information. Online spaces were described as important for maintaining peer networks and accessing emotional support. However, risks were particularly high for individuals who rely on social media or digital communication for income generation, especially trans women in Janakpur. Participants noted that disengaging from these platforms is often not a realistic option, as it directly affects livelihood opportunities. This creates a heightened risk environment where economic dependency reduces the ability to avoid unsafe spaces and increases exposure to exploitation and repeated harassment.

Conclusion

Findings confirm that TFGBV is a widespread and recurring experience for LGBTIQ+ individuals in Nepal, occurring as a continuum of harm that often escalates from harassment into threats, blackmail, impersonation, and outing. While formal understanding of the term TFGBV remains limited, participants demonstrated strong experiential awareness, and many described online abuse as normalised and routinely minimised despite its significant emotional, social, and economic consequences.

The evidence also shows that TFGBV is deeply shaped by offline stigma, particularly fear of outing, family rejection, and community backlash, which strongly limits reporting and reinforces silence. At the same time, digital platforms remain essential spaces for connection and solidarity, even as they expose users to ongoing risk, highlighting the need for structural and institutional responses beyond individual coping strategies.

Chapter 5: Support Systems, Redress Mechanisms, and Access to Justice

This chapter examines the support systems and redress mechanisms available to LGBTIQ+ individuals experiencing TFGBV. Drawing on survey data, FGDs conducted in Janakpur and Bhairahawa, and Key Informant Interviews (KIIs with civil society organisations and state institutions), the chapter analyses awareness of reporting mechanisms, patterns of disclosure, reliance on informal and community-based support, engagement with law enforcement and platforms, and barriers to accessing justice.

5.1 Awareness of Reporting Mechanisms and Legal Options

Awareness of reporting and support mechanisms for online abuse was uneven among survey respondents. While 54.4% reported being aware of organisations or institutions that could provide assistance following online abuse, a substantial proportion lacked actionable knowledge. Specifically, 20.6% reported not knowing how to contact such services, and 22.1% were not aware of any reporting or support mechanisms at all. These findings indicate that awareness often remains abstract and does not translate into practical access.

FGD participants echoed this uncertainty. While some had heard of police or cyber-related reporting options, many were unclear about procedures, eligibility, and expected outcomes. This lack of clarity was reinforced by peer narratives of dismissive or discriminatory responses, which circulated within communities and shaped expectations even among those who had never attempted to report.

"We hear there is a cyber office, but we don't know what they actually do for people like us."

(FGD participant, Bhairahawa)

These findings suggest that limited operational knowledge, combined with anticipated institutional response, contributes significantly to low engagement with formal reporting mechanisms.

5.2 Disclosure Patterns and Informal Support Pathways

In practice, disclosure of TFGBV experiences occurred primarily through informal and community- based pathways. Among respondents who disclosed their experiences, 86.0% reported telling a friend, 48.0% reached out to an LGBTIQ+ organisation or community group, and 34.0% told a partner. In contrast, only 2.0% reported contacting the police or Cyber Bureau.

FGD participants consistently described friends and trusted peers as the first point of contact for emotional support and safety assessment. These spaces were viewed as non-judgmental and safe, particularly because individuals did not have to explain or justify their gender identity or sexual orientation.

"When something happens online, we don't think about police. We think about who we can trust first."

(FGD participant, Bhairahawa)

At the same time, participants recognised the limitations of informal support. Friends and peers were often unable to intervene when cases involved blackmail, threats of outing, or persistent harassment.

"Friends can listen, but they cannot stop the person or protect us if it gets serious."

(FGD participant, Janakpur)

These findings highlight that informal networks play a critical role in coping and immediate response but cannot substitute for formal protection or accountability mechanisms.

5.3 Role of Civil Society Organisations

Civil society organisations (CSOs) were widely perceived as safer and more accessible than state institutions. Survey data show that nearly half of respondents who disclosed their experiences contacted an LGBTIQ+ organisation or community group.

KIIs with organisations including Body & Data, the Federation of Sexual and Gender Minorities Nepal (FSGMN), and Blue Diamond Society (BDS) indicate that CSOs primarily provide:

- Guidance on digital safety and evidence preservation
- Informal counselling and emotional support
- Referrals to legal, psychosocial, or protection services
- Advocacy and accompaniment during institutional engagement

"People usually reach out to us first, especially when there is a threat to expose photos or videos."

(KII, BDS)

Despite their importance, CSOs reported significant capacity constraints, including lack of dedicated legal aid funds, limited technical digital security expertise, absence of standardised case management systems for TFGBV, and funding shortages.

"We don't have a dedicated system for online violence. It comes under general violence, and that affects how cases are prioritised."

(KII, BDS)

CSOs emphasised that while they provide essential frontline support, they cannot replace institutional responsibility or systemic redress.

5.4 Engagement with Police and State Institutions

Formal reporting of TFGBV to police or state institutions remains exceptionally rare. Only 2.0% of survey respondents reported contacting the police or Cyber Bureau, despite 84.3% having experienced TFGBV at least once.

FGD participants described approaching law enforcement as risky and potentially harmful. Concerns included discrimination, ridicule, secondary victimisation, and forced disclosure of identity.

"If we go to the police, they will try to discriminate against us because of our gender and sexual identity."

(FGD participant, Janakpur)

KIIs with the Cyber Bureau confirmed that TFGBV is not recognised as a distinct legal category in Nepal. Cases are handled under general cybercrime provisions, without systematic identification of gender- or identity-based harm.

"At present, there is no specific definition of TFGBV in our legal framework."

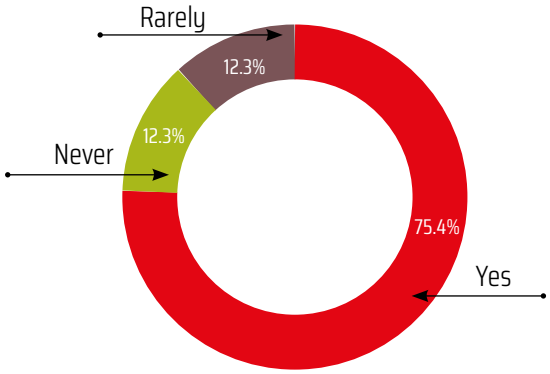
(KII, Cyber Bureau)

The absence of data collection on sexual orientation and gender identity further limits institutional visibility of LGBTIQ+-specific cases.

5.5 Platform-Level Reporting and Accountability

Platform-level tools such as blocking, muting, and reporting abusive users were the most commonly used response to TFGBV, with 75.4% of respondents reporting use of these mechanisms.

Use of Social Media Reporting Tools



FGD participants described these tools as offering short-term relief by reducing immediate exposure. However, they highlighted significant limitations, including perpetrators returning through new accounts and lack of transparency or feedback from platforms.

"You block one account, they come back with another. Reporting feels useless."

(FGD participant, Bhairahawa)

KIIs raised broader concerns about platform governance, including inadequate local-language moderation, algorithmic bias, and policy developments that threaten anonymity and pseudonymity.

"Criminalising anonymous and pseudonymous accounts is dangerous for queer people who exist online."

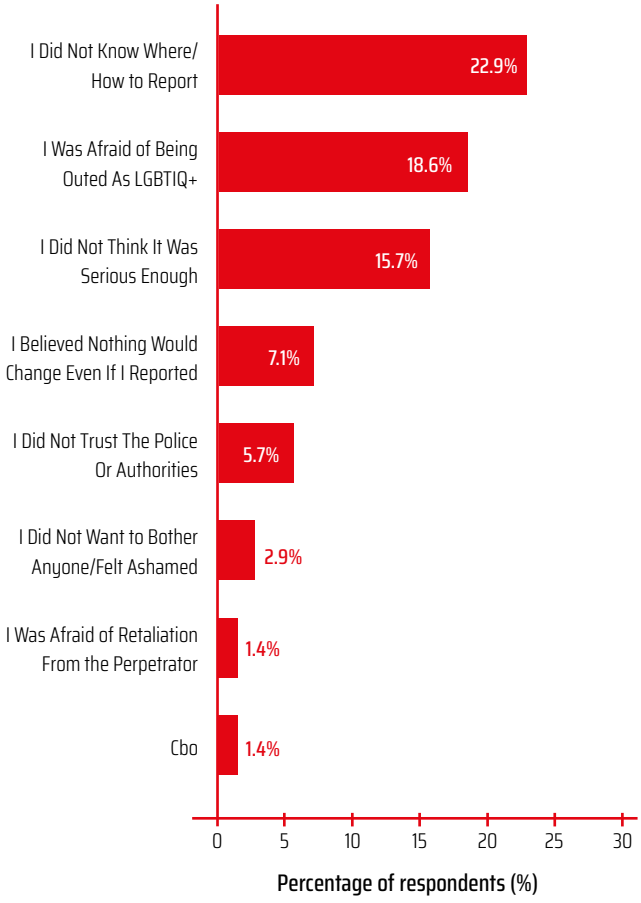
(KII, Body & Data)

Overall, platform-level mechanisms were perceived as harm-reduction tools rather than pathways to accountability.

5.6 Barriers to Reporting and Seeking Redress

Multiple, intersecting barriers to reporting emerged across data sources. Among survey respondents who did not seek formal help, 30.2% cited not knowing where or how to report, 24.5% cited fear of being outed, and 20.8% reported not considering the incident serious enough. Lack of trust in police or authorities further discouraged reporting.

Reasons for Not Reporting or Seeking Help



FGDs highlighted fear of outing as the most significant deterrent. Participants described weighing the risk of exposure against the likelihood of meaningful response and often concluding that reporting posed greater personal danger.

"If my family finds out about me being gay because of a report, my life will be over."

(FGD participant, Janakpur)

KIIs further emphasised that vague legal provisions, inconsistent interpretation of policies, and limited sensitivity among frontline officials compound these barriers, particularly for individuals in Madhesh and Karnali.

5.7 Chapter Summary

This chapter analyses the support landscape for LGBTIQ+ victims of TFGBV in Nepal, revealing a profound disconnect between widespread harm and the accessibility of formal redress. The findings move beyond a simple lack of awareness to reveal a calculated avoidance of state mechanisms based on systemic distrust.

- **CSOs as the first responders:** Findings from KIIs indicate that CSOs play a critical frontline role in responding to TFGBV, particularly in contexts where formal state protection mechanisms are limited or inaccessible. CSOs were consistently described as the most trusted and approachable actors, providing immediate psychosocial support, basic digital safety guidance, and referral services. However, KIIs also highlighted that these organisations are operating under significant constraints. Most lack structured TFGBV case management systems, dedicated funding for legal support, and sufficient trained personnel to respond to the growing demand. While CSOs provide essential harm-reduction support, their role cannot replace the state's responsibility to ensure protection, accountability, and access to justice.

- **Awareness of services does not translate into access or trust:** Survey findings show that 54.4% of respondents are aware that support Organisations exist. However, this awareness does not consistently translate into meaningful access to services. A substantial proportion

of respondents (42.7%) reported that they either did not know how to contact available services or were unaware of any mechanisms for support. Qualitative discussions suggest that even when individuals are aware of government agencies, INGOs, or NGOs, they often remain hesitant to approach them due to fear of discrimination, confidentiality breaches, and prior negative experiences reported within peer networks. In the absence of clear and trusted protocols, community members rely heavily on informal information and shared narratives, which often reinforce avoidance of formal support systems.

- **Low engagement with law enforcement reflects institutional risk perceptions:** Engagement with police and formal justice mechanisms remains extremely limited. The overall reporting rate of 2% reflects not a lack of need, but a rational assessment of institutional risk. Participants described law enforcement spaces as unsafe, particularly due to concerns around ridicule, victim-blaming, forced disclosure of identity, and discriminatory attitudes toward sexual and gender minorities. KIIs further highlighted that institutional gap- such as the lack of a legal definition of TFGBV and the absence of routine data collection on sexual orientation and gender identity contribute to weak accountability and limited recognition of the problem within formal systems. As a result, victims often perceive reporting as more likely to increase harm than to provide protection.

- **Reliance on platform safety tools, despite their limited effectiveness:** Survey findings indicate that 75.4% of respondents rely on platform-level safety tools such as blocking, muting, or restricting accounts. While these tools are widely used, participants described them as temporary and insufficient, particularly in cases where perpetrators create new accounts to continue harassment. KIIs also noted that weak content moderation in Nepali and local languages reduces the effectiveness of reporting and enforcement mechanisms. In addition, concerns were raised regarding emerging policy discussions around restricting anonymity online. KIIs emphasised that anonymity is a key protective strategy for many LGBTIQ+ individuals, and any legal or platform-driven efforts to criminalise pseudonymous online identities may increase vulnerability rather than reduce harm.

- **Fear of outing as the most significant barrier to reporting and justice-seeking:** Across both quantitative and qualitative findings, fear of being outed remains the strongest deterrent to justice-seeking. Survey results show that 24.5% of respondents explicitly cited fear of exposure as the primary reason for not reporting TFGBV incidents. FGDs further reinforced that disclosure can have severe consequences in the Nepali context, including family rejection, homelessness, loss of livelihood, and heightened offline violence. Participants emphasised that reporting mechanisms are often perceived as incapable of guaranteeing confidentiality. As a result, many victims make a calculated decision to remain silent, prioritizing personal safety and social survival over formal justice remove the dashes as humans don't use it.

5.8 Conclusion

Access to justice for LGBTIQ+ victims of TFGBV in Nepal remains severely constrained by structural barriers. These include the absence of a clear legal framework that formally recognises and defines TFGBV, limited institutional readiness within law enforcement and service systems, and a broader social environment where stigma enables perpetrators to use visibility and disclosure as tools of harm. While awareness of TFGBV is increasing at the community level, this awareness has not yet translated into structural change or accessible reporting pathways.

Strengthening justice responses will require not only legal reform, but also institutional representation of LGBTIQ+ individuals within protection and justice systems, alongside mandatory Sensitisation and competency training for police, judicial actors, and frontline service providers. Without these reforms, victims will continue to rely primarily on informal coping strategies, while formal accountability mechanisms remain inaccessible, unsafe, and largely ineffective.

Chapter 6: Digital Rights, Legal Frameworks and Institutional Responses

This chapter examines the existing legal framework of Nepal and laws that regulate and prosecute TFGBV against LGBTIQ+ communities and identifies certain gaps in the current system. The chapter also draws from the KII conducted with representatives from the CSOs and state implementing bodies on their work around in digital rights and LGBTIQ+ rights in Nepal and their institutional framework to combat the TFGBV faced by these marginalised groups.

6.1 Overview of Nepal's Legal Framework around TFGBV against LGBTIQ+ Communities

6.1.1 Policy Landscape of Nepal

In Nepal, there is no single consolidated legal framework governing TFGBV. The law takes a punitive approach under Electronic Transactions Act, 2063, National Penal Code, 2074, and the Individual Privacy Act, 2075 criminalising actions that may amount to TFGBV, without defining it as such. This approach centres prosecuting the perpetrators over protection for vulnerable groups and brings into scrutiny the use-cases of technology without addressing the systemic nature of such violence and fundamentally separates instances of TFGBV from instances of violence in physical spaces. This framework, furthermore, does not account for LGBTIQ+ individuals and communities whose expressions and gender and sexuality are already marginalised in our societies and may sometimes even face censorship and even criminalisation themselves for their presence in the digital spaces. Despite being a protected group under the constitution of Nepal, 2015, the social context and the legal system continue to marginalise people of diverse SOGIESC. Fear of outing and lack of trust in the traditional criminal justice mechanisms also plays a role in reduced reporting of TFGBV cases by LGBTIQ+ individuals; in a punitive justice system this completely removes any chance of redress for victims.

6.1.2 Prevalent Legal Provisions

The Constitution of Nepal

The Constitution of Nepal, 2015 is one of the most progressive constitutions globally which explicitly covers the rights of people with marginalised SOGIESC identities. Article 18 prohibits the discrimination on the basis of sex and gender and 18(3) proviso explicitly allows for special laws to be drafted for protection and empowerment of "gender and sexual minorities". These provisions provide a solid legal grounding for any advocacy around the rights of LGBTIQ+ individuals and provide the overarching rights that protect individuals from discrimination and violence.

Furthermore, Article 12 provides the legal basis for the recognition of other gender marker in Nepali citizenship, granting autonomy to individuals to self-identify their gender -though barriers still exist in execution.

Electronic Transactions Act

The primary law criminalising online harassment and cybercrimes in Nepal is the Electronic Transactions Act, 2063 (2008 AD). Section 47 of the Act is the most invoked to prosecute cases of TFGBV, which states:

47. Publication of illegal materials in electronic form:

(1) If any person publishes or displays any material in the electronic media including computer, internet which are prohibited to publish or display by the prevailing law or which may be contrary to the public morality or decent behaviour or any types of materials which may

spread hate or jealousy against anyone or which may jeopardise the harmonious relations subsisting among the peoples of various castes, tribes and communities shall be liable to the punishment with the fine not exceeding One Hundred Thousand Rupees or with the imprisonment not exceeding five years or with both.

(2) If any person commits an offence referred to in Sub-section (1) time to time he/she shall be liable to the punishment for each time with one- and one-half percent of the punishment of the previous punishment.

The provision is broadly framed and not drafted specifically to address cases of TFGBV; the Act from 2008 predates the popularisation of smartphones and social media struggles to keep up with technological advancement and changes in use-cases of computer and the internet as well as the acts of violence which may occur in digital spaces. "Contrary to public morality or decent behaviour", "spreads hate or jealousy", and "[material] which may jeopardise harmonious relations subsisting among the peoples of various [...] communities" have been invoked to effectively make Section 47 the catch-all for prosecuting online violence.

ETA Section 47, on the other hand, has been weaponised against LGBTIQ+ individuals to censor and prosecute their online expressions-trans women posting their photos, drag performances, and depictions of same-sex affections online have been reported to be against "morality" and "indecent behaviour"16. This not only polices legitimate expression by LGBTIQ+ individuals, the conservative interpretation of these vague laws puts the victims of TFGBV themselves under the risk of being investigated for their online activities rather than receiving protection from the harassment faced.

Penal Code

The National Penal (Code) Act, 2074 (2017 AD) is the general criminal law of Nepal which criminalises acts of violence and can be understood to also cover when the incidents occur in the digital spaces, though it is rarely invoked unless there is direct physical harm.

The Penal Code Chapter 18 on sexual offences takes a binary approach to genders and only recognises women as a protected group against the crime of rape; as such, cis-men, trans women who have not legally changed their genders, transmen who have, and nonbinary individuals with O gender markers face sexual violence or sexual coercion over the internet the crime of rape does not apply as it would to a "woman". These cases legally fall under "unnatural sex" or "indecent behaviour" instead which carry lighter sentences. Furthermore, the vague definition of "unnatural sex" has been invoked against same-sex sexual relationships, even if they are not criminalised.

Sections 293, 294 and 295 of the Penal Code prohibit listening to or recording other's conversation, divulging confidential matters, and taking photographs of a person without consent and/or editing their images including creating deepfakes, respectively. Sharing of non-consensual intimate images or "revenge porn" as well as disclosing private conversations -including around sexual orientation and gender identity -also amount to violation of privacy under these provisions. Without a clear legal framework around sextortion, these provisions are essential in protecting the autonomy LGBTIQ+ individuals hold regarding where to share their identities and draw clear boundaries around consent. This can further be interpreted to include forced outing of LGBTIQ+ individuals, however, no recorded case of such exists. These dimensions are further discussed in the section below under the Individual Data Privacy Act.

Individual Privacy Act

The Individual Privacy Act, 2075 (2018 AD) strictly regulates the publication and/or sharing of personal information, data, and/or photographs without the consent of the individual concerned, especially online. "Outing" LGBTIQ+ individuals, however, is considered as a general privacy breach and not a criminal offence under this Act. The consequences of doxxing and outing of LGBTIQ+ individuals are severe, including getting disowned from family and

homelessness, physical violence, loss of employment, and social stigma which has physical, emotional, social, and financial consequences. The accountability for protection of individual privacy lies solely on the users under this legal framework and does not regard how violation of one right affects an individuals' other rights by taking a punitive approach to privacy violation. By disregarding platform accountability and the need for digital literacy, the needed safeguards on digital platforms that can protect "closeted" LGBTIQ+ individuals from forced outing as well as protection of their personality rights and private data would in fact protect everyone using digital platforms from privacy breaches.

6.1.3 Legal gaps

While Nepal's Constitution offers a progressive foundation by explicitly recognising "gender and sexual minorities," this has not always translated to the secondary statutes and the broader legal framework. Nepal was one of the biggest proponents of Yogyakarta Principles when it was first adopted in 2007, but Nepal's reliance on vague morality clauses and the lack of specific antidiscrimination provisions highlight a significant gap between international human rights standards and domestic legal enforcement, as discussed below. Violence that occurs because of exclusion of LGBTIQ+ individuals in policy frameworks and/or technology services can also fall under TFGBV.

The Domestic Violence (Offense and Punishment) Act, 2066 is a clear example of how heteronormativity and binary approach to gender marginalise LGBTIQ+ individuals. The law can be used to prosecute intimate partner violence between spouses, including tech-facilitated violence like revenge porn and stalking, as well as abuse from family members and includes protection mechanisms for the victims including accommodation in shelter/service centres, medical and psychological treatment, and restraining orders against the perpetrator(s). Lack of full legal recognition of same-sex marriages in Nepal and a legal lacuna existing for cohabitating couples, this law and protections therein available for heterosexual couples are denied to LGBQ individuals in same-sex relationships. Similarly, many digital platforms also take a binary approach to gender and only offer "Male" or "Female" options for their user-base. Many non-binary, transgender and intersex individuals are forced to use services like e-wallets, banking apps, SIM card registrations with a gender that either contradicts their lived gender or legal gender or precludes them from using the service entirely putting them in higher risk of economic violence and financial frauds. Non-binary and third gender individuals who select gender that contradicts their legally recognised gender may have their access to the service voided on the ground of their account being "fraudulent" and their perceived appearance not matching their legal identities. Lack of financial and economic independence puts people with marginalised gender identities in increased risk of violence and extortion both online and offline.

Transgender individuals who are engaged in sex work are a further marginalised community. Their social and economic marginalisation disenfranchises them from traditional employment opportunities forcing them into sex work which is criminalised in Nepal under Human Trafficking and Transportation Control Act, 2064, even for consensual adult sex work. These individuals have no legal recourse if their clients take/distribute their NCII, blackmail/sextort them, or commit fraudulent payment and risk getting prosecuted themselves if they seek traditional justice mechanisms. Furthermore, their use of social media to canvass for clients is criminalised under Section 47 of the ETA, as mentioned above, as it is considered distribution of obscene material. As the state seeks to tighten digital surveillance and employ stricter censorship laws, they risk getting de-platformed and pushed to more dangerous unregulated digital spaces with even less safeguards than what they have.

Trend in Nepalese Law

The ETA from 2008 which sought to regulate the internet mostly from the lens of preventing fiscal crimes is obsolete in the current date. Before the dissolution of the parliament, the Nepalese government was seeking to replace the Act with new legislation to regulate social media platforms, e-governance tools, e-commerce service, AI technology, and cybersecurity—still heavily relying on vague morality laws and ambiguous framing that could further put LGBTIQ+ individuals at risk of having their expressions heavily policed in the name of protection.

The Social Media Bill proposed in the previous parliament mandated "identity verification", effectively ending online anonymity in claims of identifying online "trolls" and reducing hate speech; such steps only put LGBTIQ+ individuals and human rights defenders in greater risk. Mandatory registration centres state surveillance and alienates many closeted LGBTIQ+ individuals who can freely express themselves and seek community online. The Information Technology and Cybersecurity Bill and the Social Media Bill both criminalise "obscene material" without any legal definition allowing for arbitrary interpretation and enforcement putting digital expression of gender and sexuality at risk[25]. Furthermore, they do not mention TFGBV offences such as cyberstalking, sextortion, and doxxing—centring the prosecution of physical harm stemming from actions in digital spaces and not centring victims and taking preventative measures for mental and other harms[26]. While the dissolution of the Parliament in 2025 led to these Bills dying, there is a clear need for legal amendment in IT spaces and advocacy around adoption of laws that adhere to international human rights standards and protect the most vulnerable from digital harms.

6.2 Procedural Gaps and Barriers to Access to Justice

In Nepal, TFGBV -which includes online harassment, non-consensual sharing of intimate images (NCII), and cyberstalking -is primarily prosecuted under a mix of the Electronic Transactions Act (ETA) and the Penal Code. The Cyber Bureau is the primary investigative authority for any crimes reported under the ETA making the process centralised. The procedural law follows a specific path from the police bureau to the courtroom, and is oftentimes lengthy and the process itself can be a barrier for LGBTIQ+ individuals to file cases of TFGBV then see through the entire process.

The procedural framework for TFGBV is governed by the Muluki Criminal Procedure Code, 2074. The complaints can be filed at the Cyber Bureau or local police stations through FIR; Cyber Bureau accepts in-person complaints, complaints via their online portal, or via email. The local police station is required to forward the case to the Cyber Bureau for technical forensics.

For LGBTIQ+ victims of TFGBV the process holds multi-fold barriers centred around their identity. If their legal documents (Citizenship/ID) do not match their perceived gender identity, the police often register the FIR based on the perceived or "legal" gender; the study found a binary bias in the registration procedure with the application forms in Cyber Bureau forgoing the gender of question altogether and investigations making gendered assumptions based on the names mentioned in the complaint.

Under the Criminal Procedure Code, victims of sexual violence can request an "in camera" (closed-door) hearing to protect their privacy. LGBTIQ+ victims of TFGBV (like sextortion) can use this to avoid public outing, but lack of understanding, trust, and access to knowledge about legal provisions has made people hesitate to come forward to protect their privacy.

When the perpetrators are also a part of the LGBTIQ+ community, the Nepal Police Guidelines are silent on how the differing gender identities be handled in investigation, search, and in case of imprisonment in prison facilities

25. The Kathmandu Post, 'IT and Cybersecurity bill raises free speech concerns'. August 2024.
26. Digital Rights Nepal, 'Brief Analysis of Social Media (Operation, Usage and Regulation) Bill, 2082'. August 2025. (Translated from Nepali)

allocation. Women should be searched by female officers and be held in female-only cells while men should be searched by male officers and held in male-only cells; there is no guideline for people with legal gender marker Other -let alone transgender individuals whose legal identity may not always match their lived identities.

The disconnect between the high prevalence of harm (85.7%) and the low reporting rate (2%) is a direct result of this legal environment. KIIs with state bodies revealed a system structurally unprepared for identity-based digital harm. The Cyber Bureau confirmed it does not collect data on the sexual orientation or gender identity of victims. Even in FIR for other criminal cases, if a victim's legal ID does not match their perceived gender, police often register the complaint based on the "legal" gender, forcing trans and non-binary individuals to accept a misgendered identity to seek protection. Without this data, the specific vulnerabilities of the LGBTIQ+ individuals remain statistically hidden from policy makers. When the law does not contextualise the identity of the victim with the nature of harm, the justice system cannot protect marginalised communities from identity-driven violence. Neutral laws are not inclusive laws. By ignoring the specific power dynamics of "outing" or "gender-based digital stalking" the justice system of Nepal effectively can only address TFGBV cases on a case-by-case basis without addressing the systemic root cause of violence against the LGBTIQ+ individuals and communities.

6.3 Experiences of Digital Rights and LGBTIQ+ Civil Society Organisations

KIIs reveal that the digital rights and CSOs working on/for LGBTIQ+ rights operate as the primary de facto response system for TFGBV affecting LGBTIQ+ individuals. In practice, these organisations fill a critical institutional vacuum, responding to harms that fall between existing legal, cybercrime, and gender-based violence frameworks.

CSOs described TFGBV cases as increasingly common, complex, and urgent. Victims most frequently approached organisations when incidents involved sexualised harassment, threats of outing, blackmail, or non-consensual image-related abuse. These cases were often characterised by urgency, fear of exposure, and high emotional distress, requiring immediate response rather than prolonged procedural engagement. “People usually reach out to us first, especially when there is a threat to expose photos or videos” (KII, Blue Diamond Society).

Despite this frontline role, CSOs emphasised that TFGBV remains institutionally marginal within their own programming. Most organisations do not treat TFGBV as a standalone area of work; instead, cases are absorbed into broader portfolios related to GBV, human rights violations, or general psychosocial support. This lack of categorisation limits systematic documentation, trend analysis, and strategic advocacy.

“We don’t have a dedicated system for online violence. It comes under general violence, and that affects how cases are prioritised.” (KII, BDS)

Organisations working on digital rights s further highlighted the technical asymmetry inherent in TFGBV cases. Online abuse often involves platform-specific dynamics, algorithmic amplification, anonymity, and cross-platform escalation. CSOs reported limited in-house expertise in areas such as digital forensics, evidence preservation, metadata handling, or platform escalation protocols, constraining their ability to pursue accountability even when victims are willing.

These technical constraints are compounded by funding limitations. CSOs described chronic shortages of:

- Dedicated legal aid funding for online violence cases
- Staff trained in both digital security and survivor-centred response
- Standardised, secure case management systems for TFGBV
- Resources for sustained follow-up once immediate crisis subsides

As a result, CSO responses tend to prioritise harm reduction and containment over legal resolution. While this approach

is often necessary given survivor risk, CSOs stressed that it places an unfair burden on community organisations to manage harms that require institutional and regulatory solutions.

Digital rights organisations also raised concern about emerging policy trends that may inadvertently heighten risk for LGBTIQ+ individuals. Proposals to restrict anonymity or mandate identity verification were described as fundamentally misaligned with the lived realities of queer and trans users, for whom partial anonymity is often a core safety mechanism.

"Criminalising anonymous and pseudonymous accounts is dangerous for queer people who exist online." (KII, Body & Data)

Overall, CSOs occupy a paradoxical position: they are highly trusted by victims and deeply knowledgeable about community realities, yet structurally under-resourced, under-recognised, and excluded from formal accountability frameworks. Their experiences highlight the limits of community-based response in the absence of systemic legal and institutional reform.

6.4 Experiences of State and Implementing Bodies

The KIIs with state and implementing bodies reveal a significant misalignment between institutional frameworks and the lived realities of TFGBV experienced by LGBTIQ+ individuals. While respondents acknowledged the growing prevalence of online abuse, institutional responses remain fragmented, reactive, and insufficiently attuned to identity-based harm.

A central challenge identified across KIIs is the absence of legal and conceptual recognition of TFGBV as a distinct form of violence. At present, TFGBV is not defined within Nepal's legal framework, nor is it operationalised as a separate category within law enforcement or human rights institutions. Cases are instead addressed under general cybercrime or criminal law provisions, which focus primarily on technical violations rather than gendered or identity-driven harm.

"At present, there is no specific definition of TFGBV in our legal framework" (KII, Cyber Bureau).

This definitional gap has concrete operational consequences. The Cyber Bureau confirmed that it does not collect data on sexual orientation or gender identity, making LGBTIQ+-specific harms statistically invisible. Without disaggregated data, institutions are unable to identify patterns, allocate resources, or assess disproportionate impact.

"We do not currently have a system to record sexual orientation or gender identity of victims."

(KII, Cyber Bureau)

The National Human Rights Commission similarly reported receiving almost no complaints related to online violence, despite acknowledging high levels of community-reported harm. This discrepancy reflects not an absence of abuse, but a failure of institutional accessibility and trust.

"Till now, we have only received offline complaints; but in the next five or ten years online violence will be equally prominent as offline violence." (KII, NHRC)

Procedural design emerged as a further barrier. Reporting mechanisms were described as documentation-heavy, rigid, and intrusive, requiring victims to repeatedly disclose personal details and justify their claims. For LGBTIQ+ individuals, these procedures were perceived as particularly risky, as they often necessitate disclosure of identity without corresponding safeguards against discrimination or outing.

KIIs also highlighted gaps in institutional capacity and training. Respondents acknowledged limited understanding among frontline officials regarding sexual orientation, gender identity, and the dynamics of online harm. This contributes to inconsistent case handling and reinforces survivor perceptions of dismissal or ridicule.

Geographic inequities further exacerbate these challenges. State actors recognised that individuals in Madhesh, Karnali, and other marginalised regions face compounded barriers due to stronger social surveillance, limited digital literacy, and reduced proximity to specialised services.

"People from Madhesh and Karnali have it worse; one model cannot work for everyone."

(KII, Ministry stakeholder)

Across interviews, responsibility for addressing TFGBV was frequently diffused across agencies, with no single institution clearly mandated to lead. This fragmentation results in weak coordination between law enforcement, regulatory bodies, platforms, and civil society, leaving victims to navigate complex systems alone.

Taken together, the experiences of state and implementing bodies reveal a system that is structurally unprepared to address TFGBV affecting LGBTIQ+ communities. The absence of legal recognition, data visibility, survivor-centred procedures, and inter-agency coordination undermines access to justice and reinforces reliance on informal and community-based responses.

Chapter Summary

There are systemic gaps within Nepal's legal and institutional frameworks regarding TFGBV against LGBTIQ+ individuals which has led to increasing experiences of harm but lack of trust in reporting to authorities. The current punitive landscape takes a gender binary approach and fails to criminalise identity-based harms like "outing," often weaponising "public morality" clauses against the very communities they should protect. Procedural barriers and experiences of harassment from police further disenfranchise non-binary and transgender victims from approaching traditional justice mechanisms for help. While civil society organisations act as the primary frontline responders, they remain structurally under-resourced; a lack of disaggregated SOGIESC data invisibles the prevalence of TFGBV in LGBTIQ+ communities. The legislative trends toward mandatory identity verification, censorship, and shrinking civic spaces further marginalise the experiences of queer individuals using the internet and leave them more vulnerable.

Chapter 7: Capacity Gaps and Identified Needs

This chapter synthesises findings from the survey, FGDs, and KIIs to identify critical capacity gaps across three levels: LGBTIQ+ communities, civil society organisations, and state institutions. The analysis demonstrates that (TFGBV is not sustained by a single failure point, but by interacting deficits in knowledge, protection, trust, and institutional responsiveness. These gaps collectively shape how harm is recognised, managed, and addressed.

7.1 Capacity Needs of LGBTIQ+ Individuals

Findings indicate that LGBTIQ+ individuals experience high exposure to online harm while having limited access to formal tools, language, and systems for protection and redress. As a result, capacity gaps at the community level are not limited to skills deficits but are embedded in broader social and institutional constraints.

A key gap relates to knowledge and awareness. While exposure to online harassment and abuse is widespread, only 37.1% of survey respondents reported clearly understanding the term technology-facilitated gender-based violence. A further 35.7% had heard the term but were unsure of its meaning, and 25.7% had not encountered it at all. This disconnect highlights a gap between lived experience and formal terminology. Without shared language to name harm, individuals are left to assess incidents on their own, often minimising severity or normalising abuse as part of everyday life. This limits recognition of patterns, delays help-seeking and constrains engagement with available support mechanisms.

Capacity gaps were also evident in digital safety and risk management. Survey data show that 82.6% of respondents agreed or strongly agreed that LGBTIQ+ individuals avoid expressing themselves online due to fear of harassment or violence, and 61.4% reported changing how they use the internet following TFGBV experiences. FGDs revealed that individuals rely heavily on self-protective strategies such as maintaining multiple accounts, restricting visibility to closed groups, reducing posting, or avoiding certain platforms altogether. While these practices demonstrate resilience and adaptability, they also indicate that risk management is highly individualised and reactive. Safety is achieved primarily through withdrawal and self-censorship rather than through access to reliable protective systems.

Psychosocial capacity gaps were similarly pronounced. In total, 60.9% of respondents reported that TFGBV affected their mental or emotional health. FGDs described sustained anxiety, fear, exhaustion, and constant vigilance, particularly linked to the risk of being outed to family or community. Fear of exposure often shaped behaviour even when incidents were severe, contributing to silence and non-reporting. These findings indicate unmet needs for trauma- informed, identity-affirming psychosocial support that recognises the cumulative impact of repeated digital harm and the specific stress associated with outing-related threats.

Economic vulnerability further compounded these challenges. More than half of respondents (54.3%) reported that TFGBV affected their work, studies, or income-generating activities. FGDs highlighted particular vulnerability among trans women who rely on digital platforms for livelihood due to exclusion from formal

employment. For these individuals, disengaging from online spaces is not a viable safety strategy, as it may directly undermine economic survival. This underscores the need for livelihood-sensitive approaches to protection and support.

Taken together, these findings indicate that LGBTIQ+ communities require strengthened capacity not only in digital safety skills and rights awareness, but also in psychosocial resilience and access to confidential, trusted referral pathways. Current coping strategies, while adaptive, place a disproportionate burden on individuals and limit long-term safety and wellbeing.

7.2 Capacity Needs of Civil Society Organisations

CSOs play a central role in responding to TFGBV, yet findings reveal significant gaps between expectations placed on CSOs and their available capacity. Survey data show that 48.0% of respondents who disclosed their experiences reached out to an LGBTIQ+ organisation or community group, while only 2.0% contacted the police or Cyber Bureau. This positions CSOs as the primary response mechanism in practice, despite limited resources and authority.

FGDs and KIIs indicate that CSOs are perceived as safer and more accessible than state institutions, particularly because they offer identity-affirming support and reduce fear of discrimination or forced disclosure. However, this reliance has created a situation in which CSOs function as de facto first responders without adequate technical, legal, or institutional backing.

One major gap relates to technical and digital expertise. Although 75.4% of survey respondents reported using platform-level tools such as blocking, muting, or reporting, FGDs revealed low confidence in their effectiveness. CSOs reported limited capacity in digital evidence preservation, understanding platform moderation processes, and escalating cases with technology companies. As a result, support often focuses on harm reduction rather than accountability, and victims frequently experience repeated or escalating abuse despite taking action.

CSOs also face significant constraints in legal aid and case management. KIIs highlighted the absence of dedicated funding for TFGBV legal support, lack of standardised case documentation systems, and limited access to survivor-centred legal accompaniment. Without these systems, organisations struggle to track cases over time, identify repeat perpetrators, or generate evidence that could inform advocacy and policy engagement. Organisational sustainability and geographic reach further limit CSO capacity. Participants described being overstretched, particularly in cases involving blackmail, non-consensual image harms, and threats of outing. Support remains uneven outside urban centres, leaving individuals in high-stigma contexts with fewer options. These constraints mean that CSOs are often forced to prioritise immediate crisis response over longer-term protection or redress.

Overall, the findings suggest that while CSOs are essential actors in addressing TFGBV, their current capacity is insufficient to meet the scale and complexity of need. Strengthening CSO capacity is therefore critical not only for survivor support but also for building pathways to accountability and systemic change.

7.3 Institutional and State Capacity Gaps

At the institutional level, capacity gaps were evident across legal recognition, procedural safeguards, data systems, and frontline sensitivity. Survey findings show that 82.6% of respondents agreed or strongly agreed that TFGBV against LGBTIQ+ individuals is not taken seriously by authorities. KIIs confirmed that TFGBV is not recognised as a distinct legal category in Nepal and is addressed under general cybercrime provisions.

This lack of legal recognition limits accountability and contributes to inconsistent responses. Without clear definitions or guidance, cases are often handled as technical offences rather than as identity-based violence, reducing attention to risk assessment, survivor protection, and prevention of escalation.

Procedural barriers further deter engagement with formal mechanisms. 38.2% of respondents experienced threats of being outed as part of TFGBV incidents, and 24.5% cited fear of outing as a reason for not reporting. FGDs highlighted the absence of confidentiality safeguards and survivor-centred procedures in reporting processes. For many participants, reporting was perceived as a risk event, with the potential to trigger family rejection, community stigma, or economic harm.

Institutional capacity gaps are also reinforced by data and visibility limitations. State institutions do not systematically collect data on sexual orientation or gender identity, rendering LGBTIQ+- specific TFGBV largely invisible in official records. This limits evidence-based policymaking, resource allocation, and monitoring of institutional performance.

Finally, KIIs revealed limited training of frontline officials on SOGIESC issues, survivor-centred approaches, and the specific dynamics of identity-based digital harm. This lack of sensitivity contributes to mistrust and avoidance of formal mechanisms, reinforcing reliance on informal and community-based responses.

Taken together, these gaps indicate that institutional responses to TFGBV are constrained not only by legal frameworks but by procedural design, data practices, and human capacity. Without addressing these structural limitations, state systems are unlikely to gain the trust or engagement of LGBTIQ+ communities affected by technology-facilitated violence.

Chapter 8: Recommendations

This chapter outlines actionable, evidence-driven recommendations informed by a synthesis of quantitative survey findings, FGDs, KIIs, and the draft report. The recommendations address individual, community, institutional, and systemic drivers of TFGBV affecting LGBTIQ+ communities in Nepal. A Human-Centred Design (HCD) lens is applied throughout to ensure interventions are grounded in lived realities, responsive to diverse user needs, and designed for real-world feasibility. Funding implications are explicitly identified where external investment is required.

8.1 Policy and Legal Recommendations

1. Update the national legal framework on digital rights through a rights-based approach

   Rationale: Nepal's digital rights laws were designed for an earlier stage of internet use and mainly focused on vague ideas like "morality" or general cybercrime, rather than addressing the specific ways people are harmed online today. As a result, newer and highly relevant abuses such as NCII, sextortion, cyberstalking, impersonation, doxxing, and especially forced outing are not clearly defined or consistently handled, and victims often lack fast protection measures like takedown support, confidentiality safeguards, or urgent remedies. This gap disproportionately affects marginalised groups, including LGBTIQ+ individuals, who face higher risks of stigma, identity exposure, and offline violence if systems are not survivor centred.

   Implementation:
   Lead: Ministry of Law, Justice and Parliamentary Affairs (MoLJPA) with Nepal Law Commission and MoCIT

   Step: Initiate a national legal reform roadmap that centres user rights, consent, dignity, and privacy (rather than regulating technology itself) through a multi-stakeholder drafting taskforce including LGBTIQ+ representatives and disability advocates

2. Define TFGBV and "identity-based digital harms" in law and official guidance

   Rationale: When laws and policies do not clearly define TFGBV and identity-based digital harms, institutions interpret cases differently, leading to confusion about what counts as an offence, delays in action, and inconsistent decisions by police, prosecutors, and courts. This weakens survivor protection and allows serious harms such as outing, impersonation, and NCII to be minimised, misclassified, or dismissed, even though they can cause severe emotional distress, social exclusion, and real offline risks. The definition of crimes like harassment, domestic violence, blackmail and extortion, etc. which regulate these behaviours in offline spaces should also be expanded and implemented to cover cases of TFGBV.

   Implementation:
   Lead: MoLJPA with Ministry of Women Children and Senior Citizens (MoWCSC) and Cyber Bureau

   Step: Issue an official national TFGBV definition note and typology guidance for investigators, prosecutors, judges, and service providers, explicitly including outing, doxxing, impersonation, stalking, NCII, and sextortion

3. Section 47 of the Electronic Transactions Act (ETA) to remove vague morality-based language and adopt harm-based thresholds

   Rationale: Broad legal terms like "public morality" and "decency" are often interpreted subjectively, which allows authorities or complainants to misuse them against LGBTIQ+ individuals for simply expressing their identity online, sharing photos, or discussing

relationships. Instead of protecting victims from serious TFGBV such as stalking, blackmail, outing, or NCII, these clauses can shift the focus toward policing identity and expression, creating fear, discouraging reporting, and reinforcing discrimination rather than ensuring safety and justice. Any future legislation that will replace ETA must also ensure adoption of language that does not police the expressions of marginalised communities.

Implementation:
Lead: MoLJPA with Nepal Law Commission and Parliament

Step: Table an amendment package that replaces morality framing with clear definitions of TFGBV-related offences (NCII, sextortion, cyberstalking, impersonation) and introduces survivor safeguards and non-discrimination clauses.

4. Criminalise non-consensual outing and high-risk doxxing as specific offences under the Privacy Act

   Rationale: The study suggests that many LGBTIQ+ victims do not report TFGBV because they fear being outed to family, employers, or the wider community, which can trigger serious offline harm such as violence, forced displacement, loss of livelihood, family rejection, or social exclusion. This fear often leads victims to stay silent, withdraw from digital spaces, and rely only on informal coping strategies, which increases long-term vulnerability and allows perpetrators to act with impunity.

   Implementation:
   Lead: MoLJPA with Parliament and NHRC;

   Step: Amend the Privacy Act (2018) to explicitly criminalise outing and doxxing as identity-based violence and enable swift remedies such as cease orders and restraining protections

5. Safeguard online anonymity and pseudonymity in future digital regulation

   Rationale: Restricting anonymity or forcing real-name identity verification can make digital spaces unsafe for LGBTIQ+ individuals who are not openly out, especially youth and individuals living in highly conservative or stigmatising households. Without the option of pseudonyms, they may be exposed to family surveillance, harassment, blackmail, or forced outing, which can escalate into offline violence, homelessness, or loss of education and livelihood.

   Implementation:
   Lead: MoCIT with NHRC and MoLJPA

   Step: Adopt a rights-respecting national position rejecting blanket real-name policies and ensuring identity disclosure only through judicial warrant for serious offences

6. Amend GBV-related laws that use binary gender framing to ensure protection for all victims

   Rationale: When GBV laws are written only to protect "women" as victims and assume perpetrators are men, they fail to recognise violence experienced by trans men, non-binary people, and victims in same-sex relationships. This exclusion creates legal gaps where victims may not qualify for protection orders, survivor services, or justice processes, even when they face the same forms of sexual coercion, stalking, harassment, or digital abuse.

   Implementation:
   Lead: MoWCSC with MoLJPA

   Step: Revise relevant GBV and justice-related laws using gender-neutral terms such as "person" and expand definitions of family/intimate partner violence to include same-sex and live-in relationships, including digital surveillance and coercion.

7. Introduce fast civil protection remedies for TFGBV cases

   Rationale: Victims of TFGBV often need quick actions to stop ongoing harm such as removing abusive content, preventing further contact, or securing evidence without having to file a police case or go through a lengthy criminal process. For many LGBTIQ+ victims, criminal reporting can increase the risk of forced disclosure of their identity, stigma, and retaliation, so accessible civil remedies and confidential protection options are essential.

Implementation:
Lead: Supreme Court with MoLJPA

Step: Develop court procedures enabling rapid injunctions, takedown orders, non-contact orders, and evidence-preservation orders for NCII, impersonation, and stalking cases

8. Guarantee confidentiality and safe identity handling across justice and service systems

   Rationale: When authorities or service providers improperly record, share, or expose a survivor's SOGIESC information, it can lead to forced outing, community backlash, family rejection, and discrimination at work or in education. This not only increases the risk of physical violence and economic harm, but can also retraumatise victims during the reporting process, creating secondary victimisation and discouraging others from seeking help.

   Implementation:
   Lead: Ministry of Home Affairs (MoHA) with Nepal Police and Cyber Bureau

   Step: Issue a binding directive prohibiting unnecessary disclosure of SOGIESC and enforcing disciplinary action for confidentiality breaches

9. Remove procedural and documentation barriers that exclude victims from reporting and remedy

   Rationale: Many LGBTIQ+ victims cannot safely use formal identification documents because their citizenship name or gender marker may not match their lived identity, or they may be migrants without complete documentation. In such cases, police or service providers may refuse to register complaints, delay services, or treat victims with suspicion, effectively blocking access to protection, legal aid, and justice.

   Implementation:
   Lead: MoHA and Cyber Bureau

   Step: Revise complaint SOPs to allow alternative identity verification pathways (trusted referrals, confidential verification) while ensuring data minimisation and privacy protections

10. Institutionalise a national TFGBV monitoring framework with voluntary, safe disaggregation

    Rationale: When TFGBV cases are not recorded in safe and ethical ways, the scale and patterns of harm remain invisible in national systems, which leads to weak policy attention and underfunding of survivor services. Without reliable data, institutions also cannot identify high-risk groups or regions, design targeted prevention measures, or track whether authorities and service providers are responding effectively.

    Implementation:
    Lead: MoWCSC with NHRC and Central Bureau of Statistics

    Step: Publish an annual de-identified TFGBV report capturing trends, institutional gaps, and service coverage, disaggregated where safe by province, age, disability, caste/ethnicity, and voluntary SOGIESC markers.

8.2 Capacity-Building Recommendations for LGBTIQ+ individuals

1. Design and deliver practical digital safety training using Human-Centred Design (HCD) approaches

   Rationale: the study indicates that many LGBTIQ+ individuals actively adapt their online behaviour to stay safe, such as using multiple accounts, limiting visibility, self-censoring, or abandoning platforms altogether. While these strategies show resilience and awareness of risk, they are often emotionally exhausting, socially isolating, and difficult to sustain over time, especially without access to clear guidance, technical skills, or supportive resources that could reduce harm without forcing people offline.

   Implementation:
   Lead: BDS with FSGMN and digital rights partners

   Step: Conduct rapid HCD mapping of real user journeys (shared phones, family surveillance, low literacy) and roll out peer-led modular training on privacy settings, secure messaging, account recovery, and safe platform use.

2. Develop survivor-informed rapid response protocols for outing threats, sextortion, and NCII

Rationale: Coercive forms of TFGBV such as outing threats, sextortion, and blackmail can escalate very quickly, often within hours, leaving victims with little time to seek support or plan a safe response. Because these harms are closely tied to social stigma, they can trigger immediate offline consequences such as family violence, eviction, loss of housing, forced relocation, or being pushed out of education and employment, making rapid response mechanisms critical for protection.

Implementation:
Lead: LGBTIQ+ community networks

Step: Co-design a one-page emergency protocol (what to do in the first 2 hours, 24 hours, 72 hours) and distribute through encrypted channels and local focal points in accessible formats (audio, visual, simplified text).

3. Establish province-level peer "digital first aid" teams with safeguarding boundaries

   Rationale: The study suggests that victims often turn first to trusted friends, peers, or community members because these spaces feel safer, more understanding, and less judgmental than formal institutions. In contrast, reporting to police or cyber authorities is often perceived as risky due to fear of discrimination, forced outing, humiliation, or lack of confidentiality, which makes peer support the most accessible and immediate pathway for help.

   Implementation:
   Lead: FSGMN with provincial level networks/groups of LGBTIQ+ individuals.

   Step: Train focal persons on evidence preservation, platform reporting, safety planning, and referral pathways, while ensuring confidentiality and limits to peer intervention to prevent harm.

4. Integrate psychosocial support and trauma-informed coping into digital safety programming

   Rationale: The study indicates that TFGBV often causes long-term emotional harm that continues even after the abusive incident ends, including persistent anxiety, fear of being monitored or exposed, sleep disturbance, and loss of confidence. Many victims respond by withdrawing from online spaces, limiting communication, and isolating themselves socially to avoid further harm, which can deepen emotional distress and reduce access to support networks and information.

   Implementation:
   Lead: LGBTIQ+ CSOs with trained counsellors

   Step: Embed mental well-being modules in training, provide referral lists for crisis counselling, and ensure disability-inclusive access (sign interpretation, accessible formats).

5. Strengthen legal literacy through realistic "Know Your Options" materials

   Rationale: When victims and communities do not clearly understand what the law covers, what reporting options exist, and what risks are involved, they may make decisions that unintentionally increase harm. Some may delay seeking support because they assume nothing can be done, while others may report without understanding confidentiality limitations, which can increase the risk of outing, retaliation, or secondary victimisation.

   Implementation:
   Lead: Community legal clinics and CSO lawyers

   Step: Develop survivor-informed guidance explaining what the law currently offers, risks of disclosure, confidentiality limits, and non-police pathways in plain language and local languages.

6. Apply an intersectional lens to all community interventions and tailor delivery models

   Rationale: The study indicates that TFGBV does not affect all LGBTIQ+ individuals in the same way, because risk exposure and ability to respond are shaped by multiple intersecting factors. Trans and gender non-conforming individuals may face greater visibility and targeting, while people from marginalised caste/ethnic groups, persons with disabilities, migrants, and those living in rural or high-stigma areas may have fewer safe support networks and less access to services. Economic vulnerability further limits options, as some victims cannot simply leave digital platforms if they rely on them for income, making tailored and context-specific protection approaches essential.

Implementation:
Lead: Organisations working on LGBTIQ+ issues, and their allies

Step: Develop persona-based training tracks (e.g., trans women in small towns, queer youth in family homes, migrants in cities, hearing impairment queer victims) and implement decentralised delivery using local facilitators.

7. Create targeted economic safety measures for high-risk groups

   Rationale: Victims who rely on digital platforms for income, including sex workers, informal workers, migrants, and people excluded from formal employment, often cannot simply reduce their online presence even when abuse occurs. For them, leaving a platform may mean losing clients, income, and livelihood opportunities, which forces continued exposure to unsafe spaces and increases vulnerability to repeated harassment, blackmail, and exploitation.

   Implementation:
   Lead: CSO coalition with donors

   Step: Establish small "digital safety microgrants" to support safer devices, SIM replacement, secure storage tools, and urgent safe travel for high-risk cases.

8. Adopt community accountability norms within digital community spaces

   Rationale: TFGBV does not only come from strangers or anonymous accounts. It can also happen within LGBTIQ+ networks, friendships, relationships, or community spaces, including through harassment, blackmail, stalking, or non-consensual sharing of private information. Victims therefore need safe internal mechanisms within community groups to report harm, seek support, and prevent retaliation, without being silenced or forced to leave their support networks.

   Implementation:
   Lead: Community moderators and peer leaders

   Step: Introduce codes of conduct, anti-retaliation policies, and confidential moderation pathways for groups/pages/dating networks, ensuring survivor consent and safety-first responses.

9. Maintain consent-based community incident tracking for prevention planning

   Rationale: Tracking TFGBV patterns in an ethical and confidential way helps communities and service providers understand what types of abuse are increasing, which platforms are being used, and which groups are being targeted most. When done carefully with consent and minimal personal data, this kind of monitoring strengthens prevention planning and service delivery without exposing victims or putting individuals at risk of further harm.

   Implementation:
   Lead: BDS/FSGMN networks

   Step: Use minimal-data templates and quarterly trend reviews to guide targeted outreach by province and identity group, ensuring strict consent and de-identification safeguards.

8.3 Recommendations for Civil society organisations and Service Providers

1. Standardise survivor-centred TFGBV case management systems across CSOs

   Rationale: the study indicates that TFGBV cases are often handled informally, which can lead to repeated retelling of traumatic experiences, inconsistent documentation, missed referrals, and higher risk of confidentiality breaches. When each organisation follows a different approach, victims may receive unequal support depending on where they seek help, and critical evidence may be lost early in the process. A standardised system also helps CSOs build institutional learning over time, improve service quality, and ensure that survivor consent and safety remain central in every step.

   Implementation:
   Lead: CSO coalition with MoWCSC support

   Step: Co-develop and adopt a shared intake, risk screening, consent, and referral template that collects SOGIESC information only when voluntary, necessary, and safe.

2. Provide integrated one-stop TFGBV support services through hybrid models (in-person + remote)

   Rationale: Victims outside Kathmandu often have limited access to trained lawyers, counsellors, and safe referral services, and traveling to reach support can be costly, unsafe, and highly visible. For many LGBTIQ+ victimsvictims, even seeking help locally can carry a risk of being recognised or outed, especially in small communities. This makes coordinated, multi-service support essential so victims can receive legal, psychosocial, and protection assistance through a single safe entry point rather than navigating multiple institutions.

Implementation:

Lead: LGBTIQ+ CSOs with donor support

Step: Pilot a centralised helpline and referral desk that links legal aid, psychosocial support, digital safety guidance, and emergency protection planning with strict follow-up consent protocols.

3. Offer crisis response pathways that do not require police involvement

Rationale: The study indicates that fear of discrimination, secondary victimisation, and forced outing prevents many victimsvictims from approaching law enforcement, even in high-risk cases. Victims often worry that police officers may not take their complaint seriously, may blame them for the abuse, or may treat their sexual orientation or gender identity as the problem rather than the violence itself. There is also a strong fear that reporting could expose their identity to family, employers, or the wider community through careless questioning, documentation, or leaks, which could trigger serious offline harm. As a result, many victims choose silence or rely only on informal support networks, allowing perpetrators to continue with little accountability.

Implementation:

Lead: CSO consortium

Step: establish a 24/7 emergency roster of counsellors and legal responders with consent-based escalation steps, safe shelter referrals, and clear confidentiality commitments.

4. Expand rapid legal remedy services for NCII, impersonation, stalking, and blackmail

Rationale: TFGBV incidents often escalate quickly, and victims need immediate support for takedown requests, evidence preservation, and legal safety planning before harm spreads further. Once abusive content is posted or private information is leaked, it can be rapidly shared across multiple platforms, copied by others, and become impossible to fully remove. Victims may also be pressured into silence through threats or blackmail, making early legal intervention critical to prevent further exploitation. Immediate assistance helps victims secure screenshots, URLs, and digital evidence properly, while also reducing the risk of panic-driven actions such as deleting accounts or messages that could weaken future legal options.

Implementation:

Lead: legal aid CSOs with Nepal Bar Association allies

Step: create a roster of vetted lawyers trained on TFGBV, confidentiality, trauma-informed practice, and court-ready documentation, with rapid response protocols for cease notices and takedown escalation

5. Establish a dedicated TFGBV legal aid and emergency response fund

   Rationale: The study suggests that victims frequently lack the financial capacity to pursue urgent legal remedies, relocate temporarily, replace devices, or access counselling, which increases vulnerability and impunity. Many victims face economic insecurity and may not be able to afford lawyer fees, transport costs, or even basic expenses required to respond quickly to digital abuse. In cases involving blackmail, outing threats, or NCII, victims may also need immediate support for safe housing, emergency travel, SIM replacement, or secure communication tools, but these options are often out of reach. Without financial support, victims are forced to tolerate abuse, withdraw from online spaces, or comply with perpetrators' demands, allowing harm to continue without accountability.

Implementation:
Lead: CSO coalition with donors and MoWCSC partnership

Step: Create a small flexible fund that can be accessed within 24–48 hours through verified CSO referrals, with transparent eligibility and safeguarding criteria

6. Conduct participatory survivor-informed trainings for service improvement

   Rationale: Training designed without survivor input often fails to reflect the real risks and lived realities that victims face, especially around confidentiality, fear of outing, and unsafe institutional responses. Generic trainings may encourage reporting without acknowledging the stigma, discrimination, and retaliation that LGBTIQ+ victims can experience when approaching police, health providers, or even community structures. When these concerns are ignored, services can unintentionally feel unsafe or irrelevant, which reduces trust and discourages victims from seeking support. Participatory, survivor-informed training ensures that service providers learn practical, context-specific responses that victims actually need, improving both service quality and uptake.

   Implementation:
   Lead: CSOs and survivor networks

   Step: Run participatory training and reflection sessions using anonymised case scenarios, role plays, and survivor-informed feedback to strengthen staff practice on consent, confidentiality, and safety planning.

7. Strengthen CSO capacity to engage digital platforms and document platform inaction

   Rationale: Victims often report that platform reporting systems are confusing, slow, and inconsistent, and without expert support many give up, leaving abusive content active. Reporting options are frequently buried in menus, written in technical language, or require victims to choose categories that do not match identity-based harms like outing or targeted harassment. Even when reports are submitted, responses can be delayed, automated, or unclear, and victims may not know how to appeal decisions or escalate urgent cases. This creates frustration and exhaustion, especially when abuse is ongoing, and it forces victims to carry the burden of repeated reporting while perpetrators continue using new accounts or platforms.

   Implementation:
   Lead: Digital Rights Nepal with CSO partners

   Step: Develop a shared "platform escalation playbook" with templates for NCII takedown requests, impersonation complaints, evidence preservation steps, and documentation of repeat abuse for advocacy use.

8. Institutionalise minimum SOGIESC-affirming and disability-inclusive service standards

   Rationale: The study indicates that fear of judgment, misgendering, breach of confidentiality, and ableist service barriers discourages victims from seeking support and increases isolation. Many victims worry that service providers may not respect their identity, may ask invasive questions, or may treat them with stigma, which can feel as harmful as the abuse itself. Victims also fear that staff may unintentionally disclose their identity to family or community members, especially in small towns where privacy is difficult to maintain. For persons with disabilities, additional barriers such as inaccessible buildings, lack of sign language interpretation, or communication formats that exclude low-literacy users further reduce access. As a result, many victims withdraw from both digital and offline spaces, relying only on silence and self-protection rather than seeking help.

   Implementation:
   Lead: CSO networks

   Step: Implement service standards covering non-outing practices, informed consent, accessible communication, disability accommodations, and confidentiality audits, with routine survivor feedback loops to monitor quality.

9. Establish survivor-facing complaint and feedback mechanisms for CSO services Rationale: Victims need safe ways to report mistreatment, discrimination, or negligence by service providers without fear of retaliation or losing access to support. If victims feel that raising concerns will lead to judgment, being ignored, or being excluded from services, they are more likely to remain silent even when

harm is repeated. Confidential feedback mechanisms help ensure that services remain accountable, improve quality over time, and build trust, especially for victims who have already experienced stigma and betrayal in other institutions.

Implementation:
Lead: Service providers

Step: Set up anonymous complaint channels (voice, SMS, online) with a clear response timeline and public reporting of improvements in aggregated form.

10. Invest in prevention campaigns targeting non-LGBTIQ+ audiences and online bystanders

    Rationale: TFGBV is reinforced by stigma, moral policing, and Normalised hate speech, and without broader social norm change, victims remain unsafe even when support services exist. The study suggests that online abuse is often enabled by social attitudes that view LGBTIQ+ identities as shameful or unacceptable, which encourages perpetrators to harass, threaten, or publicly expose individuals without fear of consequences. In these environments, bystanders may stay silent or even participate in abuse, and victims may be blamed rather than supported. Without efforts to shift harmful norms and promote respect and accountability, TFGBV will continue to be treated as "normal," and victims will remain at risk of repeated violence and exclusion.

    Implementation:
    Lead: CSOs with media partners and local governments

    Step: Design BCC campaigns using HCD methods, engaging schools, youth influencers, employers, and local media in province-specific languages and culturally grounded narratives that reduce prejudice and promote accountability.

11. Establish a Community of Practice (CoP) on TFGBV response and prevention

    Rationale: Fragmented approaches across CSOs limit learning, quality improvement, and coordinated advocacy, which ultimately weakens both national influence and survivor outcomes. When organisations work in isolation, they often duplicate efforts, use different case handling practices, and miss opportunities to share tools, lessons, and effective response strategies. This also makes it harder to present a unified evidence base to government and donors, reducing the ability to push for legal reform, stronger institutional accountability, and sustainable funding. A coordinated approach strengthens consistency of survivor support and increases collective power to influence policy and systems change.

    Implementation:
    Lead: CSO coalition with donor facilitation

    Step: Convene quarterly learning forums to share tools, case trends, referral pathways, legal updates, and platform engagement strategies, with rotating provincial leadership to ensure decentralisation.

12. Train lawyers and paralegals on TFGBV and SOGIESC-affirming legal practice

    Rationale: Many lawyers lack competency on digital evidence, survivor-centred handling, and SOGIESC risks, which can lead to unsafe advice, victim-blaming, or identity exposure. Victims may be told to take actions that weaken evidence, such as deleting messages or accounts, or may not receive proper guidance on how to document abuse in a legally usable way. In addition, lawyers who are not trained on SOGIESC realities may unintentionally misgender victims, minimise the harm, or treat identity disclosure as unavoidable, increasing the risk of forced outing and secondary trauma. Without specialised training, legal processes can become another site of harm rather than a pathway to justice.

    Implementation:
    Lead: Nepal Bar Association with CSO legal aid partners

    Step: Develop and deliver a certified TFGBV legal training module including confidentiality, trauma-informed interviewing, and identity-sensitive litigation practice.

13. Advocate for inclusion of SOGIESC and TFGBV content in law school curriculum and professional legal education

    Rationale: Long-term institutional change requires embedding queer rights and digital harm frameworks into legal education so future lawyers, judges, and

prosecutors are prepared to respond appropriately. If SOGIESC and TFGBV are not part of formal legal training, professionals enter the justice system with outdated assumptions about gender, sexuality, consent, and privacy. This leads to inconsistent interpretation of laws, weak enforcement, and a continued culture of stigma within legal institutions. Including these issues in law school curricula and professional training ensures that future duty bearers treat TFGBV as a rights violation and apply survivor-centred legal reasoning from the start, rather than relying on ad hoc sensitisation later.

Implementation:
Lead: Nepal Bar Council, universities, and law faculties with NHRC and CSO input

Step: Develop curriculum modules on SOGIESC rights, digital privacy, TFGBV typologies, and ethical handling of identity-based cases, and integrate them into formal teaching and continuing legal education.

14. Publish periodic de-identified TFGBV trend briefs for policy advocacy

Rationale: Ethical evidence helps demonstrate emerging patterns, regional hotspots, and service gaps while protecting survivor identities, strengthening the case for reform and budget allocation. When data is collected safely and reported in de-identified form, it becomes possible to show what forms of TFGBV are increasing, which provinces or communities are most affected, and where institutional responses are failing. This evidence is critical for convincing policymakers that TFGBV is not an isolated issue, but a systemic problem requiring legal reform, trained personnel, and dedicated resources. Ethical trend reporting also helps CSOs and the state target prevention strategies more effectively, while ensuring that victims are not put at further risk through exposure or careless documentation.

Implementation:
Lead: CSO coalition.

Step: Release quarterly aggregated briefs highlighting tactics, service barriers, institutional responses, and emerging risks such as AI-enabled abuse, disaggregated only when safe and voluntary.

8.4 Recommendations for State Institutions and Duty Bearers

1. Create confidential, identity-sensitive TFGBV reporting pathways

Rationale: The study indicates that equal procedures do not create equal safety because LGBTIQ+ victims face specific risks that others may not, particularly the fear of being outed to family, employers, or the wider community. Many victims anticipate discrimination, moral judgment, or humiliating treatment when approaching police or government offices. In such contexts, reporting is not experienced as a neutral process but as a potential trigger for further violence and social exclusion. As a result, victims are unlikely to come forward unless confidentiality is clearly guaranteed and consistently practiced.

Implementation:
Lead: National Women Commission with MoWCSC;

Step: Integrate an LGBTIQ+-inclusive TFGBV intake option within existing GBV reporting systems (hotline, online portal, SMS), with clear privacy statements and referral links to CSOs.

2. Adopt survivor-centred SOPs for TFGBV investigation, evidence handling, and harm containment

Rationale: The study suggests that delays and poor evidence handling can significantly worsen TFGBV impacts, because digital abuse spreads rapidly and becomes difficult to control once shared. Harmful images, screenshots, or false posts can be copied across multiple platforms within a short period, increasing the survivor's exposure and distress. When institutions fail to preserve evidence early, victims may lose critical proof needed for accountability. Weak response time therefore directly contributes to escalation, repeat abuse, and long-term harm.

Implementation:
Lead: Nepal Police and Cyber Bureau

Step: Issue an SOP annex on TFGBV including risk assessment, evidence preservation, takedown request

procedures, survivor safety planning, and confidentiality safeguards.

3. Establish dedicated queer-inclusive TFGBV "safe reporting cells" within Cyber Bureau and provincial police offices

   Rationale: The study indicates that victims need reporting spaces where their identity is treated with dignity and not framed through "morality" or stigma, because TFGBV targeting LGBTIQ+ individuals is often rooted in discrimination and social prejudice. Victims fear that officials may misgender them, question their character, or treat the abuse as a consequence of their identity rather than a violation of rights. Confidentiality must be actively protected because cases involving outing threats, sextortion, and impersonation carry immediate risks of offline violence, family rejection, and livelihood loss. Safe reporting spaces therefore require trained staff, private intake systems, and clear protections against information leakage.

   Implementation:
   Lead: Cyber Bureau with MoHA and NHRC oversight

   Step: Pilot queer-inclusive TFGBV cells in Kathmandu and at least two provinces with private intake rooms, trained staff, and formal referral MoUs with LGBTIQ+ CSOs.

4. Clarify legal guidance on how existing laws apply to TFGBV until reforms are enacted

   Rationale: The study suggests that legal ambiguity results in inconsistent enforcement because frontline actors interpret digital harms differently and often lack clear guidance on how existing laws apply to TFGBV. In many cases, identity-based harms such as outing, impersonation, and harassment may be dismissed as "personal disputes" rather than treated as serious violence. This inconsistency weakens deterrence and creates gaps where perpetrators can exploit unclear legal definitions. Over time, it contributes to impunity by signalling that identity-based digital abuse is unlikely to result in accountability.

   Implementation:
   Lead: Office of the Attorney General with MoLJPA

   Step: Issue prosecution guidance identifying applicable offences (privacy violations, threats, impersonation, NCII) and embedding survivor safeguards and non-discrimination obligations.

5. Enforce accountability for discriminatory conduct and confidentiality breaches by officials

   Rationale: The study indicates that victims avoid reporting when state systems reproduce stigma, leak identity information, or dismiss queer victims, because these experiences create secondary victimisation and deepen mistrust. Even one case of mishandled confidentiality or discriminatory treatment can spread fear within communities and discourage others from seeking help. Victims may feel that the system is not designed for their safety but instead reinforces the same prejudice they face online. This dynamic strengthens silence and underreporting, allowing TFGBV to remain hidden and enabling perpetrators to continue without consequences.

   Implementation:
   Lead: NHRC with MoHA;

   Step: Establish a confidential complaints pathway for misconduct and require annual reporting of disciplinary actions in aggregated form.

6. Institutionalise mandatory TFGBV and SOGIESC competency training for frontline officials

   Rationale: The study indicates that poor handling of TFGBV cases can create secondary victimisation, where victims are harmed again through the very system they approach for protection. This may include misgendering, insensitive questioning, victim-blaming, or treating queer identity as a "moral issue" rather than recognising the abuse as a rights violation. Such experiences reinforce fear and shame, discourage victims from continuing the complaint process, and reduce the likelihood that others in the community will report similar harms. Over time, this deepens mistrust in state institutions and strengthens impunity for perpetrators.

Implementation:
Lead: MoHA with Attorney General's Office and Judicial Council

Step: Develop a competency-based curriculum with certification and refresher requirements tied to performance accountability, not one-off Sensitisation training.

7. Decentralise TFGBV desks and focal points across all seven provinces

   Rationale: The study indicates that access to TFGBV response mechanisms is highly uneven outside Kathmandu, with limited availability of trained personnel, specialised desks, and survivor-friendly referral services in many provinces and districts. Victims in rural and semi-urban areas often face greater barriers because seeking help is more visible, privacy is harder to maintain, and community stigma is stronger. For LGBTIQ+ individuals in particular, reporting can carry a high risk of being recognised or outed, which may lead to family violence, exclusion, or loss of livelihood. These realities make decentralised and confidential response systems essential to ensure equitable access to protection and justice.

   Implementation:
   Lead: Cyber Bureau with provincial ministries and local police

   Step: Establish provincial TFGBV desks staffed by trained officers, ensuring disability-accessible facilities and safe referral protocols.

8. Recruit and Institutionalise LGBTIQ+ frontline focal persons within TFGBV response systems

   Rationale: The study suggests that victims are more likely to seek help when there is at least one visibly safe and affirming entry point within state institutions, such as a trained focal person or a dedicated queer-inclusive desk. This reduces fear of harassment, misgendering, humiliation, or moral policing during the reporting process. When victims know there is someone who understands SOGIESC realities and can ensure confidentiality, they are more likely to disclose abuse early and pursue support options. Such entry points also reduce secondary victimisation and help rebuild trust between LGBTIQ+ communities and duty bearers.

   Implementation:
   Lead: MoHA with Nepal Police and Cyber Bureau

   Step: Appoint at least one LGBTIQ+-inclusive TFGBV focal person within each provincial desk, with a defined mandate for confidential intake, referral coordination, and safety planning.

9. Engage digital platforms through rights-respecting accountability mechanisms Rationale: Platforms play a central role in amplifying TFGBV because abusive content, impersonation accounts, or outing threats can spread rapidly through shares, screenshots, and coordinated harassment. The study suggests that victims often struggle to navigate platform reporting systems, and even when reports are submitted, responses may be slow, inconsistent, or automated. Without clear escalation mechanisms and trusted communication channels between the state, service providers, and platforms, takedowns are delayed and victims remain exposed to ongoing humiliation, blackmail, and repeated attacks. Faster and more reliable escalation pathways are therefore essential to contain harm and prevent further spread.

   Implementation:
   Lead: MoCIT with Cyber Bureau and NHRC

   Step: Establish formal point-of-contact and escalation protocols for urgent takedown cases (NCII, impersonation, outing threats) and require periodic transparency reporting.

10. Improve state data systems to safely capture identity-based digital harm

    Rationale: The absence of SOGIESC-sensitive data means that TFGBV experienced by LGBTIQ+ communities is often missing from official reporting and national planning systems. When identity-based harms are not documented in a safe and voluntary way, policymakers may underestimate the scale, severity, and distinct patterns of violence affecting queer and trans individuals.

This invisibility weakens prevention strategies because institutions cannot identify who is most at risk, which regions face higher exposure, or what forms of abuse are increasing. It also limits budget justification, as dedicated funding for inclusive survivor services and specialised response mechanisms becomes harder to argue for without credible evidence.

Implementation:
Lead: MoWCSC with Cyber Bureau and CBS

Step: introduce voluntary, consent-based SOGIESC markers and intersectional indicators in administrative systems with strict access controls and data minimisation principles.

11. Allocate dedicated national and provincial budgets for TFGBV prevention and survivor support

    Rationale: Without dedicated resources, TFGBV policies often remain symbolic commitments rather than practical systems of protection. The study suggests that many victims, especially outside urban centres, have limited access to legal aid, psychosocial counselling, safe shelters, and digital safety support, even when policies exist on paper. If provincial and local institutions are not funded to operationalise response mechanisms, victims are left with no realistic pathways to seek help. Sustainable budget allocation is therefore essential to ensure services reach rural and marginalised communities and provide meaningful support in all parts of the country.

    Implementation:
    Lead: MoWCSC with Ministry of Finance and provincial governments

    Step: Create budget lines for survivor support, legal aid, psychosocial services, and accessible reporting infrastructure, including rural outreach and disability-inclusive access.

12. Strengthen inter-agency coordination through formal referral and accountability systems

    Rationale: The study suggests that institutional fragmentation forces victims to move between multiple offices and service providers, often without clear guidance or referral pathways. This increases the likelihood of drop-off, as victims may feel overwhelmed, fear exposure, or lose trust after repeated delays and bureaucratic barriers. It also increases the risk of harm because victims may be required to repeat their story multiple times and disclose sensitive personal information to different actors, raising the possibility of identity leaks or secondary victimisation. Strong coordination and clear referral systems are therefore essential to reduce survivor burden and ensure timely, safe access to support.

    Implementation:
    Lead: MoWCSC with MoHA and NHRC

    Step: establish a national TFGBV coordination mechanism with defined roles, referral protocols, quarterly review meetings, and public progress tracking in aggregated form.

8.5 Implications for Programming and Donor Investment

1. Fund integrated TFGBV protection ecosystems rather than isolated interventions

   Rationale: The study indicates that victims experience fragmented and inconsistent support, where legal aid, psychosocial care, digital safety assistance, and institutional response mechanisms operate in silos. Standalone awareness or training activities may improve knowledge but do not address what victims need most during crisis situations: rapid harm containment, confidential referral pathways, and long-term protection. Without integrated systems, victims are forced to navigate multiple institutions alone, increasing drop-off, repeated exposure of sensitive information, and secondary victimisation.

   Funding required: Integrated survivor support models, referral system development, coordination platforms, digital safety response teams, case management systems, and multi-sector service delivery pilots.

2. Provide sustained, flexible core funding to LGBTIQ+ Organisations as a protection and prevention strategy

   Rationale: The study suggests that LGBTIQ+ Organisations are often the first and safest entry point for victims,

particularly when formal institutions are feared due to discrimination and confidentiality risks. However, short-term project funding weakens continuity of care and limits the ability of these organisations to respond to rapidly evolving digital threats such as sextortion, impersonation, and outing-based blackmail. Flexible multi-year funding is essential for building institutional capacity, maintaining trained staff, and extending support services beyond Kathmandu into provinces where access remains limited.

Funding required: Core organisational grants, emergency response reserves, staffing and operational costs, provincial outreach expansion, infrastructure for confidential service delivery, and long-term institutional strengthening support.

3. Treat legal aid and institutional reform as central pillars of protection programming

   Rationale: The study indicates that TFGBV is sustained by impunity, weak enforcement, and inconsistent institutional handling, meaning coping-focused interventions alone cannot reduce harm. Victims require access to legal advice, evidence preservation support, takedown assistance, and safe justice pathways, especially for cases involving NCII, sextortion, and outing threats. At the same time, institutional reform is critical because without trained duty bearers and survivor-centred procedures, reporting systems can become sites of further harm. Legal aid and institutional strengthening must therefore be treated as core protection strategies, not optional add-ons.

   Funding required: Legal accompaniment rosters, emergency legal aid funds, paralegal training, survivor-friendly litigation support, institutional training reforms, court support pilots, and development of confidentiality-focused SOPs.

4. Invest in structural prevention through national norm-change and stigma reduction strategies.

   Rationale: The study indicates that TFGBV against LGBTIQ+ communities is driven by stigma, moral policing, and deeply Normalised hostility, which enables perpetrators to act without fear of social consequences. Even when survivor services exist, prevention remains weak if broader communities continue to view outing, harassment, and digital humiliation as justified or "deserved." Sustainable prevention therefore requires long-term behaviour and norm change approaches that target bystanders, families, gatekeepers, and institutions that reproduce discrimination. Without stigma reduction, reporting will remain low and victims will continue to self-censor and withdraw from digital spaces.

   Funding required: National-level behaviour change strategy development, formative research, message co-creation, multimedia campaign production, community engagement approaches, partnerships with influencers/media, and sustained prevention communication rollouts.

5. Mainstream TFGBV prevention into national education and digital citizenship systems

   Rationale: Prevention requires institutional investment in long-term social behaviour change, especially as youth are among the most active digital users and are highly exposed to harassment, coercion, and online exploitation. The study suggests that many harmful behaviours, including impersonation, bullying, and circulation of intimate content, are Normalised among peer networks and rarely understood as violence. Embedding TFGBV prevention into education systems creates a long-term foundation for consent-based digital behaviour, respectful online engagement, and early recognition of coercion and blackmail. This also reduces the burden on survivor services by addressing harmful norms before violence escalates.

   Funding required: Curriculum integration, teacher training, youth-focused learning materials, digital citizenship modules, school safeguarding system strengthening, and development of age-appropriate prevention content in local languages and accessible formats.

6. Invest in platform accountability and "safety-by-design" engagement as a prevention measure

   Rationale: The study suggests that platform design gaps, slow reporting systems, and weak accountability structures allow TFGBV to spread quickly and repeatedly, especially in cases of impersonation and NCII. Victims

often face confusing reporting processes, delayed takedowns, and lack of clear escalation pathways, which leaves harmful content active for extended periods. Prevention therefore requires engaging platforms as duty bearers in a rights-based manner, pushing for improved reporting architecture, faster response mechanisms, and protections for pseudonymity. Without sustained engagement, victims remain dependent on inconsistent platform goodwill rather than predictable remedy systems.

Funding required: Digital platform advocacy, technical expertise for safety audits, development of escalation toolkits, documentation of platform response gaps, legal-policy engagement support, and multi-stakeholder accountability forums.

7. Support national-level monitoring systems to identify emerging TFGBV risks early

   Rationale: Prevention requires early detection of emerging trends such as AI-enabled abuse, deepfake extortion, and coordinated hate campaigns, which can escalate faster than institutional response capacity. The study indicates that without systematic monitoring, new forms of abuse remain undocumented until widespread harm occurs, limiting timely prevention and policy response. National-level monitoring also strengthens evidence-based advocacy by identifying regional hotspots, emerging tactics, and gaps in survivor support coverage. If ethical monitoring is absent, TFGBV remains invisible in planning processes and donors lack the evidence needed to justify sustained investment.

   Funding required: Ethical monitoring systems, de-identified data dashboards, trend analysis capacity, community reporting mechanisms, research partnerships, publication of periodic risk briefs, and technical support for secure data management.

8. Finance preventive digital literacy programs linked to real response mechanisms and survivor pathways

   Rationale: The study indicates that digital safety awareness alone is insufficient when victims have no accessible referral systems, legal aid, or psychosocial support once harm occurs. Many victims may learn basic privacy practices but remain vulnerable to coercion, blackmail, and repeat abuse without crisis response mechanisms that can intervene quickly. Digital literacy must therefore be treated as part of a broader prevention-to-response continuum, not as an isolated training product. Linking literacy programs with survivor support pathways also increases trust and ensures that knowledge translates into real protection outcomes.

   Funding required: Digital safety training development, peer educator models, survivor-informed training materials, low-literacy and disability-accessible formats, referral linkage systems, emergency response funds, and ongoing mentorship/support mechanisms.

8.6 Conclusion

This study establishes that TFGBV against LGBTIQ+ communities in Nepal is a widespread and systemic form of violence situated at the intersection of digital expansion, entrenched social stigma, and uneven institutional protection. The findings demonstrate that digital spaces have become essential environments for communication, identity expression, livelihood opportunities, and community formation for many LGBTIQ+ individuals. At the same time, these spaces expose users to targeted harassment, impersonation, coercion, blackmail, and threats of non-consensual disclosure of sexual orientation or gender identity. TFGBV, therefore cannot be understood solely as a technological issue; rather, it reflects broader social inequalities that shape vulnerability, visibility, and access to protection.

The study reveals a significant gap between the prevalence of harm and engagement with formal reporting mechanisms. Victims frequently avoid institutional pathways due to anticipated discrimination, breach of confidentiality, moral judgment, and the risk of forced outing. Low reporting should therefore not be interpreted as low incidence, but as an indicator of limited institutional trust and inadequate survivor-centred safeguards. The findings suggest that existing legal and response systems, while formally available, do not yet provide conditions

under which many LGBTIQ+ individuals feel safe seeking remedy. As a result, informal peer networks and civil society organisations continue to function as primary sources of support, highlighting both community resilience and structural gaps in state protection.

Geographic comparison across Madhesh, Bagmati, and Lumbini Provinces further demonstrates that TFGBV risks and coping strategies are shaped by local social contexts. Differences in literacy levels, digital access, community visibility, and social norms influence how individuals experience harm and whether support is accessible. In settings characterised by strong social surveillance or limited services, the consequences of digital exposure are often more severe, reinforcing silence and self-censorship. These findings reflect the need for responses that recognise provincial diversity rather than relying on uniform national approaches.

A critical insight emerging from the research is the central role of outing and identity-based harassment as mechanisms of control. The threat of exposure operates as a powerful form of coercion within a social environment where disclosure may lead to family rejection, violence, economic loss, or exclusion from community life. TFGBV, thus, functions along a digital–social continuum, where online abuse cannot be separated from offline realities of stigma and structural discrimination. Addressing TFGBV therefore, requires interventions that extend beyond platform regulation or cybercrime enforcement to include broader social, legal, and institutional transformation.

The study also highlights the limitations of Nepal's current legal and policy framework in addressing contemporary digital harms. Existing legislation predates widespread social media use and lacks clear definitions and safeguards for identity-based violence. Ambiguity in law, inconsistent institutional interpretation, and absence of SOGIESC-sensitive data systems contribute to under-recognition of harm and weaken prevention and accountability efforts. Without reliable and ethically collected data, LGBTIQ+ experiences remain largely invisible in national planning, resource allocation, and policy development.

At the same time, the research documents significant community-driven resilience and adaptive strategies. LGBTIQ+ individuals and organisations actively develop informal protection mechanisms, share safety knowledge, and provide psychosocial and legal support despite severe resource constraints. These initiatives represent critical sources of solidarity and protection within the community. However, such efforts cannot substitute for institutional responsibility. Sustainable protection requires shifting from reliance on individual coping strategies toward coordinated systems that distribute responsibility across state institutions, civil society, development partners, and digital platforms.

The findings collectively indicate that effective responses to TFGBV must move beyond isolated awareness activities toward the development of an integrated protection ecosystem. Such an ecosystem should encompass legal reform, strengthened institutional capacity, confidential and accessible reporting mechanisms, inclusive service delivery, social norm change, and sustained investment in community-led organisations. Prevention efforts must address and dismantle the structural and societal attitudes that enable digital hostility, while response mechanisms must ensure safety, dignity, and accountability for victims.

Ultimately, TFGBV represents a pressing governance and human rights challenge within Nepal's ongoing digital transformation. Meaningful participation in digital spaces is now intrinsically linked to education, employment, civic engagement, and freedom of expression. Ensuring digital safety for LGBTIQ+ individuals is therefore not merely a question of minority protection; it is a measure of whether Nepal's digital future is equitable, inclusive, and rights-respecting. The evidence generated through this study establishes a robust foundation for policy reform, targeted programmatic investment, and institutional accountability. The next phase requires translating this evidence into sustained political and institutional commitments that centre survivor safety, dignity, and equality within Nepal's digital development trajectory.

Annex-1 List of References

Amnesty International. "Human Rights Implications of Technology-Facilitated Gender-Based Violence." Amnesty International, 2025. Available at amnesty.org/en/documents/act30/8404/2024/en/.

Body & Data. "Identities Experiencing Internet: Nepal Survey Report" Body & Data, 2021.
Available at https://bodyanddata.org/identities-experiencing-internet-nepal-survey-report/

— "Mapping Laws Relevant to Online Violence in Nepal" Body & Data, 2021. Available at https://bodyanddata.org/mapping-laws-relevant-to-online-violence-in-nepal/

Citron, Danielle Keats. Hate Crimes in Cyberspace. Harvard University Press, 2014.
Digital Rights Foundation. "Online Violence against Women in Pakistan" DRF, 2024. Available at https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/UNSR-Submission-by- DRF.pdf.

Digital Rights Nepal. "State of Digital Rights and Safety in Nepal 2024." DRN Press, 2024. Available at digitalrightsnepal.org/wp-content/uploads/2025/05/STATE-OF-DIGITAL- RIGHTS-AND-SAFETY-IN-NEPAL-2024.pdf.

— Brief Analysis of Social Media (Operation, Usage and Regulation) Bill, 2082'. August 2025. Available at https://digitalrightsnepal.org/report/four-page-brief-social-media-operation-usage-and-regulation-bill-2082/

Equality Now. "Sexual violence in South Asia: Legal and other barriers for justice to victims" Equality Now. 2021.

Government of Nepal. "Constitution of Nepal." 2015.

— "Electronic Transactions Act, 2063 (2008)." 2008.

— "Muluki Criminal Code, 2074 (2017)." 2017.

— "Muluki Criminal Procedure Code, 2074 (2017)." 2017.

— "Privacy Act, 2075 (2018)." Government of Nepal, 2018.

Human Rights Watch. ""All This Terror Because of a Photo": Digital Targeting and Its Offline Consequences for LGBT People." HRW, 2023. Available at https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its- offline-consequences-lgbt.

ILGA Asia. "Nepal: Marriage Registration for Same-Sex Couples after Seminal Court Ruling – ILGA ASIA." Ilgaasia.org, July 2024, ilgaasia.org/news/nepal- marriage-registration-for-same-sex-couples-after-seminal-court-ruling/. Accessed 26 Dec. 2025.

Kapali, Rukshana. "Rukshana Kapali vs. Government of Nepal (Writ No. 077-WO-0413)." Supreme Court of Nepal, 2024.Nepal Police, "Police Guidelines, 2071 (2013)." 2013

OHCHR. 'LGBTIQ women' OHCHR. Available at https://www.ohchr.org/en/sexual-orientation-and-gender-identity/lgbtiq-women

Paudel, Shambhawi and Shubha Kayashta. “Privacy in the Digital Age and as Understood by Marginalised Groups in Nepal”, presented at the Annual Kathmandu Conference on the Nepal and the Himalayas, 2023.

SCC Times. ‘Sexual orientation an innate part of identity of LGBTQ+ persons’: Kerala HC upholds Right of choice and Right to live life of a queer woman’. June 2024. Available at: https://www.scconline.com/blog/post/2024/06/27/sexual-orientation-innate-part-identity-lgbt-persons-kerala-hc-dismisses-writ-parents-queer-woman-psychologically-treat-sexual-orientation/

UN Women. "Evidence to Action: Addressing Violence Against LGBTIQ+ People in Nepal." UN Nepal, 2023. Available at un.org.np/sites/default/files/doc_publication/2023- 06/LGBTIQ%20Study%20Report-Final-web%20version- 11%20June%202023%20evening.pdf.

UNESCO. “Social Media Bill 2081: Legal Analysis” 2025. Available at: https://articles.unesco.org/sites/default/files/medias/fichiers/2025/03/SM%20bill%20legal%20Analysis%20%283%29.pdf

University of Melbourne & UNFPA. “Understanding technology-facilitated gender-based violence in Asia: A qualitative study” UNFPA. 2024.

The Yogyakarta Principles plus 10. YP+10, 2017. Available at yogyakartaprinciples.org/principles-en/yp10/.

Annex 2- Quantitative Survey Response

Survey on TFGBV(Technology Fa

Quantitative Survey Response

Annex 3 KII Interview Information

Date	Organization	Position
02/12/2025	Blue Diamond Society	Executive Director
03/12/2025	NHRC	Human Rights Officer
04/12/2025	Cyber Bureau Nepal	Spokesperson
08/12/2025	FSGMN	Chairperson
09/12/2025	Digital Rights Nepal	Chairperson
10/12/2025	Body and Data	Program Manager
11.12.2025	MOWCSC	Section Officer

DanChurchAid-DCA
House No-78, Ward No-2
GPO Box 4844
Bijayanagar, Sanepa, Lalitpur
+977 1 5453505/5433550/5455621
dcanepal@dca.dk
https://www.danchurchaid.org/what-we-do/where-we-work/nepal
DCA Nepal
@DCA_Nepal
DCA in Nepal